# WIRE Technology & Cyber

**UNCLASSIFIED // OPEN SOURCE | Sunday, 1 November 2026 | Vol. 2026-305 | As of 010730 EST NOV 26**

**BLUF.** The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS**, trend **=** after yesterday's turn up. Moldova's officials say attackers pulled data on about 750,000 people from government digital services between 19 and 23 Oct, forcing 82 services offline, and the prime minister points to foreign state actors without naming one. Russia's statistics service, Rosstat, says it took "targeted destructive cyberattacks" from 29 Oct to 1 Nov with no data compromise. University Hospitals in Cleveland still has no restoration date for MyChart. CISA published nothing new over the weekend; the KEV catalog stays at 1,766. Ransomware leak-site postings reached 268 for 26 Oct to 1 Nov, close to the TEC-08 bar, which resolves on Monday. Chips and AI governance stay at **NO CRISIS**, and MOFCOM No. 70 still ends on 10 Nov. TEC-21 is 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: University Hospitals MyChart and e-prescribing still down; Moldova state services breach | = |
| **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 information requests, no finding | = |
| **TEC-T2 Semiconductors and compute** | NO CRISIS | ABNORMAL | X-1: MOFCOM No. 70 end date 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 = (no new KEV entries or directives over the weekend). Family trend ↑ to =.

**Moved indicators (vs 31 Oct).** None changed score. K-4 stays ROUTINE, but the week count rose from 253 to 268, or 117% of the 8-week mean.

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

**Facts.** Moldova's Electronic Government Agency says attempts to extract data tied to personal identification numbers ran from 19 to 23 Oct and targeted about one million people. Authorities suspended 82 digital public services and disconnected more than 30 information systems, and say bank card data was not affected (RFE/RL, 29 Oct). Moldova's state IT and cybersecurity service, STISC, estimates data on around 750,000 people may have been extracted (Moldpres). The prime minister cited "indications of a broader campaign involving foreign state actors" without naming a country, and the national Cybersecurity Agency head called attribution "premature" (RFE/RL). Rosstat says it recorded "targeted destructive cyberattacks" on its information resources from 29 Oct to 1 Nov, found no database compromise or leak, and is restoring public access to its website (Interfax, 1 Nov). University Hospitals told ISMG on 30 Oct it has no clear estimate for when systems, including MyChart, will return, and did not say whether ransomware was involved (BankInfoSecurity); its incident page still says MyChart remains offline (UH). The KEV catalog is unchanged at version 2026.10.30 with 1,766 entries; CVE-2026-111357 (Ivanti) is due for federal agencies on 2 Nov and CVE-2026-118527 on 13 Nov (KEV JSON). The directives page lists no new emergency directive (CISA directives). Volexity still assesses with low confidence that the Ivanti actor, UTA0576, is criminally rather than espionage-motivated (Volexity). Ransomware.live counts 268 victims discovered 26 Oct to 1 Nov (UTC) so far, including 84 on 31 Oct, 50 of them from one group (feed).
**Indicators.** K-1: ABNORMAL (10 in week of 26 Oct, carried). K-2: ABNORMAL (carried). K-3: SIGNIFICANT (UH). K-4: ROUTINE (117% of mean). K-5: ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** Moldova's own cyber agency calls this its largest recorded cyberattack, and it fits a pattern of pressure on a small state bordering the war, but no official attribution exists yet, so it is not scored as a state attack. Volexity's low-confidence criminal read on the Ivanti actor makes TEC-19 slightly less likely than when it was made. TEC-08 needs about 288 postings by the end of 1 Nov UTC; with 268 logged and the bulk dump done, it is now roughly even that it hits.

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

**Facts.** No new ground-station or cable attack was found. Coverage on 31 Oct restates that Lithuanian police link the Lithuanian, Polish and Bulgarian Starlink attacks to one group (Space Security News, 31 Oct). **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.** No new Commission AI Act decision, finding or penalty was found; the AI Office's information requests on "loss of control" incidents remain at the investigation stage with no infringement established (2eu.brussels). Moldova's Cybersecurity Agency head said he believes AI tools were used to find vulnerabilities in the attack (RFE/RL). **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's No. 70 notice still suspends the October 2025 export-control package only "until 10 November 2026" (MOFCOM No. 70); MOFCOM's 28 Sep statement extending the wider Kuala Lumpur arrangement to 10 Jan 2027 named neither No. 70 nor No. 72 (Materials Dispatch, 27 Oct). No new BIS chip rule was found. **Indicators.** X-1: ABNORMAL. X-2 to X-4: ROUTINE. Roll-up: NO CRISIS (=).

## V. PREDICTIONS

**Resolved:** none. TEC-08 checks on 2 Nov (268 so far, about 288 needed). TEC-02 open, 9 days to the No. 70 end date. TEC-05/06/07/11/12/13/19/20 open. New (logged in the prediction ledger): - **TEC-21:** The Moldovan government (president, prime minister, SIS, Cybersecurity Agency or prosecutors) publicly names Russia or a Russian state body as responsible or likely responsible for the 19–23 Oct attack on state digital services by 30 Nov 2026. **50%, roughly even chance.**

## VI. GAPS AND UNVERIFIED

- **Moldova:** the STISC estimate was read from the Moldpres headline; the full Moldpres text was not readable from the box, so details come from RFE/RL quoting officials. Which services remain offline is not public.
- **Rosstat:** the attack vector and any claimed perpetrator are not public; the statement was read via Interfax.
- **Leak-site claims** in the 31 Oct bulk posting are unconfirmed and not named here.
- **TSMC IR, gpsjam.org, AIID and EDGAR full-text search** not queried today (weekend); TSMC's October revenue is due about 10 Nov.

## Sources

RFE/RL; Moldpres; Interfax; BankInfoSecurity; University Hospitals; CISA (KEV, directives); Volexity; ransomware.live; Space Security News; 2eu.brussels; MOFCOM; Materials Dispatch.