PERIODIC OPEN-SOURCE ASSESSMENT

Kings Secure Technologies
Security Threat Intelligence and Risk Outlook

Edition 16 November 2026

Reporting period	9 November 2026 09:17 GMT to 16 November 2026 09:13 GMT
Information cut-off	16 November 2026 09:13 GMT, Europe/London
Comparison basis	Previous successfully distributed corrected edition, cut off 9 November 2026 09:17 GMT
Audience	KST leadership, operations, Grapevine analysts and client heads of security

Key judgement

The most consequential change is the demonstrated physical impact of compromised connected plant: France attributes destructive attacks on supermarket refrigeration controls to an Iranian state-linked unit. Combined with new allegations around RAF Fairford, this reinforces the need to treat operational technology, contractors and apparently low-level logistics as part of protective security. In the UK, most immediate disruption is more likely to arise from hoax communications, technology outages, acquisitive crime and winter transport impacts than from a change in the official terrorism threat level.

Status: Validated for external circulation subject to successful attachment and recipient checks at distribution.

Contents

1 Executive Security Briefing
2 Global Geopolitical Outlook
3 European Security Outlook
4 UK Security Overview
5 UK PESTLE Security and Resilience Assessment
6 Forward Look and Priority Actions
7 Sources and Methodology

1 Executive Security Briefing

This edition identifies five material developments since the 9 November cut-off. The focus is operational consequence: preventing physical effects from compromised systems, maintaining proportionate responses to ambiguous threats, preserving alternative communications and planning for travel and staffing disruption.

Issue	Geography / sector	Change	Operational implication	Priority	Confidence
Connected refrigeration sabotage	France; retail, food and operational technology	Worsening	A national attribution links destructive cyber activity to fires and food loss at more than 700 sites. UK operators should test whether connected plant can be isolated and operated safely offline.	ACT	Moderate
RAF Fairford allegations	UK defence-related sites and adjacent supply chains	Worsening	New US charges allege overseas direction and UK logistics for the September plot. Proceedings remain active and allegations are unproven.	ACT	Moderate
Mass school threat emails	UK education and public-facing estates	New; low assessed credibility	Thousands of near-identical messages caused concern but were assessed by police as hoaxes. Proportionate triage and police liaison reduce avoidable evacuation and service loss.	PREPARE	High
Maritime and aviation continuity	Red Sea, Gulf, Black Sea and transatlantic travel	Materially unchanged maritime risk; new aviation outage	Chokepoint risk remains elevated. A non-malicious FAA network failure also demonstrated the scale of disruption from ageing critical systems.	PREPARE	Moderate
UK service and winter disruption	Police communications, transport and northern UK sites	New	Microsoft disruption affected some police email and online reporting. Snow warnings and planned London industrial action add short-term staffing and journey risk.	PREPARE	High

Rating definitions. Act means an immediate control or assurance check is justified. Prepare means complete a time-bound readiness step before exposure increases. Monitor means maintain watch and pre-agreed escalation criteria.

Confidence describes evidence strength, not severity: High is supported by current authoritative evidence; Moderate is credible but includes attribution, allegation or unresolved detail; Low would indicate material uncertainty.

Priority actions this week

- Act: estates and technology owners should confirm that connected refrigeration, building-management and other safety-critical plant have unique credentials, restricted remote access, current supplier contacts, tested isolation steps and safe manual or offline operation.
- Act: security and facilities teams at defence-linked, critical-infrastructure and logistics locations should refresh contractor challenge, suspicious-vehicle reporting, perimeter observation and fuel or precursor escalation procedures without profiling lawful visitors or staff.
- Prepare: public-facing sites should use a documented threat-message triage process, retain original messages, avoid unnecessary forwarding, consult police promptly and make evacuation decisions from assessed credibility and site conditions.
- Prepare: maintain tested voice and radio alternatives for email, online reporting and supplier-platform outages; independently verify unexpected technical-support contact.
- Prepare: review staffing, lone-working and journey plans for snow-affected regions and London sites exposed to planned Piccadilly line and wider Tube industrial action.

2 Global Geopolitical Outlook

Middle East maritime routes remain costly and exposed

Confirmed or attributed facts. UKMTO assessed the threat in the Southern Red Sea and Bab el-Mandeb as SUBSTANTIAL on 12 November, meaning deliberate attacks were a strong possibility, despite no reported attack on shipping in that area during the week. It also warned that disclosure of voyage details in response to Houthi communications may increase targeting risk and that favourable sea conditions support small-boat activity in the Gulf of Aden. On 13 November, the UN said the IMO had recorded 134 confirmed incidents in the Strait of Hormuz and wider Middle East maritime area as at 11 November, with 25 seafarer deaths; it separately noted no recent reported commercial-vessel attack in the Red Sea. [1][2]

KST assessment. The position is materially unchanged but remains operationally significant. Likelihood is route-dependent and not uniform across the region; consequence remains high because delay, diversion, insurance cost, crew exposure and fuel-price effects can reach UK logistics and facilities even where KST has no direct regional presence. Confidence is High on the published maritime posture and Moderate on the short-term trajectory because control claims around the Bab el-Mandeb approaches are contested.

Recommended action. Logistics and procurement leads should retain route and lead-time contingencies, confirm that carriers follow current maritime-security guidance and identify where stock or maintenance commitments depend on single corridors. Monitor verified UKMTO and carrier updates rather than social-media claims.

Black Sea spillover continues to affect civilian transport

Confirmed or attributed facts. Associated Press reported on 15 November that three commercial vessels in the Black Sea were struck by drones overnight. Romania’s Ministry of National Defence dashboard, updated 15 November, records 117 attacks near the border, 39 unauthorised airspace entries and six drones brought down during 2026. The Romanian public data do not assign the origin of every incident. [3][4]

KST assessment. Exposure is worsening for shipping and infrastructure close to the conflict area, with plausible knock-on effects for grain, energy, marine insurance and onward road and rail capacity. UK sites are more likely to experience schedule and cost volatility than direct physical impact. Confidence is Moderate because the regional pattern is clear but individual drone attribution and vessel-damage details remain incomplete.

Recommended action. Supply-chain owners should flag Black Sea dependencies, preserve alternative ports and transport modes, and use contractual notification thresholds for material delay or route change.

Aviation outage illustrates non-malicious systemic risk

Confirmed facts. The US Federal Aviation Administration said a technical problem on 13 November destabilised communications and radar feeds at 17 of 22 Air Route Traffic Control Centers. A nationwide ground stop ran until 20:15 Eastern Time. The FAA said it had no indication of a cyberattack or hostile actor and reported approximately 12,462 cancellations that day, not all directly caused by the ground stop. [5]

KST assessment. This is an availability and concentration-risk indicator, not evidence of hostile action. The operational lesson is the speed at which failure in a shared legacy network can propagate into passenger welfare, staffing, freight and executive-travel disruption. Confidence is High.

Recommended action. Travel and logistics functions should retain manual contact paths, avoid time-critical single-flight dependencies and include prolonged recovery, not only outage duration, in continuity assumptions.

3 European Security Outlook

France attributes destructive attacks on connected retail plant to Iran

Confirmed attribution. On 10 November, France stated that cyber attacks during the night of 11 to 12 October targeted supermarket refrigeration controllers at more than 700 retail sites. The French government reported fires, material damage and food losses valued at tens of millions of euros, and attributed the activity to SHAHID KAVEH, an offensive cyber unit affiliated with the Islamic Revolutionary Guard Corps. France said it would seek further EU sanctions. The underlying technical evidence has not been published for independent review. [6]

KST assessment. This is the edition's clearest example of cyber activity producing physical and commercial harm through connected operational technology. Relevance extends beyond refrigeration to building management, access control, CCTV, alarms and remote maintenance platforms where insecure credentials or exposed supplier access could affect safety and availability. The threat is worsening at European level. Confidence is Moderate: the incident and official attribution are clear, but the evidential basis and access path are not public.

Recommended action. Act within seven days: identify internet-connected plant, confirm ownership of remote accounts, remove dormant supplier access, require multi-factor authentication where supported, document safe isolation, and test recovery from known-good configurations. Treat unexpected temperature, set-point or device-state changes as a possible security event as well as a maintenance fault.

Estonia reports an attempted sabotage operation against a drone company

Attributed facts. Estonia's government said on 15 November that its Internal Security Service assessed an attempted attack on drone manufacturer Threod Systems to have been ordered by Russia's military intelligence service, the GRU. The Prime Minister asked officials to prepare possible steps to close the Estonia-Russia border and described cooperation between the state and business as central to stopping the attempt. [7]

KST assessment. The development reinforces the exposure of defence, dual-use technology and their suppliers to proxy recruitment, surveillance and low-complexity sabotage. It does not mean equivalent risk at all commercial premises. Confidence is Moderate because the attribution is official but supporting intelligence is not public.

Recommended action. Operators supporting defence or critical infrastructure should review contractor assurance, unusual approaches to staff, off-site storage, perimeter surveillance and the security of publicly available logistics information. Escalation criteria should focus on behaviour and access, not nationality or lawful political belief.

European airports seek clearer hybrid-threat responsibilities

Sector evidence. Airports Council International Europe issued a strategy on 12 November in response to bomb threats, drone incursions and cyber attacks affecting European aviation. It calls for clearer division of responsibility between airports and public authorities, stronger cooperation and sustainable funding for resilience. [8]

KST assessment. This is a sector-readiness indicator rather than an official change in threat level. It is relevant to airport suppliers, nearby commercial property and transport partners because uncertain ownership can delay threat assessment and recovery. Confidence is High on the publication and Moderate on how quickly recommendations will be implemented across countries.

Recommended action. Aviation-linked sites should document who decides on evacuation, airside or landside restriction, drone escalation and restoration, and should validate out-of-hours contact details across landlords, operators, police and suppliers.

European outlook

The region's most credible near-term indicators are further official attribution of sabotage or proxy activity, additional restrictions at the Estonia-Russia border, confirmed drone damage to civilian shipping or infrastructure, and new national measures affecting airport or critical-infrastructure security. Material improvement would require sustained absence of incidents, clearer de-escalation around maritime corridors and evidence that resilience measures are reducing disruption.

4 UK Security Overview

Official terrorism threat levels

Verified at 09:13 GMT on 16 November 2026. The official UK national terrorism threat level is **SEVERE**, meaning an attack is highly likely. This covers England, Wales, Scotland and Northern Ireland from all forms of terrorism. The separately published threat level from Northern Ireland-related terrorism in Northern Ireland is **SUBSTANTIAL**, meaning an attack is likely. [9]

There has been no change since the previous edition. These are official terrorism threat levels, not KST all-hazards ratings, and they do not imply equal likelihood or exposure at every site. Protective measures should remain proportionate to site, activity, footfall, symbolic value, access and local information.

New US allegations add detail to the RAF Fairford investigation

Confirmed procedural position and allegations. Counter Terrorism Policing reported on 27 October that two men had been charged under the National Security Act 2023 following the RAF Fairford investigation. On 10 November, the US Department of Justice unsealed a superseding indictment alleging that three Iran-backed operatives supported nearly 20 attacks or attempted attacks across Europe and the United States and that one directed the September RAF Fairford plot through UK contacts. An indictment is an allegation; the defendants are presumed innocent unless proved guilty. UK proceedings are active and must not be prejudiced. [10][11]

KST assessment. The new material worsens the assessment of hostile-state use of criminal or proxy logistics around sensitive sites, but it does not establish the guilt of those charged in the UK or US. Relevant exposure includes vehicle acquisition, fuel and precursor procurement, surveillance and the use of apparently legitimate service branding. Confidence is Moderate because public charging documents provide detail but findings have not been tested at trial.

Recommended action. Maintain robust visitor and contractor verification, report suspicious observation or vehicle behaviour promptly, and ensure procurement and facilities staff understand escalation routes for unusual bulk purchases or attempts to bypass normal access. Avoid operational speculation about named defendants or communities.

School threat messages assessed as hoaxes

Confirmed facts. On 11 November, the Police Service of Northern Ireland said more than 300 schools had reported the same threatening email, which originated outside the UK; checks had found nothing untoward and police assessed the public risk as low. Police Scotland later said the same message had been sent to thousands of addresses across several countries in a short period and did not represent a credible or wider threat. Investigation of the source remains ongoing. [12][13]

KST assessment. The immediate threat from this campaign is assessed as low on police evidence, but disruption, anxiety and copycat behaviour remain plausible. The position is new but not an indication of a broader rise in credible threats. Confidence is High for the police assessment and Moderate for recurrence.

Recommended action. Preserve original messages and headers, restrict onward circulation, check for site-specific detail or corroborating behaviour, consult police and use dynamic risk assessment before evacuation. Staff communications should distinguish a police-assessed hoax from a general instruction to remain vigilant.

Police contingency arrangements tested by Microsoft disruption

Confirmed facts. NPCC said on 13 November that a global Microsoft service disruption beginning on 12 November affected some police email and online reporting services. Essential policing continued through contingency arrangements, but delays were expected. NPCC also warned of fraudsters impersonating Microsoft technical support. [14]

KST assessment and action. The direct operational position was improving, but the event demonstrates reliance on shared cloud services and the opportunity for follow-on impersonation. Confidence is High. Control rooms and client teams should retain tested telephone, radio and offline contact lists, and independently verify unexpected support calls before granting access or disclosing codes.

5 UK PESTLE Security and Resilience Assessment

Political

Material change. New US allegations provide further detail on suspected Iranian-linked hostile activity around RAF Fairford, while the official national terrorism threat level remains SEVERE. The operational implication is continued attention to proxy methods, reconnaissance, contractors and apparently ordinary logistics at sensitive or symbolically

relevant sites. Action: refresh suspicious-activity escalation and contractor assurance within seven days. Confidence: Moderate, because the detailed claims are allegations in active proceedings. [9][10][11]

Economic

Material change. ONS estimated that UK GDP grew by 0.7% in Quarter 3 2026 and 0.2% in September, while construction output fell by 0.7% across the quarter. This does not establish a direct change in security risk. It does, however, support continued scrutiny of supplier capacity, vacancy, maintenance deferral and margin pressure where these affect guarding, repairs or resilience. Maritime disruption remains a separate source of cost and lead-time uncertainty. Action: monitor service-level exceptions and critical supplier concentration rather than inferring crime from economic conditions. Confidence: High on the statistics; Moderate on site-level implications. [15]

Social

Material change. Police assessed the mass school emails as hoaxes, but the campaign shows how high-volume messages can create rapid public-facing disruption. Separately, NPCC reported a new pilot targeting prolific retail offenders and said police-recorded shop theft fell by 4% in the year ending March 2026, while organised groups remain significant. The NCA reported 349 arrests and £2.2 million cash seized during the October phase of Operation Machinize, alongside wider commodity seizures; these are enforcement results, not proof about any uninvestigated business. [12][13][16][17]

Security implication. Retail, high-street and commercial-property teams should combine staff-welfare measures, evidence preservation and police information-sharing with proportionate access and cash controls. Peaceful protest should remain distinct from violence, criminal damage or evidenced obstruction. Action: review incident-reporting quality, staff support after threats or abuse, and landlord-tenant escalation routes. Confidence: High on the published operations; Moderate on local displacement of offending.

Technological

Material change. The Microsoft disruption affected police communications, and France’s attribution shows that compromised operational technology can cause physical damage. No new malicious-AI involvement was verified in the selected UK incidents. The 3 November NCSC Annual Review nevertheless assesses that AI is improving reconnaissance, social engineering, vulnerability discovery and exploit development, while INTERPOL has documented deepfake-enabled impersonation risks including voice and video requests. [6][14][18][19]

Security implication. Connected security systems, building controls and supplier portals should be treated as availability and safety dependencies. Action: maintain separate administrative accounts, multi-factor authentication, network segmentation where feasible, offline recovery material and independent verification for urgent payment, access or credential requests. Confidence: High on the incidents and official assessments; Low for any claim that AI played a part in the incidents covered, because none was evidenced.

Legal

Material change. The Terrorism (Protection of Premises) Act 2025 is enacted, but the SIA states that Martyn’s Law will not come into force before spring 2027. On 9 November the regulator published planning tools for standard-tier premises and an enhanced-tier template, updated on 10 November to correct links and typographical errors. These are preparation tools; organisations should not submit completed templates until the regime is in force. The Cyber Security and Resilience (Network and Information Systems) Bill remains proposed legislation, not enacted law, and would expand and strengthen duties for essential and digital services if passed. [20][21][22]

Operational awareness. In-scope organisations should identify accountable functions, map procedures and retain evidence of proportionate preparation without presenting draft material as a regulatory submission. Relevant organisations should track the Cyber Security and Resilience Bill and regulator guidance. This is operational awareness, not legal advice. Confidence: High.

Environmental

Material change. At cut-off, the Met Office had yellow warnings covering snow and travel disruption on 16 and 17 November across parts of Scotland and northern England, with some warning areas extending into the Midlands and Yorkshire. The Environment Agency reported two flood alerts in England at 05:16 on 16 November, while the five-day national flood risk was assessed as very low. [23][24]

Security implication. Local snow, ice and wind effects may disrupt high routes, rail, power lines, staffing and response times despite the low national flood outlook. Action: affected sites should check gritting, welfare, battery and generator readiness, contractor attendance and safe lone-working arrangements. Confidence: High at cut-off; warnings are transient and should be rechecked before action.

6 Forward Look and Priority Actions

Next 14 days

Window	Indicator or event	Why it matters	Action	Responsible function
16-17 Nov	Met Office snow warnings	Higher routes, rail, power and staffing may be disrupted locally.	**ACT**	Operations / facilities
20-21 Nov	Planned Piccadilly line service-control strike	Severe Piccadilly line disruption, no Friday Night Tube and some District line effect if action proceeds.	**PREPARE**	Workforce planning
26-27 Nov	Planned Tube drivers' strike	Broader London journey and shift-cover disruption if action proceeds.	**PREPARE**	Operations / HR
Daily	UKMTO, Black Sea and airline recovery updates	Route or schedule changes could affect freight, travel and staff welfare.	**MONITOR**	Travel / procurement
Daily	Follow-on school, public venue or technical-support hoaxes	Copycats can create disruption even where credibility is low.	**MONITOR**	Security / communications
Seasonal	Christmas markets and rising festive footfall	Crowding, theft, staff abuse and transport demand increase exposure at retail and public sites.	**PREPARE**	Site security / retail ops

Transport dates are current at cut-off and may change. TfL advises passengers to check before travel. [25]

Selected 30 to 90 day indicators

- Martyn's Law: publication of a confirmed commencement date, regulator consultation or sector-specific guidance would move preparation into a firmer delivery window. Current official position is not before spring 2027.
- Hostile-state activity: further UK or European charges, sanctions, official attributions or disruption of proxy networks would change the assessment. Convictions or acquittals, not allegations alone, should guide conclusions about individual culpability.
- Operational technology: disclosure of the access method used in France, exploitation of the same controller family elsewhere, or UK NCSC guidance would justify targeted technical assurance beyond the current baseline.
- Maritime routes: confirmed attacks on commercial vessels, mine or drone incidents nearer NATO waters, or sustained reopening and lower insurance costs would change the continuity outlook.
- Winter resilience: escalation from yellow to amber or red weather warnings, material power disruption or rising flood risk would require local continuity activation.

Action summary

- ACT now: assure connected plant and supplier remote access; refresh contractor and suspicious-activity controls at higher-exposure sites; implement local snow precautions where warnings apply.
- PREPARE this week: test alternative communications; rehearse threat-message triage; confirm London shift and journey contingencies; use the SIA tools to structure Martyn's Law readiness.
- MONITOR: verified maritime, police, weather, transport and regulator sources. Escalate on confirmed operational impact, not solely on volume of online reporting.

7 Sources and Methodology

1. UK Maritime Trade Operations Joint Maritime Information Center, *JMIC Advisory Update 113*, 12 November 2026. Source (accessed 16 November 2026).

2. United Nations Department of Political and Peacebuilding Affairs, *Remarks by the Assistant Secretary-General at the Security Council on the Middle East*, 13 November 2026. Source (accessed 16 November 2026).

3. Associated Press, *Zelenskyy says Starshield restrictions threaten Ukraine's energy defenses ahead of winter*, 15 November 2026. Source (accessed 16 November 2026).

4. Romanian Ministry of National Defence, *Drone and sea-mine incident dashboard*, updated 15 November 2026. Source (accessed 16 November 2026).

5. US Federal Aviation Administration, *Nationwide Ground Stop Questions and Answers*, 15 November 2026. Source (accessed 16 November 2026).

6. France Diplomatie, *Declaration of attribution to Iran of cyber attacks against France*, 10 November 2026. Source (accessed 16 November 2026).

7. Government of Estonia, *Preparedness and cooperation stopped another sabotage attempt by Russian intelligence services*, 15 November 2026. Source (accessed 16 November 2026).

8. ACI EUROPE, *European airports set out new strategy as hybrid threats intensify*, 12 November 2026. Source (accessed 16 November 2026).

9. MI5, *Threat Levels*, live page; verified 16 November 2026 at 09:13 GMT. Source (accessed 16 November 2026).

10. Counter Terrorism Policing, *Two men charged under the National Security Act in RAF Fairford investigation*, 27 October 2026. Source (accessed 16 November 2026).

11. US Department of Justice, *Three Iranian-Backed Operatives Indicted for Their Roles in Nearly 20 Terrorist Attacks and Attempted Attacks*, 10 November 2026. Source (accessed 16 November 2026).

12. Police Service of Northern Ireland, *Threatening emails to over 300 schools being treated as a hoax*, 11 November 2026. Source (accessed 16 November 2026).

13. Police Scotland, *Statement after threatening messages sent to a number of schools in Scotland*, 11 November; updated 13 November 2026. Source (accessed 16 November 2026).

14. National Police Chiefs' Council, *Police continue to operate during Microsoft disruption*, 13 November 2026. Source (accessed 16 November 2026).

15. Office for National Statistics, *GDP monthly estimate UK September 2026*, 12 November 2026. Source (accessed 16 November 2026).

16. National Police Chiefs' Council, *Forces crackdown on prolific retail offenders*, 11 November 2026. Source (accessed 16 November 2026).

17. National Crime Agency, *Operation Machinize crackdown across the UK*, 11 November 2026. Source (accessed 16 November 2026).

18. National Cyber Security Centre, *NCSC Annual Review 2026 The impact of AI on cyber threat*, 3 November 2026. Source (accessed 16 November 2026).

19. INTERPOL, *Public awareness campaign highlighting risk of AI deepfake scams*, 18 October 2026. Source (accessed 16 November 2026).

20. Security Industry Authority, *New tools to support preparation for Martyn's Law*, 9 November 2026. Source (accessed 16 November 2026).

21. Security Industry Authority, *Martyn's Law enhanced tier template*, 9 November; updated 10 November 2026. Source (accessed 16 November 2026).

22. UK Government, *Cyber Security and Resilience Network and Information Systems Bill summary*, updated 3 November 2026. Source (accessed 16 November 2026).

23. Met Office, *UK weather warnings*, live page; verified 16 November 2026 at 09:13 GMT. Source (accessed 16 November 2026).

24. Environment Agency and Met Office, *Check for flooding in England*, updated 16 November 2026 at 05:16 GMT. Source (accessed 16 November 2026).

25. Transport for London, *Strikes*, live page; verified 16 November 2026. Source (accessed 16 November 2026).

Methodology and limitations

This is a periodic open-source assessment, not restricted intelligence, a live warning service, legal advice or a site-specific risk assessment. Research prioritised current primary sources and separately identified facts, official or legal allegations, KST assessment and recommended action. Event dates were distinguished from publication dates. Consequential attributions were qualified where underlying intelligence was not public.

Confidence definitions. High: current authoritative evidence with limited material uncertainty. Moderate: credible evidence but unresolved attribution, allegation, incomplete technical detail or an uncertain trajectory. Low: significant information gaps or a largely inferential judgement. Confidence describes evidence strength, not severity.

Material limitations. French and Estonian attribution evidence is not public. UK and US RAF Fairford proceedings are unresolved. The origin and responsibility for individual Black Sea drone incidents remain incomplete. Microsoft’s root-cause account may develop. Weather, flood, transport and threat-level pages are transient. No malicious-AI involvement was verified in the physical incidents selected for this edition.

Information cut-off: 16 November 2026 at 09:13 GMT, Europe/London. Sources published after the cut-off are outside this edition.