WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Tuesday, 3 November 2026 | Vol. 2026-307 | As of 030730 EST NOV 26

BLUF. The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS**, and the trend stays ↑. Overnight into 2 Nov, attackers switched supermarket refrigeration units in seven European states to defrost mode, with about 40 Delhaize stores hit in Belgium and Luxembourg. This repeats an October attack on French stores, and the equipment operator says the fix needs physical changes, not just software. It came the same weekend as the hijacking of public alert apps in Ukraine and Russia. University Hospitals in Cleveland still lists MyChart as offline, with no timeline. The UK's cyber agency said on 3 Nov that it sees a "real prospect" of an unprecedented rise in incidents. CISA has added no KEV entries since 30 Oct, has issued no new directive, and EDGAR shows no Item 1.05 filing since 13 Oct. Chips, space and AI are unchanged, and MOFCOM No. 70 lapses in seven days without a published extension. No calls resolve today. TEC-24 and TEC-25 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: seven-country attack on supermarket refrigeration; UH MyChart still down	↑
TEC-T3 Space and undersea infrastructure	ENVIRONMENT FOR CRISIS	SIGNIFICANT	O-1: two Starlink-site attacks in 30 days; gpsjam Baltic steady	=
TEC-T4 AI governance and incidents	NO CRISIS	ABNORMAL	AI-1: AI Office still assessing replies; only minor AI outages	=
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 stays ↑ (a second disruptive multi-country attack in two days). Family trend stays ↑.

Moved indicators (vs 2 Nov). None changed score. K-3 gains a new event (the refrigeration attack). K-5 has now been checked: no Item 1.05 8-K since 13 Oct.

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

Facts. Refrigerators and freezers in dozens of supermarkets in Belgium, Luxembourg, Sweden, Ireland, the Netherlands, Estonia and Finland were attacked overnight, and their evaporators were switched to defrost mode. About 40 Delhaize stores were hit, along with 15 Carrefour stores in Belgium, 13 SuperValu stores in Ireland and seven Coop stores in Sweden. Sabcobel, which runs Delhaize's systems, called it a cyber-attack and said it is believed to use the same method as the October attack on French stores, and that units need physical modification. Belgium's and Sweden's national cyber agencies said they were monitoring the incident, the UK NCSC said it was working with partners, and no one has been named as responsible (BBC, 2 Nov; Euronews). University Hospitals' 2 Nov update says it is working to restore systems, that MyChart is still offline, and that there is "no estimated timeline for completion" (UH). UNM Health Sciences says its 26 Oct event affected some end-user devices but not core systems. A new group called Byod has claimed the attack on its leak site, and that claim is not verified (BleepingComputer). The UK NCSC published its Annual Review on 3 Nov. It judges it "highly likely" that AI-powered malware will have been used in a ransomware attack on UK critical national infrastructure by 2028 (NCSC; Guardian). On the alert apps, the Record reports that a group calling itself "Hitcore Corp" claimed the Ukrainian breach and "DC8044" claimed the Russian one. Ukraine's strategic communications center blamed Russia but named no service or group (The Record; Euronews). Moldova has made no attribution. The Cybersecurity Agency's director said at least 700 IP addresses were involved and attribution is "premature" (Radio Moldova; RFE/RL). The KEV catalog is still version 2026.10.30, with 1,766 entries and 0 additions so far in the week of 2 Nov (KEV JSON). The newest numbered directive is still ED 26-03, and the newest CISA advisory is dated 30 Oct (directives; advisories). EDGAR full-text search shows no 8-K with Item 1.05 filed between 14 Oct and 3 Nov; the last was Park Dental Partners on 13 Oct. Quest Diagnostics disclosed unauthorized access to its Quanum LSM system under Item 8.01 on 22 Oct (EDGAR FTS; Quest 8-K). Ransomware.live has logged 49 victims for 2–3 Nov (to 10:56 UTC), against an 8-week mean

of 239 per week for 7 Sep to 1 Nov (feed). **Indicators.** K-1: ABNORMAL (carried from 10 additions in the week of 26 Oct; 0 so far this week). K-2: ABNORMAL (carried; no new joint advisory). K-3: SIGNIFICANT (UH outage; alert-app hijacks; refrigeration attack). K-4: ROUTINE (week to date on pace). K-5: ROUTINE (no Item 1.05 since 13 Oct). Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** A repeat, multi-country hit on the food cold chain, which the operator says software alone cannot fix, shows an attacker can return at will to an exposed industrial control fleet. It is not yet a utility, pipeline or multi-sector outage, so the level holds. If it recurs or is attributed to a state, that would argue for POTENTIAL CRISIS.

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

Facts. No new ground-station or cable attack was found. The 2 Nov gpsjam.org daily file shows 160 of 585 Baltic-area H3 cells with more than 10% of aircraft reporting low navigation accuracy, close to 148 of 600 on 26 Oct and 162 of 612 on 19 Oct. The Black Sea showed 153 of 321 cells, against 107 to 132 in the three prior Mondays (gpsjam data). EASA's GNSS interference bulletin still names the Baltic as a key affected area (EASA). **Indicators.** O-1: SIGNIFICANT (2 in 30 days). O-2: ABNORMAL (steady; Black Sea higher). O-3: ABNORMAL (carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =.

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

Facts. No new Federal Register AI rule or presidential action was found for 29 Oct to 3 Nov (Federal Register API). Outages on 2 Nov were short and minor: GitHub reported 38 minutes of elevated errors on one hosted model, blamed on an upstream provider, with a root-cause analysis to follow (Pingoru). The AI Office has issued no finding on its information requests. **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. BIS's only Federal Register item since 26 Oct is a renewed temporary denial order (27 Oct), not a chip rule (FR 2026-21840). TSMC's September revenue was NT$511.86B, −0.6% m/m, which is ROUTINE. October is due about 10 Nov (TSMC). No MOFCOM notice amending No. 70 (ends 10 Nov) or No. 72 (ends 27 Nov) has been found (Nami; MOFCOM No. 70). **Indicators.** X-1: ABNORMAL. X-2 to X-4: ROUTINE. Roll-up: NO CRISIS (=).

V. PREDICTIONS

Resolved: none today. **Due soon:** TEC-11 and TEC-13 (6 Nov; the CISA PHP alert was last revised 26 Oct, and MyChart is still down), TEC-20 (KEV week of 2 Nov, 0 so far), TEC-02 (No. 70, 10 Nov). **Still open:** TEC-01, 05 to 07, 09, 10, 12, and 14 to 23. New (logged in the prediction ledger): - **TEC-24:** A national government body of an affected state (Belgium, Luxembourg, Sweden, Ireland, the Netherlands, Estonia, Finland or France) publicly names a specific state, state agency or named threat group as responsible for the November supermarket refrigeration attacks by 30 Nov 2026. **20%, unlikely.** - **TEC-25:** A new cyber-attack on retail refrigeration or cooling controllers in an EU or EEA state, with an incident date of 4–30 Nov 2026, is confirmed by an affected company, the equipment operator or a national cyber agency. **40%, unlikely.**

VI. GAPS AND UNVERIFIED

- **Refrigeration attack:** the vendor and model are not officially confirmed, and Danfoss's comment comes via NOS as reported by the BBC. Exact store counts in Finland, Estonia and the Netherlands vary by outlet. The link to the October French attack is the operator's belief.
- **Alert apps:** the hacker-group claims, including Hitcore's claimed access method, are unverified.
- **UNM:** the Byod leak-site claim is unverified.
- **gpsjam:** cells were counted by the desk from the raw daily file (>10% bad aircraft, rough lat/lon boxes). This is not an official bulletin.
- **AIID:** the incidentdatabase.ai API refused the request, and the list page shows no recent entries, so it was not checked. The ransomware.live count for 2–3 Nov is partial.

Sources

BBC; Euronews; University Hospitals; BleepingComputer; NCSC; Guardian; The Record; Radio Moldova; RFE/RL; CISA KEV, directives and advisories; SEC EDGAR; ransomware.live; gpsjam.org; EASA; Federal Register; Pingoru; TSMC; Nami Tech Solutions; MOFCOM.