WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Monday, 2 November 2026 | Vol. 2026-306 | As of 020730 EST NOV 26

BLUF. The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS**, with the trend turning ↑. On the night of 1 Nov, attackers sent false nuclear, radiation and chemical warnings through Ukraine's Air Alert app, which was suspended and then restored, and Russia's emergency-ministry app sent fake alerts hours later. Public warning systems in two warring states were turned against their own users on the same night. University Hospitals in Cleveland still lists MyChart as offline, and Moldova has still not named a culprit for its state-services breach. Ransomware leak-site postings for 26 Oct to 1 Nov closed at 279, which is 121% of the 8-week mean and under the 125% bar, so **TEC-08 resolves as a miss**. CISA has added nothing to the KEV catalog since 30 Oct. Chips and AI governance stay at **NO CRISIS**, and MOFCOM No. 70 ends in eight days with no extending notice. TEC-22 and TEC-23 are new.

0. WIRE Technology & Cyber Dashboard

TOPIC	CRISIS LEVEL	DOM. INDICATOR	KEY DRIVER (today)	TREND
TEC-T1 Critical-infrastructure cyber	ENVIRONMENT FOR CRISIS	SIGNIFICANT	K-3: emergency-alert apps hijacked in Ukraine and Russia; UH MyChart still down	↑
TEC-T3 Space and undersea infrastructure	ENVIRONMENT FOR CRISIS	SIGNIFICANT	O-1: two Starlink attacks in 30 days; no new attack	=
TEC-T4 AI governance and incidents	NO CRISIS	ABNORMAL	AI-1: AI Office still assessing replies, no finding	=
TEC-T2 Semiconductors and compute	NO CRISIS	ABNORMAL	X-1: MOFCOM No. 70 ends 10 Nov, still unamended	=

Indicator: ROUTINE ABNORMAL SIGNIFICANT EXTREME **Crisis level:** NO CRISIS ENV. FOR CRISIS POTENTIAL PROBABLE IMMINENT

Family level = highest topic level (TEC-T1 and TEC-T3). Roll-up per WIRE_METHOD §1a. Trend key: ↑ toward crisis, ↓ away, = no net change.

Change line. No level changes. TEC-T1 trend = to ↑ (a new disruptive attack on public warning services). Family trend = to ↑.

Moved indicators (vs 1 Nov). None changed score. K-4 closed its week at 279 postings (121% of the 8-week mean of 230), still ROUTINE. K-1 starts a new week at 0 additions.

I. TEC-T1 CRITICAL-INFRASTRUCTURE CYBER | ENVIRONMENT FOR CRISIS

Facts. Late on 1 Nov, Ukraine's Air Alert app pushed false warnings of nuclear, radiation and chemical danger, including a message saying an Oreshnik missile was incoming. The app was temporarily suspended and later restored, and Ukraine's Digital Transformation Ministry said sirens and other alert channels kept working (AP, 2 Nov; Kyiv Independent). Hours later, Russia's emergency-ministry app also sent fake alerts. Ukraine's strategic communications agency blamed Russia for the Ukrainian attack, and the Russian app's developers said unauthorised parties had interfered (NBC News; BBC). University Hospitals' incident page still says MyChart remains offline with no estimated timeline, and that UH servers are not connected to the internet (UH). Moldova's prime minister says further attack attempts on 25 and 27 Oct were blocked, and most targeted services have been remediated (Moldpres). Moldova's economy and digitalisation minister pointed to "geopolitical motives" but said he had no data to confirm Russian involvement (MLive.md, 30 Oct). Lumen's Black Lotus Labs published research on a China-linked operation it calls "Silent Train," attributed to Volt Typhoon, that used chains of compromised routers and zero-days against water, energy, transport and satellite-communications targets (Industrial Cyber, 2 Nov). This is vendor research, not a government advisory. The KEV catalog stays at version 2026.10.30 with 1,766 entries (KEV JSON). Ransomware.live logged 279 victims discovered 26 Oct to 1 Nov (UTC) against an 8-week mean of 230 for 31 Aug to 25 Oct (feed). **Indicators.** K-1: ABNORMAL (10 in the week of 26 Oct; 0 so far in the week of 2 Nov). K-2: ABNORMAL (carried; the Lumen report does not count because it is not a joint advisory). K-3: SIGNIFICANT (UH; alert-app hijacks). K-4: ROUTINE (121%). K-5: ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** Fake nuclear warnings sent through a trusted wartime alert channel are a step up from data theft: they target public behaviour, not just systems. The attack does not touch US or allied infrastructure directly, so it raises the trend but not the level. The quick restore and working sirens limited the harm.

II. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | ENVIRONMENT FOR CRISIS

Facts. No new ground-station or cable attack was found. Coverage on 2 Nov restates the Lithuanian finding of 29 Oct that one network carried out the Starlink-site arsons in three NATO states, and that terrorism charges were filed (Tech Times, 2 Nov). **Indicators.** O-1: SIGNIFICANT (2 in 30 days). O-2: ABNORMAL (carried). O-3: ABNORMAL (carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =.

III. TEC-T4 AI GOVERNANCE AND INCIDENTS | NO CRISIS

Facts. The Commission says it has received most replies to its AI Act information requests to more than 30 AI providers, extended some deadlines, and is assessing the submissions. No finding or penalty has been announced (2eu.brussels). **Indicators.** AI-1/2/3: ABNORMAL. **Override −1 to NO CRISIS (held):** no AI incident has disrupted a critical service and no formal proceeding is open.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. MOFCOM No. 70 still suspends the October 2025 export-control package only "until 10 November 2026" (MOFCOM No. 70). As of 29 Oct, MOFCOM had published no notice amending it, and No. 72 (gallium, germanium and antimony to the US) still ends 27 Nov (Strategic Raw Material). No new BIS chip rule was found. **Indicators.** X-1: ABNORMAL. X-2 to X-4: ROUTINE. Roll-up: NO CRISIS (=).

V. PREDICTIONS

Resolved: - **TEC-08 MISS.** Postings for 26 Oct to 1 Nov closed at 279, under the 287.5 bar (1.25 times the 8-week mean of 230) (ransomware.live feed). Forecast 15%; Brier 0.0225.

Open: TEC-02 (No. 70, 10 Nov), TEC-11 and TEC-13 (due 6 Nov), TEC-20 (KEV week of 2 Nov, 0 so far), and TEC-01/05/06/07/09/10/12/14 to 19/21. New (logged in the prediction ledger): - **TEC-22:** CISA, FBI or NSA publishes an advisory or web page naming Volt Typhoon, dated 2 to 30 Nov 2026. **20%, unlikely.** - **TEC-23:** A Ukrainian government body (SSU, CERT-UA, the State Special Communications Service, the Digital Transformation Ministry or the Center for Strategic Communications) names a specific Russian intelligence service or a named threat group as responsible for the 1 Nov Air Alert app attack by 30 Nov 2026. **40%, unlikely.**

VI. GAPS AND UNVERIFIED

- **Alert apps:** the AP article could not be loaded from the box; details come from search summaries of AP, Kyiv Independent, NBC and BBC. A hacker group's claim of responsibility is unverified and not named here. How the apps were breached is not public.
- **Silent Train:** the findings come from one vendor and have not been confirmed by a government agency.
- **UH:** whether ransomware was involved is still not public.
- **TSMC IR, gpsjam.org, AIID and EDGAR full-text search** were not queried today. TSMC's October revenue is due about 10 Nov.

Sources

AP; Kyiv Independent; NBC News; BBC; University Hospitals; Moldpres; MLive.md; Industrial Cyber; CISA KEV; ransomware.live; Tech Times; 2eu.brussels; MOFCOM; Strategic Raw Material.