WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Saturday, 21 November 2026 | Vol. 2026-325 | As of 210730 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend ↑, as the cyber picture worsens while the chip front pauses. Broadcom patched VMware vCenter flaw CVE-2026-123890 on 19 Nov. Google's threat intelligence group says a China-linked espionage group exploited it as a zero-day for at least two months. CISA added the flaw to the KEV catalog on 20 Nov and gave federal agencies until 23 Nov to fix it. Monadnock Community Hospital is still on ambulance diversion and has cancelled lab, radiology and some surgeries through 30 Nov. Ransomware.live counts 367 leak-site victims for 16–21 Nov, 36% above the 8-week mean. On chips, the BIS remote-access rule is in force and no MOFCOM countermeasure has been named. The No. 72 gallium pause still lapses on 27 Nov, with no extension published. No calls are due today. New calls: TEC-55 and TEC-56.

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: Monadnock on diversion, day 13, cancellations to 30 Nov; vCenter zero-day KEV add; K-4: 367 victims	↑
TEC-T2 Semiconductors and compute	ENVIRONMENT FOR CRISIS	SIGNIFICANT	X-1: BIS rule in force; foundry pauses reported; X-2: No. 72 lapses 27 Nov, MOFCOM threat unnamed	=
TEC-T4 AI governance and incidents	ENVIRONMENT FOR CRISIS	SIGNIFICANT	AI-3 carried (CoreWeave 15 Nov); no new major outage	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-2: Gulf of Finland GNSS interference 16–17% of area-hours; no new attributed sabotage	=

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

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

Change line. No topic changes level. The trend driver moves from TEC-T2 to TEC-T1, so the family trend stays ↑.

Moved indicators (vs 20 November). No indicator changed its score. K-1 rose from 5 to 9 additions for 16–22 Nov and stays ROUTINE, one short of the ABNORMAL band. K-4 rose from 324 to 367 victims and stays ABNORMAL. The week is now 36% above the mean, outside the ±25% routine band.

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

Facts. CISA added four KEV entries on 20 Nov: SAP NetWeaver CVE-2025-42884, Cisco Expressway CVE-2026-76466, VMware vCenter CVE-2026-123890 and Apache Roller CVE-2026-129448 (CISA). The catalog is now at version 2026.11.20 with 1,790 entries. The 16–22 Nov count is 9 (KEV feed). The vCenter entry is due on 23 Nov, and forensic triage is required under BOD 26-04 (CISA KEV). Broadcom's VMSA-2026-0009 rates the flaw CVSS 9.8. It allows unauthenticated administrator access, and Broadcom offers no workaround (Rapid7). Google Threat Intelligence Group says Armory Castle (UNC5221), a China-linked espionage group, has exploited the flaw for at least two months. GTIG says a small number of organisations are confirmed compromised (Cybersecurity Dive). Canada's Cyber Centre updated advisory AV26-1185 on 20 Nov (CCCS). CISA's directives page lists no new Emergency Directive; the latest is ED 26-03 (CISA directives). Monadnock Community Hospital's update of 20 Nov says the incident is a confirmed cyber incident and that federal law enforcement is investigating. The hospital remains on ambulance diversion and has cancelled laboratory visits, radiology visits and some major elective surgeries through 30 Nov (MCH; Ledger-Transcript). Ransomware.live counts 109, 59, 69, 74 and 49 victims for 16–20 Nov and 7 so far on 21 Nov (UTC), for a total of 367. The 8-week mean is 269.5 (feed). EDGAR full-text search found no 8-K filed 18–21 Nov that cites Item 1.05 (EDGAR FTS).
Indicators. K-1 ROUTINE (9); K-2 ABNORMAL (carried; the vCenter attribution is a vendor attribution, not an official joint advisory); K-3 SIGNIFICANT (Monadnock, day 13); K-4 ABNORMAL (+36%); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** The vCenter campaign matters because vCenter controls entire virtualised estates. A three-day deadline and a forensic-triage flag show how seriously CISA rates it. An Emergency Directive or a formal attribution by a US agency would raise K-2 (logged TEC-55: 35%). TEC-44 (≥ 330) is effectively met at 367, but it is formally scored on 24 Nov. TEC-43 (≥ 10) needs one more addition on a weekend, so a miss is likely. TEC-52 (Monadnock ends diversion by 25 Nov) now looks unlikely, at roughly 10%.

II. TEC-T2 SEMICONDUCTORS AND COMPUTE | ENVIRONMENT FOR CRISIS

Facts. The BIS rule (FR Doc. 2026-23529, 91 FR 74970) has been in force since 19 Nov (Federal Register). Since then, BIS has published only a paperwork notice, and no other rule (FR API). TSMC told Reuters it "will comply" with the rule. Two people told Reuters that TSMC halted affected orders at 16 nm and below for Chinese designers unless they hold licences (Reuters via Investing.com). Seoul Economic Daily repeats the report that Samsung halted AI chip shipments to Chinese customers (SEDaily). MOFCOM's 17 Nov statement says China "will take countermeasures" but names none (Global Times). Trackers checked on 20 Nov found no MOFCOM notice extending No. 72, which suspends the US-specific gallium, germanium and antimony ban until 27 Nov (APE-M; MOFCOM No. 72). **Indicators.** X-1 SIGNIFICANT; X-2 ABNORMAL; X-3 ROUTINE (carried); X-4 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend = (no new action today). **Analyst Comment.** With 6 days left, a lapse of No. 72 without a notice is becoming more plausible. Beijing could let the rule lapse rather than announce a new countermeasure.

III. TEC-T4 AI GOVERNANCE AND INCIDENTS | ENVIRONMENT FOR CRISIS

Facts. The Federal Register shows no new AI-specific federal action on 20–23 Nov (FR API). No new EU AI Act milestone was found. The AI Omnibus, Regulation (EU) 2026/1744, has been in force since 27 July (Council). **Indicators.** AI-1 ABNORMAL (carried); AI-2 ABNORMAL; AI-3 SIGNIFICANT (carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =.

IV. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | NO CRISIS

Facts. No new attributed ground-station or cable sabotage was found. GNSS interference over the Gulf of Finland and Estonia was 16% of area-hours on 19 Nov and 17% on 20 Nov (NAVWAR monitor). **Indicators.** O-1/O-2/O-3 ABNORMAL (carried). **Override −1 to NO CRISIS (held):** the only sabotage event in the 30-day window failed. Trend =.

V. PREDICTIONS

Resolved: none (no TEC call due 21 Nov). **Pending:** TEC-43 (9 of 10; resolves 23 Nov; likely miss). TEC-44 (367 of 330; resolves 24 Nov; very likely hit). TEC-52 (Monadnock; by 25 Nov; unlikely). TEC-09 (No. 72; 27 Nov). TEC-07 (Emergency Directive; 30 Nov). TEC-51 (MOFCOM countermeasure; 18 Dec). **New:** - **TEC-55:** CISA, FBI or NSA officially attributes exploitation of CVE-2026-123890 to a PRC state-sponsored or state-linked actor by 31 Dec 2026. **35%, unlikely.** - **TEC-56:** Samsung Electronics confirms on the record that it paused shipments or orders for Chinese customers because of the BIS rule, by 15 Dec 2026. **25%, unlikely.**

VI. GAPS AND UNVERIFIED

- The vCenter attribution and victim count come from GTIG and Mandiant, which are vendors. No US government attribution has been made.
- The TSMC order halt rests on Reuters sources. The Samsung pause rests on the FT and Seoul Economic Daily; Samsung declined to comment.
- The 21 Nov GNSS reading (71%) covers only 35 area-hours and is not scored.
- A third-party status aggregator reports a 19 Nov partial OpenAI API incident. It was not confirmed on the provider's page.
- Monadnock: the attacker and any data impact are unconfirmed.

Sources

CISA; CISA KEV; Rapid7; Cybersecurity Dive; Canadian Centre for Cyber Security; Monadnock Community Hospital; Monadnock Ledger-Transcript; ransomware.live; SEC EDGAR; Federal Register; Reuters (Investing.com); Seoul Economic Daily; Global Times; APE-M; MOFCOM; Council of the EU; NAVWAR RFI monitor.