WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Wednesday, 28 October 2026 | Vol. 2026-301 | As of 280725 EDT OCT 26

BLUF. The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS (↑)**. On 26 Oct a second US hospital system was disrupted. UNM Health, home to New Mexico's only Level 1 trauma center, diverted ambulances for two hours and cancelled appointments and outpatient surgeries after a cyberattack. Its systems were back online by 27 Oct, and a new ransomware gang, Byod, has claimed the attack. University Hospitals (Cleveland) still reports MyChart down six days into its own incident. Ransomware gang Qilin has listed a Mississippi electric cooperative, but the utility has confirmed nothing. Both hospital disruptions are regional and in one sector, so this desk does not raise TEC-T1 to POTENTIAL CRISIS. CISA's 29 Oct PHP2Shell deadline arrives with no victim named. Space and ground-segment infrastructure holds at **ENVIRONMENT FOR CRISIS (=)**. AI governance and chips stay at **NO CRISIS (=)**. No prediction falls due today. TEC-14 and TEC-15 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: second hospital system disrupted in a week (UNM Health ambulance diversion, claimed by Byod)	↑
TEC-T3 Space and undersea infrastructure	ENVIRONMENT FOR CRISIS	SIGNIFICANT	O-1: two Starlink ground-site attacks within 30 days (BG 9 Oct, LT 18 Oct); no new attack	=
TEC-T4 AI governance and incidents	NO CRISIS	ABNORMAL	AI-3: only short model-level degradations on 27 Oct; override held	=
TEC-T2 Semiconductors and compute	NO CRISIS	ROUTINE	X-2: MOFCOM No. 70 suspension still ends 10 Nov on paper; no new BIS chip rule	=

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 topic changed level. TEC-T1 keeps its ↑ trend because K-3 now rests on two hospital systems, not one. The family stays at ENVIRONMENT FOR CRISIS (↑).

Moved indicators (vs 27 Oct). No score changed. K-3 stays SIGNIFICANT, with a second confirmed hospital disruption. K-1 has 4 KEV additions this week, still ROUTINE.

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

Facts. UNM Health Sciences Center says its IT teams began containment around 11 a.m. on 26 Oct. From 12:30 to 2:30 p.m. it diverted ambulance traffic and suspended outpatient surgeries and appointments for the rest of the day. By 2:02 p.m. on 27 Oct, critical systems were back online, all hospitals were open and clinics had resumed. UNM says the event "affected some end-user devices but did not penetrate core systems or servers," and it has notified state and federal law enforcement (UNM HSC Newsroom, 27 Oct). According to The Record, the system has the state's only Level 1 trauma center, burn unit and children's hospital. A spokesperson would not say whether ransomware was involved (The Record, 27 Oct). The Byod gang claims it compromised 36,000 systems and took patient, student and employee data. UNM has not confirmed the claim (BleepingComputer, 27 Oct). Ransomware.live lists "University of New Mexico" under BYOD, discovered 26 Oct, and Qilin's listing of Delta Electric Power Association, also discovered 26 Oct (ransomware.live victim page). No outage at the cooperative has been confirmed. University Hospitals' latest statement (26 Oct) still says "Patients still cannot access MyChart," and expects problems "through the week" (WKYC). On PHP2Shell, the KEV feed (catalogVersion 2026.10.27, 1,760 entries) added Adobe Commerce CVE-2026-48356 and Google Brotli CVE-2026-111497 on 27 Oct (CISA KEV JSON; CISA alert). Nextgov reports that the KEV entries for PHP2Shell name no victims. It also reports that Sophos and Palo Alto Networks Unit 42 have withdrawn earlier claims of successful exploitation, Unit 42's in an attack on a European government agency (Nextgov/FCW, 27 Oct). EDGAR full-text search still shows only one October Item 1.05 8-K, Park Dental Partners (13 Oct) (EDGAR). Ransomware.live counts 86 victims for 26–27 Oct, against a weekly mean of 230 for the prior 8 weeks (ransomware.live feed). **Indicators.** K-1 KEV/ED: ROUTINE (4 this week; no new ED). K-2 state-actor advisory: ABNORMAL (AA26-281A, 8 Oct; the 20 Oct SafePay advisory is criminal, not state). K-3 disruption: SIGNIFICANT (two hospital systems). K-4 ransomware:

ROUTINE (the two-day pace projects about +20%, inside ±25%). K-5 Item 1.05: ROUTINE (1). Roll-up: 1 Significant + 1 Abnormal = ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** Two academic hospital systems lost clinical capacity within five days. At UNM that included trauma diversion for a whole state. Patient risk from cyber incidents is therefore real this week, but it is still regional and confined to one sector. This desk would move TEC-T1 to POTENTIAL CRISIS on a confirmed operational disruption in a second sector, for example if the Mississippi cooperative or another utility confirms an outage. A confirmed PHP2Shell compromise at a hospital, utility or pipeline would also do it. Nothing links either hospital incident to PHP2Shell, and the two incidents are not linked to each other. With vendor claims being withdrawn, TEC-05 (75%) is less certain than when it was logged, but it stands.

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

Facts. No new attack on a ground station or cable was found after Vilnius on 18 Oct. The two Sofia arson suspects are held in Germany pending extradition (Novinite/BNR, 26 Oct). Separately, SpaceX's owner said the company had throttled Ukraine's Starlink access and that the limit has since been lifted (CBS News, 27 Oct). **Indicators.** O-1: SIGNIFICANT (2 in 30 days; holds to 8 Nov). O-2: ROUTINE. O-3: ABNORMAL (Cosmos 2612, 17 Oct). Roll-up: ENVIRONMENT FOR CRISIS (=). **Analyst Comment.** The Ukraine throttling was a decision by the service provider, not hostile action, so it is not scored under O-1. It does show how a single commercial operator can switch off wartime connectivity.

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

Facts. Trackers logged short degradations of model services on 27 Oct, including a ChatGPT model degradation of about 77 minutes (Tickerr). No major cloud outage with a post-incident report was found. The AI Act high-risk deferral (to 2 Dec 2027) was already law in June (Council, 29 Jun). **Indicators.** AI-1: ABNORMAL. AI-2: ABNORMAL. AI-3: ABNORMAL (Google europe-west2, 20 Oct). Formula: ENVIRONMENT FOR CRISIS. **Override −1 to NO CRISIS (held):** no critical service or market has been disrupted by an AI incident, and the Commission has opened no formal proceeding. **Analyst Comment.** Quiet.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. The only BIS item in the 27 Oct Federal Register is a temporary denial order renewal, not a chip rule (Federal Register). No MOFCOM notice extends No. 70 past 10 Nov (MOFCOM No. 70; technology.org). **Indicators.** X-1 to X-4: ROUTINE. Roll-up: NO CRISIS (=). **Analyst Comment.** Thirteen days remain on No. 70. TEC-02 (70%) still depends on a published notice.

V. PREDICTIONS

Resolved: none due. TEC-06 and TEC-12 stay open because University Hospitals still uses only "cybersecurity incident" and no leak site lists it. TEC-05 and TEC-11 stay open because no victim or CISA observation has been published. New (logged in the prediction ledger): - **TEC-14:** UNM or UNM Health publicly confirms that patient, student or employee personal data was accessed or taken in the 26 Oct incident, by 15 Dec 2026. **55%, roughly even chance to likely.** - **TEC-15:** Delta Electric Power Association (Mississippi), or a state or federal authority, publicly confirms a cybersecurity incident at the cooperative by 30 Nov 2026. **35%, unlikely.**

VI. GAPS AND UNVERIFIED

- **Byod's claims** about 36,000 systems and data theft at UNM are unverified, and UNM disputes how far the attackers got.
- **Qilin's Delta Electric Power Association listing** is a leak-site claim only, with no confirmation and no reported outage.
- **CISA's evidence** behind the PHP2Shell KEV listing remains unpublished.
- **MOFCOM's 16 Oct draft** of controls on AI and chip-design technology exports was reported only in secondary sources (briefs.co). The primary text was not read, and the draft is not scored.
- **TSMC IR, gpsjam.org, EASA and the AIID** were not queried directly today.

Sources

UNM HSC Newsroom; The Record; BleepingComputer; ransomware.live; WKYC; CISA (KEV JSON, alerts); Nextgov/FCW; SEC EDGAR; Novinite/BNR; CBS News; Tickerr; Council of the EU; Federal Register; MOFCOM; technology.org; briefs.co.