

Critical Incidents, Infrastructure and Resilience Signals in 2026

January–October 2026 Overview

206 critical incidents or major signals recorded since January 2026.

Cyberattacks, energy, telecommunications, subsea cables, GNSS, transport and strategic flows.

Growing focus on civil and military preparedness and the continuity of essential services.

JANUARY 2026

Date	Country / area	Category	Event
Jan. 2	Lithuania / Latvia	Telecommunications / cables	Subsea telecommunications cable damaged in the Baltic Sea.
Jan. 2	Republic of the Congo	Internet / cables	WACS subsea cable rupture; Internet traffic fell by up to approximately 82%.
Jan. 3	Germany	Energy / sabotage	Sabotage of Berlin's power grid; nearly 100,000 people left without electricity and heating.
Jan. 4	Greece	Air transport	Major aviation communications outage; airspace disrupted for several hours.
Jan. 8	Iran	Internet	Nationwide Internet blackout.
Jan. 8	International	Cyber / AI	Massive reconnaissance of exposed AI infrastructure; more than 91,000 sessions detected.
Jan. 8	Europe / Croatia	Energy / power grid	European grid incident; frequency dropped to 49.8 Hz and automatic protection systems were triggered.
Jan. 8	France	Military / resilience	ORION 26 presented as a high-intensity exercise incorporating degraded environments and national resilience.
January	Lithuania / Baltic	GPS / aviation	Significant GPS jamming and spoofing activity; 169 incidents reported by pilots during the month.
Jan. 12	France	Military / counter-drone	Counter-drone capabilities described as an "operational emergency" amid the growing threat.
Jan. 13	Poland	Energy / cyber	Destructive cyberattack against several energy infrastructure facilities disclosed.

Date	Country / area	Category	Event
Jan. 14	United States	Telecommunications	Nationwide Verizon mobile network outage.
Jan. 15	Europe / NATO	Military / preparedness	Steadfast Dart 2026 begins; 10,000 troops from 11 countries and first Allied Reaction Force deployment.
Jan. 21	International	Cyber	Critical Cisco vulnerability actively exploited.
Jan. 26	International	Internet / network	BGP incident at Cloudflare causes network disruptions worldwide.
Jan. 26	International	Cyber	Microsoft Office zero-day vulnerability actively exploited.
Jan. 26	United States	Military / resilience	Citadel Shield-Solid Curtain 2026 begins, testing protection of US Navy installations.
Jan. 27	Switzerland / Europe	Air transport / infrastructure	IT failure at Geneva air traffic control; airspace temporarily closed and flights diverted.
Jan. 29	International	Cyber	Critical Ivanti vulnerabilities; active exploitation reported.
Jan. 29	France	Civil preparedness / resilience	"Tous responsables" guide released to prepare the population for major crises and service disruptions.
Jan. 31	Ukraine / Moldova	Energy / power grid	Major grid incident; widespread outages and temporary separation from the Continental European power system.

January 2026 overview

- 21 critical incidents or major signals recorded
- 13 countries or geographic groupings directly affected, in addition to incidents with international scope
- 7 events directly related to cybersecurity
- 5 events affecting the Internet, telecommunications, cables or GPS navigation
- 4 events directly related to energy or power grids
- 4 events related to preparedness, resilience or military posture
- 2 major events affecting air transport
- 2 incidents directly involving subsea cables
- 2 events related to civil preparedness or resilience
- 1 significant GPS jamming/spoofing signal in the Baltic region
- 1 major physical sabotage incident targeting power infrastructure
- Several events resulting in direct physical or operational consequences for populations, transport systems or infrastructure

January is characterized by a concentration of signals affecting several essential infrastructures: power grids, telecommunications, subsea cables, the Internet and air transport. This operational dimension is accompanied by sustained cyber activity, GPS disruptions in the Baltic region and several civil or

military preparedness measures, making network resilience and the continuity of essential services a significant issue from the very beginning of the year.

FEBRUARY 2026

Date	Country / area	Category	Event
Feb. 1	Taiwan / Asia	Subsea cables	Major Trans-Pacific Express cable rupture affecting connections around Taiwan.
Feb. 3	Ukraine / Slovakia / Romania	Cyber / espionage	APT28 exploits a Microsoft Office vulnerability against several European targets.
Early Feb.	International	Cyber / supply chain / AI	Supply-chain attacks targeting the AI assistant ecosystem.
Feb. 5	Romania	Energy / cyber	Cyberattack against Conpet, the national oil pipeline operator.
Feb. 5	European Union	Cables / resilience	"Cable Security Toolbox" published to strengthen the protection of subsea cables.
Feb. 6	Europe	Cyber / espionage	Campaign targets Signal users, including political, military and media figures.
February	Lithuania / Baltic	GPS / aviation	Persistent GPS jamming; 118 incidents reported by pilots during the month.
Feb. 9-10	Grenada	Internet	Internet connectivity nearly disappears for approximately 12 hours.
Feb. 9-26	Norway / Arctic	Military / resilience	Heimdall 26 tests military and technological capabilities in Arctic and degraded environments.
Feb. 12	Netherlands	Telecommunications / cyber	Odido telecom operator hacked; more than 6 million accounts affected.
Feb. 13-26	Hungary / Slovakia / Ukraine	Energy / oil	Druzhba pipeline deliveries interrupted; emergency measures and alternative supplies activated.
Feb. 18	Germany	Transport / cyber	Cyberattack against Deutsche Bahn disrupts ticketing and passenger information systems.
Feb. 19	France	Data / cyber	FICOBA compromised; approximately 1.2 million bank accounts affected.
Feb. 19	Slovakia	Energy / reserves	Oil emergency declared and strategic stocks released following the Druzhba disruption.

Date	Country / area	Category	Event
Feb. 20	Germany / NATO	Military / resilience	Quadriga 2026 tests rapid force deployment under conditions close to a real-world scenario.
Feb. 20	Baltic / NATO	Military / counter-drone	NATO counter-drone mission over the Baltic and integrated air-defense test.
Feb. 21	Russia / Belarus	Military / cyber	Compromise claimed against systems used by Russian drone operators.
Feb. 24	United States	Cyber / national security	Sanctions imposed on a network accused of trafficking sensitive cyber tools.
Feb. 25	Taiwan	Subsea cables	Major rupture of the TPKM3 cable connecting Taiwan with its outlying islands.
February	Germany / Lithuania	Military / medical	Medic Quadriga tests strategic medical evacuation and a civil-military treatment hub.

February 2026 overview

- 20 critical incidents or major signals recorded
- 15 countries or geographic groupings affected, in addition to incidents with international scope
- 9 events directly related to cybersecurity
- 6 events related to military activity, espionage or national security
- 4 events related to energy, oil or energy resilience
- 3 events affecting the Internet, telecommunications or subsea cables
- 2 major subsea cable ruptures around Taiwan
- 2 events related to strategic reserves or continuity of energy supplies
- 1 persistent GPS jamming signal in the Baltic region
- 1 event directly affecting transport
- 2 large-scale data or account compromises

February remains marked by intense cyber activity, but several signals directly concern strategic infrastructure and interests. Disruptions to the Druzhba pipeline and the release of strategic oil reserves, subsea cable ruptures around Taiwan and persistent GPS jamming in the Baltic region coincide with several military exercises focused on resilience, rapid deployment and continuity of operations.

MARCH 2026

Date	Country / area	Category	Event
Mar. 1	Gulf / Strait of Hormuz	Maritime / strategic flows	Maritime traffic collapses in Hormuz; tanker traffic nearly comes to a halt.
Mar. 1	Persian Gulf	GPS / maritime	Massive GNSS jamming and spoofing disrupts maritime navigation across the Gulf.

Date	Country / area	Category	Event
Mar. 1	Red Sea / Middle East	Maritime / logistics	Several carriers suspend Hormuz and some Suez/Bab-el-Mandeb routes; vessels rerouted.
Mar. 2	Iran	Internet	New nationwide blackout; connectivity falls to around 1% for more than 48 hours.
Mar. 3	International	Cyber	Critical VMware vulnerability actively exploited.
Mar. 3	United Kingdom / Netherlands	Subsea cables	Circe North cable ruptures; traffic rerouted through Paris.
Mar. 4	Cuba	Energy / blackout	Blackout affects most of the country after the Antonio Guiteras power plant shuts down.
Mar. 4	Iraq	Energy / blackout	National power grid collapses following a sudden drop in gas supplies.
Mar. 9-19	Norway / Finland / NATO	Military / preparedness	Cold Response 2026; major northern-flank exercise involving forces from 14 allied countries.
Mar. 10	Albania	Institution / cyber	Cyberattack against Parliament disrupts email and internal systems.
Mar. 11	United States / International	Healthcare / cyber	Destructive cyberattack against Stryker disrupts global operations.
Mar. 12	Poland	Nuclear / cyber	Cyberattack against the National Centre for Nuclear Research.
Mar. 15	Republic of the Congo	Internet	Nationwide near-blackout of Internet connectivity for around 60 hours during the presidential election.
Mar. 16	Costa Rica	Energy / telecoms / cyber	Intrusion at the national electricity and telecommunications operator.
Mar. 17	EU / Hungary / Slovakia	Energy / oil	Druzhba remains disrupted; EU intervenes to secure alternative supplies.
Mar. 19-24	European Union	Institution / supply chain	European Commission cloud compromised; approximately 91.7 GB of data exfiltrated.
Mar. 20	International	Cyber / supply chain	Trivy open-source security tool compromised.
Mar. 23-27	Netherlands / Germany	Institution / cyber	Cyberattacks target government, police and political infrastructure.
Mar. 24	International	Cyber / supply chain / AI	LiteLLM compromised; approximately 500,000 devices potentially affected.
Mar. 25	Spain	Transport / cyber	Cyberattack against the Port of Vigo disrupts IT systems and operations.

Date	Country / area	Category	Event
Mar. 25-26	Europe	GPS / aviation	EASA and Eurocontrol launch a European plan in response to rising GNSS interference.
Mar. 26	International	Telecoms / espionage	Long-running espionage campaign targets global telecommunications infrastructure.
Mar. 26	International	Cyber / AI	Critical Langflow vulnerability exploited less than 24 hours after disclosure.

March 2026 overview

- 23 critical incidents or major signals recorded
- 18 countries or geographic groupings affected, in addition to incidents with international scope
- 12 events directly related to cybersecurity
- 5 events related to energy, oil or power grids
- 4 events affecting the Internet, telecommunications, cables or GNSS
- 4 events targeting public, political or strategic institutions
- 3 events related to maritime flows or strategic logistics
- 3 software supply-chain attacks
- 2 major power blackouts
- 2 nationwide Internet blackouts or near-blackouts
- 2 major signals related to GNSS jamming or resilience
- 1 subsea cable rupture
- 1 event targeting the nuclear sector
- 1 event affecting port infrastructure
- 1 destructive cyberattack against the healthcare sector
- 1 major NATO northern-flank preparedness exercise

March stands out for the simultaneous disruption of several strategic systems. Sustained cyber activity coincides with the collapse of traffic through the Strait of Hormuz, disruptions to maritime flows, massive GNSS jamming, two nationwide power blackouts and two Internet blackouts or near-blackouts. Energy, communications, navigation and transport are therefore affected within the same month, while pressure on oil supplies persists.

APRIL 2026

Date	Country / area	Category	Event
Apr. 1	United States	Institution / cyberespionage	Chinese intrusion into a sensitive FBI system; incident classified as major.
April	Strait of Hormuz	Maritime / strategic flows	Traffic remains extremely low; around 7 daily transits versus more than 80 before the crisis.
Early Apr.	Middle East / International	Energy / oil	Oil flows through Hormuz fall to ~3.8 Mb/d versus more than 20 Mb/d in February; alternative routes activated.

Date	Country / area	Category	Event
Apr. 5	International	Cyber / network	Critical Fortinet vulnerability actively exploited; emergency security patch released.
Apr. 6	Norway / Finland	GPS / aviation	GPS spoofing disrupts a Finnair approach to Kirkenes; a new approach is required.
Apr. 7	United States	Energy / water / cyber	Iran-attributed cyber activity targets industrial controllers used in critical infrastructure.
Apr. 7	International	Cyber / AI	Critical vulnerabilities affecting the Flowise AI platform actively exploited.
Apr. 7	International	Cyber / supply chain	North Korean supply-chain campaign linked to more than 1,700 malicious packages.
Apr. 8	International	Network / cyberespionage	APT28 compromises thousands of routers; more than 200 organizations and 5,000 devices affected.
Apr. 12	Italy	Water / infrastructure / cyber	Hackers claim control of the pumping system protecting Venice from flooding.
Apr. 13	Gulf / Iran	Maritime / security	US blockade imposed on vessels entering or leaving Iranian ports.
Apr. 14	France	Institution / cyber	Cyberattack against the Ministry of Education; student data stolen.
Apr. 15	International	Cyber	Microsoft SharePoint vulnerability actively exploited.
Apr. 15-16	International	Internet / DDoS	Major DDoS attack against Bluesky disrupts services and APIs.
Apr. 16	France	Military / cyberespionage	Russia-attributed reconnaissance targets communications linked to nuclear deterrence.
Apr. 20	France	Institution / data	Security incident at ANTS; personal data potentially compromised.
Apr. 21	Finland	State / cyberespionage	Government mobile-device management system targeted; around 50,000 users affected.
Apr. 21	Venezuela	Energy / cyber	Destructive cyber campaign against energy infrastructure and public utilities disclosed.
Apr. 21	Finland	GPS / telecommunications	Sharp rise in GNSS and mobile interference; disruptions observed daily.
Apr. 22	International	Cyber / supply chain	npm worm capable of stealing tokens and automatically propagating.

Date	Country / area	Category	Event
Apr. 23	International	Network / cyber	Campaign targets Cisco Firepower equipment and deploys a backdoor.
Apr. 24	Strait of Hormuz	Maritime / security	IMO considers transit unsafe; vessels seized and around 20,000 seafarers stranded in the Gulf.
Apr. 27	Sweden / NATO	Military / preparedness	Aurora 26 begins; more than 16,000 troops train for reinforcement of the eastern flank.
Apr. 30	European Union	Energy / resilience	EU prepares measures involving oil stocks if the Hormuz closure extends beyond May.

April 2026 overview

- 24 critical incidents or major signals recorded
- 13 countries or geographic groupings affected, in addition to incidents with international scope
- 16 events directly related to cybersecurity
- 6 events related to energy, water or critical infrastructure
- 5 events directly targeting state, government or military institutions
- 4 events related to maritime flows, Hormuz or navigation security
- 4 events directly targeting network equipment or infrastructure
- 3 events related to oil, energy or security of supply
- 2 major software supply-chain attacks
- 2 events related to GNSS jamming or resilience
- 2 events related to strategic preparedness or resilience
- 2 events directly related to nuclear issues or deterrence
- 1 major disruption affecting an international Internet service

April remains marked by intense cyber activity targeting particularly sensitive systems: public institutions, networks, energy, water and strategic communications. At the same time, the Hormuz crisis continues, with maritime traffic remaining extremely low, oil flows sharply reduced and navigation security deteriorating. GNSS disruptions also persist, while energy and military resilience measures become increasingly prominent.

MAY 2026

Date	Country / area	Category	Event
May	Strait of Hormuz	Maritime / strategic flows	Traffic falls to ~3.9 transits/day, versus 7.1 in April and nearly 85 before the crisis.
May 4	Austria	Espionage / communications	Three Russian diplomats expelled over suspected espionage targeting satellite communications.
May 4	Strait of Hormuz / United States	Maritime / security	US military escorts of vessels through Hormuz begin under "Project Freedom".

Date	Country / area	Category	Event
May 5	International	Cyber / supply chain	Daemon Tools compromised; official installers trojanized and thousands of infection attempts detected.
May 5-13	NATO / Europe / United States	Military / preparedness	Steadfast Deterrence 2026; collective-defense exercise involving all 32 NATO countries.
May 6	International	Cyber / network	Critical PAN-OS vulnerability enables root code execution; active exploitation reported.
May 6	International	Cyber / AI / supply chain	OpenClaw component compromised; developer environments and services exposed.
May 7	European Union	Energy / resilience	EU prepares coordinated response and possible use of reserves amid risks to jet-fuel supplies.
May 11	International	Cyber / supply chain	Shai-Hulud attack compromises more than 160 npm and PyPI packages.
May 11-22	Netherlands / NATO	Military / counter-drone	NATO exercise tests more than 60 drone detection and neutralization systems.
May 12	International / Israel / Iran	Cyber / supply chain / AI	mistralai Python package compromised with destructive function targeting Israel and Iran.
May 14	International	Cyber / network	Cisco Catalyst SD-WAN vulnerabilities allow privilege escalation.
May 19	United States / International	Cyber / supply chain	Around 3,800 private GitHub repositories compromised after installation of a malicious extension.
May 20	International	Cyber / cloud	Microsoft 365 and Azure accounts compromised; large-scale data exfiltration reported.
May 24	European Union / Spain	Military / preparedness	LIVEX26 begins; rapid deployment capability tested with 2,500 troops from 13 countries.
May 26	Lithuania	Institution / data	More than 600,000 national registry entries leaked; possible state involvement.
May 26	Iran	Internet	Internet restoration begins after approximately 88 days of blackout.
May 26	International	Cyber / botnet	Glassworm dismantled after compromises involving VS Code, npm, PyPI and GitHub.
May 26	Baltic / Estonia	GPS / aviation	Persistent GPS interference; aviation and defense prepare for degraded navigation conditions.

Date	Country / area	Category	Event
May 28	European Union	Energy / resilience	EU strengthens oil and gas monitoring as the Hormuz crisis continues to pressure the jet-fuel market.

May 2026 overview

- 20 critical incidents or major signals recorded
- 13 countries or geographic groupings affected, in addition to incidents with international scope
- 10 events directly related to cybersecurity
- 5 events related to software supply chains
- 4 events related to military activity, preparedness or strategic security
- 3 events related to energy, oil or energy resilience
- 2 events directly related to Hormuz and the security of maritime flows
- 3 events directly affecting network or cloud equipment, services or infrastructure
- 2 events related to the AI ecosystem
- 2 events involving espionage or possible state involvement
- 2 events related to GPS interference or satellite communications
- 1 large-scale compromise of national registry data
- 1 nationwide Internet blackout beginning to end after approximately 88 days

May remains marked by intense cyber activity, particularly through software supply chains and trusted components. At the same time, traffic through Hormuz remains extremely low, leading to military escorts and European preparations concerning energy supplies. GPS interference persists in the Baltic region, while several military exercises focus on collective defense, rapid deployment and counter-drone capabilities.

JUNE 2026

Date	Country / area	Category	Event
Jun. 2	Estonia	Institution / DDoS	Attack against national CERT name servers; disruptions affect the government network.
Jun. 2	Norway / Denmark	Energy / subsea cable	Skagerrak 2 outage; electricity interconnection capacity reduced by 245 MW for several months.
Jun. 4	International	Network / cyberespionage	Chinese campaign targets network equipment to gain persistent access to Microsoft 365.
Jun. 4-5	France / Germany / Luxembourg	Nuclear / preparedness	Cattenom 2026 simulates a nuclear accident and activates crisis-response structures.
Jun. 8	France	Institution / communications	Tchap, the encrypted messaging service used by the French government, compromised.
Jun. 8	International	Cyber	New Chrome zero-day actively exploited; emergency update released by Google.

Date	Country / area	Category	Event
Jun. 8	Latvia / NATO	Military / counter-drone	French Rafale jets intercept and destroy an unauthorized drone in Latvian airspace.
Jun. 8-20	Estonia / NATO	Military / resilience	Vigorous Warrior 2026; major medical exercise involving 38 countries and civil-military cooperation.
Jun. 10	International	Cyber	Microsoft Exchange zero-day actively exploited against Outlook Web Access.
Jun. 10	United States / China	Espionage / security	13 domains linked to Chinese intelligence-gathering operations seized.
Jun. 14	Council of Europe	Institution / data	Nearly 300 GB data leak claimed; up to 10,000 staff members potentially affected.
Jun. 15	International	Cyber / network	More than one billion login attempts target FortiGate and MSSQL systems.
Jun. 15	Estonia	Institution / cloud	Government cloud outage leaves several national public services unavailable.
Jun. 16-17	Estonia	Telecoms / energy	Telecom outage follows a power cut; calls and Mobile-ID services disrupted.
Jun. 18	International	Cyber	Operation against SocGhosh addresses nearly 15,000 infected sites and neutralizes 106 infrastructure nodes.
Jun. 19	Belgium	Intelligence / cyber	Belgian intelligence services compromised through Ivanti vulnerabilities.
Jun. 22	Estonia	Digital infrastructure	X-tee service outage affects government agencies, a hospital and banks.
Jun. 23	International	Cyber / communications	Cisco Unified Communications Manager vulnerability actively exploited.
Jun. 23	European Union	Cables / resilience	Regional hubs created and €40 million allocated to strengthen subsea cable repair capabilities.
Jun. 23-26	Strait of Hormuz	Maritime / strategic flows	Maritime evacuation corridor; 136 vessels and around 2,900 seafarers evacuated from the Gulf.
Jun. 25-26	Strait of Hormuz	Maritime / security	Partial traffic recovery interrupted by a new attack on a vessel near Oman.
Jun. 26	International	Cyberespionage / communications	FBI warns of a Russian campaign targeting Signal recovery keys.
Jun. 26	European Union	Energy / resilience	Oil flows gradually recover, supported by IEA emergency stocks.

June 2026 overview

- 23 critical incidents or major signals recorded
- 15 countries or geographic groupings affected, in addition to incidents with international scope
- 11 events directly related to cybersecurity
- 7 events affecting public, government or intelligence institutions
- 6 events related to networks, telecommunications or communication systems
- 4 events related to espionage, intelligence or operations attributed to state actors
- 4 events related to energy, physical infrastructure or resilience
- 3 events related to military, civil or strategic preparedness
- 3 major incidents directly affecting Estonia's digital infrastructure
- 2 events related to maritime flows or security in the Strait of Hormuz
- 2 actively exploited zero-day vulnerabilities
- 2 events directly related to subsea cables or interconnections
- 1 cross-border nuclear accident preparedness exercise
- 1 real-world interception and destruction of a drone in Baltic airspace
- 1 outage combining a power cut and telecommunications disruption

June brings together several incidents directly affecting state systems and essential infrastructure: government communications, intelligence services, public cloud infrastructure, telecommunications and digital services. This activity coincides with events affecting electrical interconnections and subsea cables, while military and nuclear preparedness intensifies. In Hormuz, an attempt to restore traffic and evacuate vessels is quickly undermined by a new attack, maintaining uncertainty along this strategic route.

JULY 2026

Date	Country / area	Category	Event
Jul. 1	International	Cyber / AI	Attack using an AI agent encrypts and destroys data across IT infrastructure.
Jul. 3	Europe	GPS / aviation	EASA strengthens measures against GNSS jamming and spoofing affecting aviation.
Jul. 5	Ukraine / Sevastopol	Energy / Internet	Major power outage; Internet traffic falls by up to 98% for around 8 hours.
Jul. 7	Strait of Hormuz	Maritime / security	Several merchant vessels attacked; threat level raised to "severe" and traffic sharply reduced.
Jul. 8	France	Resilience / preparedness	Vital supplies prioritized and preparations begin for a major power-blackout exercise.
Jul. 9	Latvia	Institution / ransomware	State forestry company attacked; services disrupted and 44 GB of data stolen.
Jul. 9	International	Cyber	Campaign targets more than 1.4 million WordPress domains and Java services.

Date	Country / area	Category	Event
Jul. 9	International	Cyber / ransomware	CitrixBleed 2 exploited to bypass authentication and deploy ransomware.
Jul. 10	European Union	Critical infrastructure	Recommendations strengthened against drones, hybrid threats and cross-border disruptions.
Jul. 12	Strait of Hormuz	Maritime / strategic flows	Traffic drops again after attacks; only 11 vessels transit the strait during the day.
Jul. 14	International	Cyber / supply chain	AsyncAPI npm packages used in development environments compromised.
Jul. 14	International	Cyber / network	Two SonicWall zero-days actively exploited against exposed network equipment.
Jul. 16	International	Cyber / network	Critical Fortinet vulnerabilities actively exploited.
Jul. 16	International	Cyber / AI	Autonomous AI agent compromises Hugging Face production infrastructure.
Jul. 20	Romania	Institution / destructive cyber	Attack on land registry erases systems and backups, disrupting property transactions.
Jul. 20-23	International	Cyber	Critical Microsoft SharePoint vulnerabilities actively exploited.
Jul. 21	International	Cyber / AI / cloud	Langflow vulnerability exploited for code execution and theft of cloud credentials.
Jul. 29	United Kingdom	Institution / data	Ministry of Education breached; more than 600,000 records compromised.
Jul. 30	International	Cyber / AI	Multiple autonomous AI agents gain unauthorized access to real-world production systems.
Jul. 31	Argentina	Energy / cyber	Cyberattack against Oldelval oil pipeline operator affects administrative systems.
July	United Kingdom	Energy / cyber	Cyberattack attributed to Iran-linked actors leaves an electrical facility offline for four days.
Late July	United States	Water / cyber	Cyberattacks target water systems in at least 7 states; some facilities switch to manual operations.

July 2026 overview

- 22 critical incidents or major signals recorded
- 12 countries or geographic groupings affected, in addition to incidents with international scope
- 15 events directly related to cybersecurity
- 5 events related to AI agents, platforms or components
- 6 events affecting energy, water or critical infrastructure
- 4 events related to networks, the Internet or communications equipment

- 3 events targeting public institutions or state-owned companies
- 3 events related to preparedness, resilience or infrastructure protection
- 2 events directly related to the Strait of Hormuz and maritime flows
- 2 cyberattacks resulting in physical or operational consequences for essential infrastructure
- 2 destructive events involving data erasure, encryption or destruction
- 2 actively exploited SonicWall zero-days
- 1 outage combining a power-grid failure and near-total Internet blackout
- 1 major GNSS jamming or spoofing signal affecting aviation

July stands out for the growing convergence between digital incidents and physical infrastructure: electricity, water, oil pipelines and public services are directly affected. Several events also involve AI agents capable of acting on real-world IT environments. At the same time, GNSS disruptions lead to stronger measures for aviation, France prepares a major blackout exercise, and the Hormuz crisis remains active with new attacks and another sharp decline in maritime traffic.

AUGUST 2026

Date	Country / area	Category	Event
Aug. 3	Cuba	Energy / Internet	Major power outage; national Internet traffic falls by approximately 59%.
Aug. 3-14	Latvia / NATO	Military / counter-drone	Baltic Trust 26 integrates counter-drone and electronic-warfare systems under operational conditions.
Early Aug.	Norway	Institution / DDoS	Massive attack against government digital infrastructure disrupts several services.
Aug. 11	International	Cyber / espionage	Fake CCleaner software enables espionage, credential theft and keystroke logging.
Aug. 11-14	Strait of Hormuz	Maritime / security	New attacks against vessels; traffic falls below ten transits on some days.
Aug. 12	Ukraine / Sevastopol	Energy / attack / Internet	Drone strikes hit energy infrastructure; Internet traffic falls by up to 95% for around 10 hours.
Aug. 13	International	Cyberespionage	Apple warns users in several countries about targeted spyware attacks.
Aug. 16	Latvia	Institution / cyber	Scale of the compromise affecting state-owned Latvijas Valsts Meži confirmed.
Aug. 21	Finland / NATO	GPS / resilience	Capabilities strengthened to detect and locate GNSS jamming and spoofing.
Aug. 24-25	Strait of Hormuz	Maritime / strategic flows	New attack against an oil tanker; no outbound vessels recorded for 24 hours.

Date	Country / area	Category	Event
Aug. 27-31	Strait of Hormuz	Maritime / security	Series of attacks against tankers; traffic remains far below pre-crisis levels.
August	Latvia	Institution / data	Cyberattack against road-safety systems compromises data on approximately 1.2 million people.
August	Estonia	Digital infrastructure	Disruptions affect government services, hospital networks and airport systems.
August	International	Cyber / network	Critical Citrix NetScaler vulnerabilities require urgent security updates.

August 2026 overview

- 14 critical incidents or major signals recorded
- 10 countries or geographic groupings affected, in addition to incidents with international scope
- 7 events directly related to cybersecurity
- 5 events affecting public institutions or essential infrastructure
- 3 events related to espionage or cyberespionage
- 3 events directly related to the Strait of Hormuz and the security of maritime flows
- 2 events causing sharp declines in Internet traffic
- 2 events affecting government digital infrastructure or services
- 2 events related to military preparedness, GNSS interference or electronic warfare
- 1 military attack against energy infrastructure
- 1 period of 24 hours with no outbound vessels recorded in Hormuz
- 1 event simultaneously affecting government, hospital and airport services

August remains marked by incidents directly affecting essential infrastructure, including two episodes combining energy disruptions with sharp declines in Internet connectivity. The situation in Hormuz becomes particularly unstable again, with several attacks against vessels and a temporary interruption of outbound traffic. At the same time, electronic warfare and GNSS resilience become increasingly prominent in the Baltic region, while several European government and public infrastructures continue to face significant digital disruptions.

SEPTEMBER 2026

Date	Country / area	Category	Event
Sep. 1	International	Cyber / network	Two SonicWall zero-days actively exploited against remote-access equipment.
Sep. 8	International	Cyber	New Google Chrome zero-day actively exploited.
Sep. 8-10	Strait of Hormuz	Maritime / security	Major wave of attacks against merchant vessels; several tankers hit and traffic disrupted.

Date	Country / area	Category	Event
Sep. 8-13	Australia / Singapore	Cables / Internet	Several major subsea cables offline or damaged; direct capacity sharply reduced.
Sep. 14	Portugal	Telecommunications / DDoS	Cyberattack against telecom operator MEO disrupts services.
Sep. 15-17	NATO / Europe	Resilience / preparedness	Resilience requirements published, prioritizing continuity of water, energy, healthcare and telecoms.
Sep. 15-17	Finland / Baltic / EU	Cables / infrastructure	MARSEC EU 26 simulates protection of cables, pipelines and subsea infrastructure against threats.
Sep. 17	United States	Energy / preparedness	Federal emergency order issued to secure the Mid-Atlantic power grid against outage risks.
Sep. 17	European Union	GPS / resilience	Galileo achieves first authenticated civilian GNSS position to strengthen resistance to spoofing.
Sep. 18	France	Infrastructure / security	Strengthened plan requested against drones, cyberattacks and sabotage targeting critical infrastructure.
Sep. 21	Ireland	Civil preparedness	Around 2.2 million emergency-preparedness guides distributed nationwide.
Sep. 25	International	Cyber	Microsoft SharePoint exploited, with risks of code execution and backdoor installation.
Sep. 27	International	Cyber / network	Two critical Citrix NetScaler vulnerabilities actively exploited.
Sep. 29	France	Institution / cyber	Major DGFIP compromises; data exfiltration remains undetected for several months.
Sep. 29	France	Energy / preparedness	Preparations begin for a national exercise simulating a major power outage.
Sep. 30	United States	Military / resilience	FORTRESS America launched to strengthen the autonomy and resilience of military installations.
Sep. 30	European Union	Communications / resilience	Secure network project aims to keep emergency services connected even without terrestrial networks.
September	Portugal / NATO / EU	GPS / military resilience	REPMUS 2026 tests drone navigation without GNSS in jammed or degraded environments.

September 2026 overview

- 18 critical incidents or major signals recorded
- 14 countries or geographic groupings affected, in addition to incidents with international scope
- 6 events directly related to cybersecurity
- 9 events related to preparedness, resilience or infrastructure protection
- 5 events affecting networks, telecommunications, cables or navigation systems
- 3 events related to energy, power grids or continuity of essential services
- 3 events related to military preparedness or strategic security
- 2 events directly related to subsea cables and infrastructure
- 2 events related to GNSS and operations in degraded navigation environments
- 2 measures explicitly addressing continuity of communications or services during disruptions
- 1 nationwide public preparedness campaign
- 1 national major power-outage exercise in preparation
- 1 major wave of attacks against shipping in the Strait of Hormuz
- 1 program launched to provide prolonged autonomy for military installations

September stands out above all for the growing number of measures focused on maintaining essential functions in degraded environments. Power grids, water, telecommunications, subsea cables, GNSS navigation and emergency communications are simultaneously the subject of protection or preparedness measures. This trend extends to the population through Ireland's emergency guides, to military infrastructure through FORTRESS America, and to France through preparations for a nationwide blackout exercise.

OCTOBER 2026

Date	Country / area	Category	Event
Oct. 1	Belgium	Civil preparedness	National crisis-preparedness guide launched, including recommendations for an emergency kit.
Oct. 3-11	Philippines / Vietnam / Singapore	Cables / Internet	Series of failures and disruptions affects several international subsea cables.
Oct. 6-15	NATO / Europe / United States	Military / preparedness	Steadfast Duel 26; ~8,000 participants test regional defense plans and multidomain operations.
Oct. 9	Luxembourg	Civil preparedness	National "72 hours of autonomy" guide launched for major outages and crises.
Oct. 12	France	Infrastructure / cyber	Cyberattack affects refrigeration at more than 700 supermarkets, causing significant physical losses.
Oct. 13	NATO / Italy	Nuclear / preparedness	Steadfast Noon 2026 begins; nuclear deterrence exercise involving 17 NATO countries.

Date	Country / area	Category	Event
Oct. 14	Luxembourg	Civil preparedness	Distribution of around 300,000 preparedness guides to households begins.
Oct. 14	International	Cyber / network	Critical security alert issued for Ivanti Connect Secure.
Oct. 19	European Union	Resilience / hybrid crisis	EU Integrated Resolve 2026 begins, testing European response to a complex hybrid crisis.
Oct. 19-30	NATO / Latvia	Communications / resilience	DiBaX26 tests resilient communications, 5G networks and continuity of the military digital backbone.
Oct. 20-21	International	Cyber / web infrastructure	Two critical PHP vulnerabilities enable remote code execution; emergency patches released.
Oct. 20-21	NATO / Germany	Subsea infrastructure	Meeting focuses on protection and rapid response involving subsea infrastructure.
Oct. 22	United Kingdom	Civil preparedness	"Be Ready" launched to prepare households for disruptions to essential services.
Oct. 23	France / United Kingdom	Energy / transport / weather	Major storm leaves nearly 300,000 French households without power and disrupts transport.
Oct. 25-26	United States	Military / resilience	FORTRESS America targets 90 days of autonomy for major bases during prolonged service disruptions.
Oct. 26	United States	Civil preparedness	Former FBI deputy director urges households to stock water, food, batteries and emergency equipment.
Late Oct.	International	Cyber	Critical PHP vulnerabilities actively exploited amid growing alerts involving network components.
Late Oct.	Europe	Preparedness / resilience	Government campaigns prepare populations for prolonged service disruptions.
Late Oct.	Strait of Hormuz	Maritime / geopolitics	Traffic remains exceptionally low, unlike at Suez, Bab-el-Mandeb or Panama.
Late Oct.	Spain	Transport / infrastructure	Major rail collision follows LZB failure; investigation focuses on the failure and control decisions.
Late Oct.	France	Security / terrorism	Trappes terrorist attack; profile remains unclear amid strong political polarization surrounding the case.

October 2026 overview

- 21 critical incidents or major signals recorded
- 16 countries or geographic groupings affected, in addition to events with European or international scope
- 11 events related to preparedness, resilience or infrastructure protection
- 4 events directly related to cybersecurity
- 4 events related to military preparedness, collective defense or deterrence
- 3 national civil-preparedness campaigns recorded in Belgium, Luxembourg and the United Kingdom
- 3 events affecting telecommunications, the Internet, cables or digital infrastructure
- 3 events related to continuity of communications or operations in degraded environments
- 2 major events directly affecting transport
- 2 events related to energy or the ability to operate without external network support
- 2 events related to subsea infrastructure or its protection
- 1 European exercise focused on responding to a complex hybrid crisis
- 1 nuclear deterrence exercise involving 17 NATO countries
- 1 major and persistent anomaly in maritime traffic through the Strait of Hormuz
- 1 terrorist event generating strong political and social polarization
- 1 military resilience objective reaching 90 days of autonomy

October is characterized by a strong concentration of preparedness and resilience measures. Several European governments are asking populations to prepare for prolonged disruptions to essential services, while military exercises simultaneously focus on collective defense, nuclear deterrence, hybrid crises and continuity of communications. This trend is accompanied by efforts to strengthen the autonomy of US military bases, protect subsea infrastructure and address persistent incidents directly affecting energy, cables, transport and digital systems.

Data recorded through October 29, 2026.

Overall assessment: January to October 2026

From January to October 2026, **206 critical incidents or major signals** were recorded in this chronology. Taken individually, they involve very different causes, contexts and actors. Viewed together, however, several trends emerge and either persist or intensify over the course of the year.

Cybersecurity represents the first continuous thread of the year, with attacks regularly targeting public institutions, telecommunications operators, energy infrastructure, cloud services, network equipment and software supply chains. Several incidents extend beyond the digital sphere and have operational consequences for physical services or infrastructure.

A second group directly concerns **essential infrastructure**: power grids, telecommunications, subsea cables, water systems, oil pipelines, transport, government services and digital infrastructure. Blackouts, telecommunications outages, cable failures and disruptions to essential services repeatedly occur across different regions.

Navigation and communication systems form another persistent thread. GNSS jamming and spoofing, particularly in the Baltic region, progressively lead to measures aimed at keeping aviation, drones, armed

forces and communications operational in environments where satellite systems or conventional networks may be unavailable or degraded.

From March onward, the **Strait of Hormuz crisis** adds a major strategic dimension: collapse in traffic, attacks against vessels, military escorts, disruptions to oil supplies, use of strategic reserves and successive attempts to restore maritime traffic. The situation becomes prolonged and remains visible through October.

But the clearest evolution over the course of the year concerns **preparedness for disruptions to essential services**. Military exercises, critical-infrastructure protection, counter-drone capabilities, blackout preparedness, continuity of communications, operations without GNSS, protection of subsea cables and energy autonomy gradually become more prominent.

This trend becomes particularly visible in September and October. Governments also begin directly preparing their populations for several days of autonomy, while the United States strengthens the ability of its major military installations to operate for up to **90 days without external support**. At the same time, NATO and the European Union increase exercises focused on collective defense, hybrid crises, resilient communications, subsea infrastructure and continuity of essential functions.

The chronology does not establish a causal link between all of these events. It does, however, reveal a development that is difficult to ignore: as 2026 progresses, the issue is no longer simply about protecting networks against isolated incidents, but increasingly about preparing states, armed forces, infrastructure and populations to continue operating when several essential systems are simultaneously unavailable or severely degraded. This convergence around continuity, autonomy and resilience constitutes the main underlying signal of the first ten months of 2026.

Follow the situation in France

Explore the **Palks Studio Radars** to track key indicators daily: fuel, cybersecurity, maritime flows, energy and infrastructure.

→ [View the daily Radars](#)

2026: data recorded through October 29, 2026. Non-exhaustive list based on publicly documented events.

Report edited and published by Palks Studio.

© Palks Studio, 2025. All rights reserved.

This report is made freely available to the public. Any reproduction or substantial reuse of its content must credit the source: Palks Studio.