



FENESTRA TI

GLOBAL INTELLIGENCE. **CONNECTED INSIGHT.**

SECTOR THREAT LANDSCAPE

ENERGY & UTILITIES

Q3 2026 · Winter 2026–27 Outlook

Physical attacks, maritime supply risk, ransomware and state-linked cyber activity against the global energy sector — what moved between July and September, and what to expect this winter.

EXECUTIVE SUMMARY

ENERGY IS NOW A PRIMARY TARGET, NOT COLLATERAL

Across the quarter, energy infrastructure moved from being damaged *in* conflicts to being the deliberate objective *of* them. Ukraine's long-range drone campaign has now struck most major Russian refineries while Russia pounded Ukraine's power plants and substations; the war over energy then widened in the Gulf, where attacks moved ashore, culminating in the shutdown of Saudi Arabia's East-West pipeline and Aramco suspending October crude deliveries to European customers. Brent crossed \$108.

In cyberspace, the sector faced state-linked disruption — an Iran-linked attack took a UK power plant offline for four days — alongside a steady stream of ransomware concentrated on oil & gas, including three national oil companies, and on the contractors and utilities around them, largely entering through unpatched firewalls, VPNs and stolen logins. A new front opened at sea, with a US Coast Guard and FBI cyber boarding of a US-bound tanker and a claimed takeover of an LNG carrier's safety systems.

Going into winter, both sides of the Russia-Ukraine energy war are signalling escalation, Gulf supply remains exposed, and Europe enters the season with thin buffers. Our key judgements and recommended actions close this report.

37%

Share of September's reported energy-attack days in the Gulf — up from 27% in July as strikes moved ashore

48%

Share of energy-sector ransomware victims in oil & gas; a further 18% were contractors and suppliers

\$108

Brent crude after the Saudi East-West pipeline shutdown and a fatal Hormuz strike

PHYSICAL & GEOSPATIAL SECURITY

ONE ENERGY WAR DOMINATES, A SECOND WIDENS

Share of days with a reported attack on energy infrastructure or energy shipping, by theatre:

THEATRE	JULY	AUGUST	SEPT *
Ukraine strikes on Russian energy	39%	33%	30%
Russian strikes on Ukrainian energy	30%	33%	21%
Gulf shipping: tankers, LNG & LPG carriers	20%	19%	26%
Gulf onshore energy sites	7%	7%	12%
Libya refineries, depots & substations	0%	4%	5%
European grid & pipeline sabotage	0%	2%	5%

Fenestra analysis of reported incidents across news and open-source channels; each attack counted once however widely reported. *September to 24 Sep. Remainder: other theatres.

RUSSIA & UKRAINE: A TWO-WAY ENERGY WAR

Mutual strikes on energy made up two-thirds of attack days in July and August. Ukrainian drones hit refineries from Moscow to Omsk — 3,000 km from the front¹ — halting Moscow's refinery on the last day of the Duma election² and Novorossiysk's Sheskharis terminal (~700,000 bpd)³. Russia struck Ukrainian power plants, substations and gas production on 13 days in July and 18 in August, then fewer in September — consistent with Ukrainian warnings that missiles are being held back for winter. A US-announced halt on energy strikes (14 Sep) did not hold⁴.

THE STANDOUT MOVER: THE GULF

Tanker attacks around Hormuz and the Red Sea ran at a fifth to a quarter of attack days all quarter; in September strikes intensified ashore, with Houthi attacks setting Saudi oil facilities alight on 8 September⁵ and drones from Iraq forcing the East-West pipeline — Saudi Arabia's main route around Hormuz — to close on 11 September⁶. The Gulf's share rose from 27% in July to 37% in September.

EUROPE & ELSEWHERE

Germany suffered a spate of grid attacks using rockets to throw wire across high-voltage lines; authorities link them to a militant climate activist, with no state link established^{7,8}. Libya saw a month of drone strikes on refineries and fuel depots⁹, and a deliberate blast halted a major Syrian gas pipeline¹⁰. The IAEA also reported a drone hit on a cooling tower at Russia's Kursk nuclear plant¹¹.

MARITIME & ENERGY SUPPLY CHAIN

CHOKEPOINTS UNDER FIRE, SHIPS UNDER ATTACK

HORMUZ AND THE GULF OF OMAN

Energy carriers were hit directly: a Qatari LNG carrier was among three tankers struck near Hormuz on 7 July¹², Iranian missiles hit UAE oil tankers on 14 July, killing a crew member¹³, and the LNG carrier *GasLog Shanghai* was hit while leaving the strait on 31 July¹⁴. A fatal strike on a merchant vessel in mid-September, combined with the Saudi pipeline closure, drove Brent above \$108¹⁵. With the East-West pipeline down, Saudi crude loses its main bypass of the strait — Aramco told European buyers to expect no October deliveries under long-term contracts¹⁶.

CYBER AT SEA — A GENUINE NEW FRONT

The US Coast Guard and FBI boarded a US-bound tanker in the Gulf of Mexico after its network was compromised by “foreign cyber actors”¹⁷; at least two tankers were reportedly hit, one losing communications for around 30 hours according to Iranian state media. Separately, the crew of an LNG carrier bound for Italy reported that attackers gained temporary control of steam-pressure and safety-valve systems during transit through the Strait of Gibraltar; the cargo was diverted and the class society is investigating¹⁸. The crew’s account is unconfirmed, but it describes exactly the ship-OT scenario the industry has long treated as theoretical.

RUSSIA’S EXPORT CHAIN AND THE SHADOW FLEET

Ukraine extended its campaign from refineries to export infrastructure — the Sheskhari terminal, Baltic oil ports and tankers. In parallel, European states escalated boardings and seizures of shadow-fleet tankers (UK in the Channel, Italy, EU naval forces, Norway). Moscow has threatened to “respond in kind” anywhere it chooses¹⁹ — a retaliation risk that extends to Western-flagged energy shipping and offshore infrastructure.

RANSOMWARE

OIL & GAS AT THE CENTRE, SUPPLIERS ON THE EDGE

Energy & utilities victims named on extortion sites between late June and September, by segment: **oil & gas 48%**, electrical contractors & supply chain 18%, power & grid utilities 16%, renewables 9%, water 8%. TheGentlemen (16%) and Qilin (15%) lead, followed by Akira (7%) and Deadlock (5%). The US accounts for a third of victims; Germany (6%) and Italy (5%) follow²⁰.

48%

of energy-sector victims were oil & gas — from drillers and pipeline builders to national oil companies

3

national oil companies listed in one quarter, including Colombia's Ecopetrol and South Sudan's Nile Petroleum

31%

of victims came from just two groups — TheGentlemen and Qilin

WHO WAS HIT

Named victims include US refiner Delek US, Colombia's Ecopetrol and EPM, South Sudan's national oil company, Vietnam Electricity's Hanoi utility, Laos's Nam Theun 2 hydropower operator, Thailand's PTT Oil & Retail, Turkey's largest independent oil-storage terminal operator, Italian and Spanish water utilities and a US rural electric cooperative. Clop's listing for Shell claimed engineering drawings and facility photographs — operational data with value well beyond extortion.

REPEAT VICTIMISATION

Argentina's Oleoductos del Valle pipeline operator was listed by TheGentlemen in July and again by INC Ransom in August — a pattern consistent with access being resold or reused between criminal groups. Organisations recovering from one incident should assume their access paths are known to others.

ONE LINEAGE, ALMOST A THIRD OF VICTIMS

Unit 42 assesses that TheGentlemen's operators began as an affiliate of Qilin before launching their own ransomware-as-a-service in mid-2025, so the two leading groups against energy share a lineage and, in part, a playbook²¹. Check Point counted around 332 TheGentlemen victims in the first five months of 2026 alone²².

GERMANY'S UTILITIES IN QILIN'S SIGHTS

Qilin claimed three of Germany's four energy victims in August–September, including a municipal Stadtwerke, while Stadtwerke Landsberg in Bavaria separately had its IT encrypted²³ on 1 September.

HOW THE LEADING GROUPS GET IN

FIREWALLS, VPNS AND STOLEN LOGINS

FIREWALLS ARE THE COMMON THREAD

Four of the five leading energy groups with documented playbooks have exploited Fortinet: Qilin (CVE-2024-21762, CVE-2024-55591, CVE-2025-59718), TheGentlemen (CVE-2024-55591 and FortiGate SSL-VPN logins), Akira (CVE-2022-40684, FortiClient CVE-2023-48788) and Play (CVE-2018-13379). Qilin has since moved across vendors: Arctic Wolf traced several June 2026 intrusions from Palo Alto firewall flaw CVE-2026-0257 to Qilin encryption²⁴; a Qilin affiliate exploited WatchGuard Fireware (CVE-2025-9242, CVE-2025-14733)²⁵; and Cisco reported this month that Secure Firewall Management Center flaws (CVE-2026-20079, CVSS 10, and CVE-2026-20316) are being used to deploy Qilin²⁶.

VALID ACCOUNTS, EVERY TIME

Every one of these groups is documented using valid credentials for initial access (ATT&CK T1078) — VPN and RDP logins, domain accounts, and in Qilin's case credentials harvested from browsers on compromised endpoints.

THROUGH THE SUPPLIER

Qilin affiliates spear-phished managed-service-provider administrators via ScreenConnect to reach their customers downstream — consistent with contractors and suppliers making up nearly a fifth of energy victims (18%).

BACKUPS FIRST

Both Qilin and Akira exploit Veeam Backup & Replication (CVE-2023-27532) to disable recovery before encrypting.

NEWLY EXPLOITED THIS QUARTER (CISA KEV)²⁷**CVE-2026-8452 / CVE-2026-19490 — CITRIX NETSCALER ADC & GATEWAY**

Memory-overflow RCE and a SAML authentication bypass, added 26 Aug and 9 Sep — a common front door for utility remote access.

CVE-2026-15409 / -15410 · CVE-2026-83548 / -83549 — SONICWALL SMA1000

Two exploited pairs in one quarter; INC Ransom is reported to have exploited the July pair.

CVE-2026-84869 · CVE-2026-18556 / -18577 · CVE-2026-93952 — SCREENCONNECT · N-ABLE N-CENTRAL · VELOCLOUD SD-WAN

Exploited remote-management and SD-WAN tooling — the links contractors and remote sites use.

CYBER THREAT INTELLIGENCE

STATE ACTORS REACH INTO OPERATIONAL SYSTEMS

IRAN: FROM THREAT TO IMPACT

An Iran-linked cyberattack shut down a small UK power generator for four days in July²⁸, reported after the UK allowed US operations against Iran from British bases. The US has offered \$10 million for the head of the IRGC's Cyber-Electronic Command, which directs CyberAv3ngers — the group behind previous attacks on water-utility PLCs²⁹. CISA separately observed malicious activity against more than 100 internet-exposed water and wastewater systems, with utilities in at least 12 US states attacked in July³⁰.

UTILITIES UNDER DISRUPTION AND EXTORTION

Stadtwerke Landsberg (Bavaria) had its central IT encrypted on 1 September; electricity and water supply continued²³. CenterPoint Energy confirmed customer data was taken via an external-facing system after a dark-web sale claiming ~7.5 million records³¹. Washington has banned acquisition of foreign-made bulk-power-system equipment over backdoor concerns — a supply-chain shift operators will feel in procurement³⁰.

IDENTITY IS THE SOFT UNDERBELLY

Fenestra's credential-exposure analysis found corporate single sign-on (ADFS) and Microsoft 365 credentials for an employee of an Asian national oil & gas company, stolen by infostealer malware around June 2026 — some two months before the company was hit by ransomware in August. The timing is consistent with credential-based initial access rather than proof of it, but it is the pattern to defend against. CISA also added an ADFS flaw (CVE-2026-56155) to its exploited list in July.

PLCS UNDER ACTIVE ATTACK

A joint US federal advisory, updated in July, warns of an ongoing campaign exploiting internet-exposed PLCs in energy, water and government facilities: attackers connect with legitimate engineering software and manipulate operator displays so changes go unseen. The update widened the scope from Rockwell to Schneider Electric and Siemens equipment, and — unlike a similar 2023 campaign — reports confirmed operational disruption³². Censys counts ~134,000 internet-exposed ICS hosts, around 70% on consumer and mobile networks where owners are hard to identify and notify³³. CISA also flagged critical flaws in Hitachi Energy's FACTS grid-control platform (CVSS 9.9)³⁴ and issued guidance on limiting third-party ICS integrators' access³⁵.

UNDERGROUND FORUMS

Forum-side energy activity was largely data-dump trading; one thread advertised an alleged Iranian nuclear-energy database in August (unverified).

WINTER 2026-27 OUTLOOK · KEY JUDGEMENTS

WHAT TO EXPECT THROUGH MARCH

HIGHLY LIKELY **The Russia–Ukraine energy war intensifies**

Russia's Defence Ministry announced preparations for 'massive' strikes on Ukrainian energy on 31 August³⁶, and Ukraine's refinery campaign continued through the US-announced halt. Expect grid strikes in Ukraine to peak with winter demand, and further Russian refinery and export-terminal outages.

LIKELY **Gulf energy supply remains disrupted**

Houthi and Iraq-based militia drone capability against Saudi energy is demonstrated, and Hormuz traffic remains under attack. European refiners — already cut off from October Saudi crude — face the most direct exposure; price volatility will persist.

LIKELY **Attacks on energy and water OT continue, led by Iran-linked actors**

The UK generator outage, IRGC-directed targeting of water-utility PLCs and an ongoing, disruptive PLC campaign across US energy and water show intent and capability. Smaller generators, water utilities and internet-exposed PLCs/HMIs are the most probable targets.

LIKELY **Ransomware keeps hitting utilities' soft perimeter**

Contractors, municipal utilities and oil & gas service firms will remain the bulk of victims, reached through newly disclosed firewall flaws, remote-management tools and stolen credentials rather than OT itself — Qilin's affiliates have exploited at least four firewall vendors.

REALISTIC POSSIBILITY **Sabotage against European energy infrastructure**

Russia has threatened retaliation for shadow-fleet seizures 'anywhere', and has rehearsed undersea-cable sabotage³⁷. Germany's grid attacks — with no established state link — show low-cost methods are available to any actor.

REALISTIC POSSIBILITY **Maritime cyber incidents with physical effect**

Following the tanker and LNG-carrier incidents, further attempts on ship navigation, communications and machinery systems are credible, particularly for vessels trading with the US and Europe.

Likelihood terms follow the UK Professional Head of Intelligence Assessment yardstick: highly likely 80–90%, likely 55–75%, realistic possibility 25–50%.

RECOMMENDED ACTIONS

WHERE TO SPEND EFFORT BEFORE WINTER

1 · CLOSE THE EXPLOITED EDGE

Patch or isolate the firewall and remote-access platforms named in this report — Fortinet above all, then Palo Alto, Cisco FMC and ASA/FTD, WatchGuard, NetScaler, SonicWall SMA1000 and VeloCloud — and remove any management interfaces from the internet. Treat them as incident candidates, not just patch tickets, if they were exposed unpatched.

2 · HARDEN IDENTITY AND WATCH FOR STOLEN CREDENTIALS

Enforce phishing-resistant MFA on SSO, VPN and M365; review ADFS against CVE-2026-56155; and monitor infostealer and breach sources for staff and contractor credentials so exposed accounts are reset before they are used.

3 · GOVERN THIRD-PARTY REMOTE ACCESS

Inventory every contractor route into IT and OT — ScreenConnect, N-central, SimpleHelp and similar — require brokered, time-limited, logged access, and include suppliers in incident exercises. Keep backups offline or immutable and patch Veeam; the leading groups target it first.

4 · TAKE OT OFF THE INTERNET

No PLC, HMI or telecontrol interface should be reachable from the internet. Segment IT from OT, monitor industrial protocols (Modbus, S7, IEC 60870-5-104, DNP3) and engineering-software logins, apply least privilege to ICS integrators, and rehearse manual operation.

5 · PLAN FOR PHYSICAL AND SUPPLY SHOCKS

Review perimeter protection and drone awareness at substations, depots and terminals; plan for short-notice rolling outages; and stress-test supply against continued Gulf and Russian disruption.

6 · TREAT VESSELS AS OT

For shipping and LNG operators: segment bridge and machinery systems, control satellite and remote maintenance links, and brief crews on reporting suspected interference promptly.

SOURCES

Numbered references to public reporting cited in this briefing. Theatre shares, energy-sector ransomware figures and the credential-exposure case are Fenestra analysis of its own collection.

1. Kyiv Post — Russia's Largest Oil Refinery Stops Processing After Ukraine's 3,000-km Strike (8 Jul 2026).
<https://www.kyivpost.com/post/79829>
2. Meduza — Reuters: Ukrainian drone attack halts oil processing at Moscow refinery on final day of Russia's State Duma election. Repairs could take weeks. (21 Sep 2026).
<https://meduza.io/en/news/2026/09/21/reuters-ukrainian-drone-attack-halts-oil-processing-at-moscow-refinery-on-final-day-of-russia-s-state-duma-election-repairs-could-take-weeks>
3. Meduza — Drone threat halts Russia's main Black Sea oil terminal, which normally ships 700,000 barrels a day (14 Aug 2026).
<https://meduza.io/en/news/2026/08/14/drone-threat-halts-russia-s-main-black-sea-oil-terminal-which-normally-ships-700-000-barrels-a-day>
4. Meduza — Trump claimed that Russia and Ukraine had agreed to an energy truce. Neither side stopped the strikes. (15 Sep 2026).
<https://meduza.io/en/feature/2026/09/15/trump-claimed-that-russia-and-ukraine-had-agreed-to-an-energy-truce-neither-side-stopped-the-strikes>
5. Dawn — Houthis attacks disrupt Saudi energy facilities, wound 73, authorities say (8 Sep 2026).
<https://www.dawn.com/news/20260908/houthi-attacks-disrupt-saudi-energy-facilities-wound-73-authorities-say>
6. Al Jazeera — Saudi Arabia says East-West pipeline hit by drones launched from Iraq (11 Sep 2026).
<https://www.aljazeera.com/news/2026/9/11/saudi-arabia-says-east-west-pipeline-hit-by-drones-launched-from-iraq>
7. France 24 — German power grid sabotage attack linked to 'climate extremism' (4 Sep 2026).
<https://www.france24.com/en/europe/20260904-german-power-grid-sabotage-attack-linked-to-climate-extremism>
8. Meduza — German police detain substation sabotage suspect near a power plant with explosive devices in his possession and bombs in a nearby tent (8 Sep 2026).
<https://meduza.io/en/news/2026/09/08/german-police-detain-substation-sabotage-suspect-near-a-power-plant-with-explosive-devices-in-his-possession-and-bombs-in-a-nearby-tent>
9. Al Jazeera — Fire rages after drone strikes Libya's largest oil refinery (11 Aug 2026).
<https://www.aljazeera.com/video/newsfeed/2026/8/11/fire-rages-after-drone-strikes-libya-s-largest-oil-refinery>
10. Middle East Eye — Blast at major Syrian pipeline halts gas flow, disrupts power generation (19 Aug 2026).
<https://www.middleeasteye.net/live-blog/live-blog-update/blast-major-syrian-pipeline-halts-gas-flow-disrupts-power-generation>
11. NDTV — Drone Hits Cooling Tower At Russia's Nuclear Plant, Says UN Nuclear Watchdog (18 Sep 2026).
<https://www.ndtv.com/world-news/drone-hits-cooling-tower-at-russia-s-nuclear-plant-says-un-nuclear-watchdog-12066626>
12. The Hindu — Three tankers hit in latest attacks in Strait of Hormuz: UKMT0 (7 Jul 2026).
<https://www.thehindu.com/news/international/three-tankers-hit-in-latest-attacks-in-strait-of-hormuz-ukmt0/article71194549.ece>
13. South China Morning Post — UAE says Iranian missiles struck tankers in Hormuz, killing and injuring crew (14 Jul 2026).
<https://www.scmp.com/news/world/middle-east/article/3360442/uae-says-iranian-missiles-struck-tankers-hormuz-killing-and-injuring-crew>
14. MarineTraffic — GasLog LNG Carrier Struck Off Oman; All Crew Members Safe (3 Aug 2026).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13140/gaslog-lng-carrier-struck-off-oman-all-crew-members-safe>
15. Euronews — Oil surges past \$108 as Hormuz attack and Saudi pipeline shutdown rattle markets (14 Sep 2026).
<https://www.euronews.com/business/2026/09/14/oil-surges-past-107-as-hormuz-attack-and-saudi-pipeline-shutdown-rattle-markets>
16. Meduza — Saudi Aramco tells European customers they won't receive October crude under long-term contracts after drone attack shuts down key pipeline (18 Sep 2026).
<https://meduza.io/en/news/2026/09/18/saudi-aramco-tells-european-customers-they-won-t-receive-october-crude-under-long-term-contracts-after-drone-attack-shuts-down-key-pipeline>
17. The Record — Coast Guard, FBI boarded tanker after attack by 'foreign cyber actors' (16 Sep 2026).
<https://therecord.media/oil-tanker-cyberattack-coast-guard-fbi>
18. Splash247 — Crew claims hackers seized control of LNG carrier safety systems (20 Sep 2026).
<https://splash247.com/crew-claims-hackers-seized-control-of-lng-carrier-safety-systems/>
19. BBC News — UK defends seizing shadow fleet tanker after Putin threat (13 Aug 2026).
<https://www.bbc.co.uk/news/articles/cn0npn249qvo>
20. Ransomware.live — Leak-site victim data and group profiles (Pro API) (Jun-Sep 2026).
<https://www.ransomware.live>
21. Palo Alto Networks Unit 42 — No Manners Here: The Ruthless Rise of The Gentlemen Ransomware (10 Jul 2026).
<https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/>
22. Check Point Research — Thus Spoke...The Gentlemen (13 May 2026).
<https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/>
23. The Record — Cyberattack encrypts systems at Bavarian municipal utility (8 Sep 2026).
<https://therecord.media/cyberattack-bavaria-germany-utility>
24. Arctic Wolf — Cookie Crumbles: How Exploitation of CVE-2026-0257 Leads to Qilin Ransomware (20 Jul 2026).
<https://arcticwolf.com/resources/blog/exploitation-of-cve-2026-0257-leads-to-qilin-ransomware/>
25. Ctrl-Alt-Intel — Watch Guard! Qilin affiliate exploits network appliances for initial access (1 May 2026).
<https://ctrlaltintel.com/research/Qilin/>
26. The Hacker News — Cisco FMC Flaws Exploited to Steal Credentials and Deploy Qilin Ransomware (24 Sep 2026).
<https://thehackernews.com/2026/09/cisco-fmc-flaws-exploited-to-steal.html>
27. CISA — Known Exploited Vulnerabilities Catalog (Jul-Sep 2026).
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
28. The Guardian — Iran-linked hackers blamed for cyber-attack that shut down UK power plant (23 Aug 2026).
<https://www.theguardian.com/world/2026/aug/23/iran-linked-hackers-blamed-cyber-attack-british-power-plant>
29. The Record — US offers \$10 million for info on Iranian allegedly behind cyberattacks on critical infrastructure (4 Sep 2026).
<https://therecord.media/us-reward-amir-yaryab-iran-irgc-cyberattacks>
30. The Record — White House bans foreign-made equipment for power generation over cyber backdoor concerns (27 Aug 2026).
<https://therecord.media/trump-cyber-electricity-parts>
31. The Record — Electric and gas utility CenterPoint Energy warns of data breach after dark web post (15 Sep 2026).
<https://therecord.media/centerpoint-energy-data-breach>
32. Trend Micro — Federal Agencies Warn of Ongoing PLC Exploitation Against Critical U.S. Infrastructure (23 Jul 2026).
https://www.trendmicro.com/en_us/research/26/g/plc-exploitation.html
33. Censys — 2026 State of the Internet: The Exposure Notification Gap in ICS Devices (8 Sep 2026).
<https://censys.com/blog/2026-state-of-the-internet-ics/>
34. CISA — Hitachi Energy FACTS Control Platform (FCP) (17 Sep 2026).
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-260-03>
35. CISA — Considerations for Critical Infrastructure Operators Working With Third-Party ICS Integrators (23 Sep 2026).
<https://www.cisa.gov/resources-tools/resources/considerations-critical-infrastructure-operators-working-third-party-ics-integrators>
36. Meduza — Russia's Defense Ministry says it is preparing large-scale strikes on Ukraine's energy facilities in response to Ukrainian attacks on Russian infrastructure (31 Aug 2026).
<https://meduza.io/en/news/2026/08/31/russia-s-defense-ministry-says-it-is-preparing-large-scale-strikes-on-ukraine-s-energy-facilities-in-response-to-ukrainian-attacks-on-russian-infrastructure>
37. Euronews — NATO allies successfully thwart Russian undersea cable sabotage operation (10 Sep 2026).
<https://www.euronews.com/my-europe/2026/09/10/nato-allies-successfully-thwart-russian-undersea-cable-sabotage-operation>

