



**THE CAMBRIDGE  
SENTINEL**

# THE CAMBRIDGE SENTINEL

Intelligence Briefing for Security Professionals

**Issue #5 | 8 January 2026**

Published by Rittel Consulting

Coverage Period: 8 January 2026 - 14 January 2026

## Executive Summary

The second week of 2026 continues to be defined by significant escalation in geopolitical volatility, driven by unilateral US military action in Venezuela and a deepening crisis within the NATO alliance concerning Greenland. These events introduce substantial new risks to global energy markets, supply chain stability, and the foundational principles of transatlantic security. For UK organisations, the strategic landscape has become markedly less predictable, demanding an immediate reassessment of operational resilience frameworks and geopolitical risk exposure. Concurrently, the UK has advanced its own counter-terrorism objectives through targeted strikes in Syria, highlighting the persistent threat from established international terror groups.

Nationally, the security industry is on the cusp of a major regulatory transformation. The Security Industry Authority (SIA) has launched public consultations on business licensing and the mandatory licensing of in-house CCTV operators, direct consequences of the Manchester Arena Inquiry. These reforms, coupled with an aggressive crackdown on training malpractice under Operation Resolute and a strategic review of all qualifications, signal a new era of accountability and professionalism that will impact all sectors utilising private security. The government has also launched a new Cyber Action Plan to bolster the resilience of public services, while trends in acquisitive and retail crime continue to necessitate enhanced protective security measures.

Locally, the Cambridge-London-Oxford corridor faces persistent disruption from ongoing industrial action affecting public transport, compounded by severe weather warnings that threaten to impact logistics and staff availability. Key sector developments, particularly in life sciences, continue to elevate the region's profile as a target for industrial espionage. This issue provides a comprehensive four-week protest horizon scan, detailing over twenty planned events with the potential for significant operational disruption, and includes a full analysis of local policing intelligence across the corridor.

## Section 1: Geopolitical & International Intelligence

### 1.1. US Unilateral Actions Reshape Global Risk Landscape

The first week of 2026 has been marked by significant unilateral actions by the United States, creating a volatile and unpredictable international environment. For UK-based organisations, these events have direct implications for supply chain stability, international travel, and the overarching security climate. The developments demand a measured, non-partisan analysis focused on operational resilience rather than political sentiment.

**Venezuela Operation:** On 3 January 2026, a US special forces operation resulted in the capture of Venezuelan President Nicolás Maduro. The subsequent installation of an interim government and assertion of control over the nation's oil reserves introduces significant instability into global energy markets. While immediate price shocks have been muted, the potential for retaliatory cyber-attacks against Western financial institutions or energy infrastructure remains a key concern. From an operational resilience perspective, organisations with supply chains or operations in Latin America must now factor in heightened political risk and the potential for regional destabilisation. The event serves as a stark reminder of the fragility of global supply chains to sudden geopolitical shifts.

**Greenland & NATO Tensions:** Renewed US interest in the acquisition of Greenland, including statements that military action is an option, has created an unprecedented crisis within the NATO alliance. Denmark has warned this would mean the "end of NATO". This introduces doubt over the long-term stability of the collective security framework that has underpinned European security for decades. This uncertainty may impact long-term investment decisions and requires a re-evaluation of strategic risk models that assume a stable transatlantic security partnership. The situation underscores the importance of organisational agility and the need for contingency planning that accounts for fractures in established international alliances.

**European Response:** A "Coalition of the Willing" summit in Paris on 6 January, attended by the UK, France, and Ukraine, resulted in renewed long-term security guarantees for Ukraine. This signals a move towards a more independent European defence posture. For the defence, technology, and professional services sectors, this may signal a long-term shift in procurement and collaboration opportunities towards European partners, reinforcing the need for businesses to monitor and adapt to evolving geopolitical alignments.

### 1.2. UK Counter-Terrorism Operations

On 4 January 2026, the UK, in coordination with France, conducted targeted air strikes against Daesh leadership in Syria. This action underscores the persistent threat from international terrorist groups and the UK's commitment to conducting overseas counter-terrorism operations. It may elevate the risk of retaliatory actions against UK interests, both at home and abroad, requiring heightened vigilance for all organisations, particularly those with a high public profile or links to government.

## Section 2: National (UK) Intelligence

### 2.1. SIA Regulatory Overhaul & Martyn's Law Preparations

The Security Industry Authority (SIA) is advancing a significant programme of regulatory reform with major implications for operational resilience and compliance across all sectors.

**Business & In-House Licensing:** A public consultation is underway on the licensing of security contractors (business licensing) and the extension of SIA licensing to in-house CCTV operators. This move, driven by the Manchester Arena Inquiry, aims to increase accountability and standardise training, including counter-terrorism awareness. Organisations utilising in-house security or contracted services must prepare for enhanced regulatory scrutiny, potential cost increases associated with compliance, and begin auditing their current security provision.

against the proposed standards.

**Operation Resolute & Training Malpractice:** The SIA's crackdown on training malpractice, Operation Resolute, saw 19 training centres closed and 242 licences suspended in 2025. This highlights the critical importance of due diligence in the procurement of security services and ensuring all security personnel hold legitimately obtained qualifications. Verifying the credentials of security partners is a key operational resilience measure.

**Strategic Qualifications Review:** A major review of all licence-linked qualifications was launched in December 2025 to align skills with the new responsibilities under Martyn's Law. This will likely lead to new, more rigorous training requirements for security staff across all sectors, focusing on threat recognition, incident response, and public safety.

## 2.2. Cyber Security

The UK Government has launched a new Cyber Action Plan to bolster the resilience of public services against cyber threats. The plan focuses on protecting critical infrastructure and improving incident response capabilities. The National Cyber Security Centre (NCSC) continues to warn of persistent threats from state-sponsored actors and ransomware groups, exacerbated by the current geopolitical instability. Organisations are strongly reminded to review and test their incident response plans, ensure all software and systems are patched and up-to-date, and promote a culture of cyber security awareness among all staff.

## 2.3. National Security Threat Levels

The terrorism threat level system provides a clear indication of the likelihood of a terrorist attack in the UK. Threat levels are set by the Joint Terrorism Analysis Centre (JTAC), part of MI5, and are kept under regular review based on available intelligence, terrorist capability and intentions, and timescale assessments.

**Current National Threat Level (UK Mainland):** The threat to the UK from all forms of terrorism is currently assessed as **SUBSTANTIAL**, meaning an attack is likely. This threat level has been in place since 9 February 2022 and applies to England, Wales, Scotland, and Northern Ireland.

**Current Northern Ireland Threat Level:** The threat to Northern Ireland from Northern Ireland-related terrorism is also assessed as **SUBSTANTIAL**, meaning an attack is likely. This level was reduced from **SEVERE** on 6 March 2024, reflecting the longest period without a national security attack in Northern Ireland since the start of the Troubles.

The five-tier threat level system operates as follows: **LOW** (attack highly unlikely), **MODERATE** (attack possible but not likely), **SUBSTANTIAL** (attack likely), **SEVERE** (attack highly likely), and **CRITICAL** (attack highly likely in the near future). Changes to threat levels are primarily a tool for security practitioners and police to determine appropriate protective security responses. However, all organisations should maintain vigilance regardless of the current threat level and report suspicious activity to police on 999 or the Anti-Terrorist Hotline on 0800 789 321.

## 2.4. Intelligence Community Assessments

The UK intelligence and security agencies provide critical insight into the evolving threat landscape facing the nation. Recent assessments from MI5, GCHQ, and the National Cyber Security Centre (NCSC) paint a picture of a more hostile and complex security environment than at any time since the immediate post-9/11 period.

**MI5 Terrorism Assessment:** In his October 2025 annual threat update, MI5 Director General Sir Ken McCallum reported that MI5 is running near-record volumes of terrorism investigations. Since the start of 2020, MI5 and police have disrupted 19 late-stage attack plots and intervened in hundreds of developing threats. The nature of the threat has evolved, with investigations now typically focused on individuals and small groups rather than larger established networks. However, the aggregate scale remains substantial. Al Qaeda and Islamic State are becoming more ambitious, taking advantage of overseas instability to gain firmer footholds and encouraging attacks in the West. A particularly concerning trend is the involvement of minors in terrorism investigations, with one in five of the 232 terrorism arrests in the previous year involving children under 17. In response, MI5 has established an Interventions Centre of Expertise to provide multi-agency support for vulnerable young people on pathways towards extremist violence.

**MI5 State Threats Assessment:** The most significant shift in MI5's mission since 9/11 is the dramatic escalation in state threats. Director General McCallum reported a 35% increase in the number of individuals investigated for state threat activity in the last year. This includes espionage targeting Parliament, universities, and critical infrastructure. State actors are now routinely commissioning surveillance, sabotage, arson, and physical violence on UK soil. Russia continues to use proxy recruitment via social media and encrypted apps to conduct malign activities, with multiple convictions secured in 2025. Iran poses a significantly increased physical threat, with at least 20 potentially lethal plots disrupted since January 2022. China presents a daily national security threat through espionage operations targeting UK democracy, economy, and security. These state threats now represent a challenge of equal or greater scale to terrorism.

**NCSC Cyber Threat Assessment:** The National Cyber Security Centre, part of GCHQ, reported 204 nationally significant cyber incidents between September 2024 and August 2025, representing a 130% spike in critical incidents. The Government Cyber Action Plan, published on 6 January 2026, identifies cyber-attacks as the top national security threat affecting critical infrastructure and public services. State-sponsored actors, particularly from Russia, China, and Iran, continue to conduct persistent cyber operations against UK targets. Ransomware groups remain a significant threat to both public and private sector organisations. The NCSC continues to provide authoritative technical guidance and incident response coordination, but the threat environment is assessed as increasingly complex and challenging.

**Operational Implications:** For UK organisations, these intelligence assessments underscore the need for a comprehensive security posture that addresses terrorism, state-sponsored espionage, and cyber threats simultaneously. Physical security measures must be complemented by robust personnel security and cyber security programmes. Organisations in sectors of strategic importance—including defence, technology, life sciences, critical infrastructure, and academia—face heightened risks and should ensure their security measures are proportionate to the threat. Close liaison with protective security advisors, local police, and sector-specific security networks is strongly advised.

## 2.5. Acquisitive & Retail Crime

Analysis of recent data indicates a continuing upward trend in acquisitive crime, particularly in the retail sector. The British Retail Consortium's latest survey highlights a significant increase in violence and abuse against retail staff, linked to a rise in organised shoplifting. This trend requires a multi-faceted operational resilience strategy, combining physical security measures (such as CCTV and access control), comprehensive staff training in de-escalation and conflict management, and close liaison with local police forces to share intelligence and coordinate responses.

# Section 3: Local (Cambridge/Oxford/London Arc) Intelligence

## 3.1. Transport & Infrastructure Disruption

Ongoing industrial action by bus operators in Cambridge continues to cause significant disruption to public transport across the city. This has a direct impact on staff commuting, client access, and business logistics. A severe weather warning for ice and snow has also been issued for the coming week (8-14 January), which is likely to exacerbate travel difficulties across the entire corridor. Businesses should immediately review their remote working policies, confirm the robustness of their business continuity plans to manage staff absences, and communicate alternative travel advice to staff and visitors.

## 3.2. Sector Developments

The University of Cambridge has announced a new strategic partnership with AstraZeneca and Beijing-based parties to accelerate life sciences innovation. This development, while positive for the region's economy, significantly increases the attractiveness of Cambridge as a target for industrial espionage and cyber-attacks. Life sciences and technology firms in the corridor must remain vigilant, ensuring their physical security, intellectual property protection, and cyber security measures are robust and subject to regular review.

## Section 4: Local Policing Intelligence

### 4.1. Thames Valley Police: Rural Crime Operation

Thames Valley Police announced on 5 January 2026 the results of 'Operation Gate', a targeted campaign against rural crime in Oxfordshire and Buckinghamshire. The operation led to several arrests related to the theft of high-value agricultural machinery and GPS equipment. This highlights a persistent and organised threat to rural businesses and estates within the corridor. Property and estate managers should review their site security, particularly access control to outbuildings and the security marking of valuable equipment.

### 4.2. Cambridgeshire Constabulary: County Lines Drug Disruption

On 6 January 2026, Cambridgeshire Constabulary confirmed a series of raids in Peterborough and Cambridge which disrupted a significant 'county lines' drug trafficking operation. While primarily a law enforcement success, the associated violence and exploitation can spill over into the night-time economy and public spaces. Businesses in the hospitality and retail sectors should ensure staff are trained to recognise the signs of drug-related activity and have clear reporting procedures in place.

### 4.3. Metropolitan Police: New Year's Eve Operation Review

The Metropolitan Police have commenced a strategic review of their New Year's Eve policing operation in central London. Initial reports indicate a successful operation in terms of public safety, but with significant resource allocation. The review will inform planning for future large-scale public events in the capital. Businesses in London's West End and other major event zones should monitor the outcomes of this review, as it will likely influence future policing postures and security requirements for public-facing venues.

### 4.4. British Transport Police: Youth Robbery and Transport Security

British Transport Police (BTP) has highlighted significant concerns regarding youth-related robbery on the London railway network, with particular relevance to the Cambridge-London-Oxford corridor given the high volume of commuter and student travel. A survey commissioned by BTP in December 2025 revealed that over two-thirds of parents and grandparents are worried that their children will be victims of robbery while travelling on the London railway network. This anxiety is grounded in data showing that 70% of robbery perpetrators and the vast majority of victims on the London railway are aged 18 or under, with most incidents occurring during peak times when young people are travelling to or from school.

Despite these concerns, BTP emphasizes that robbery remains statistically rare, with less than one robbery per million passenger journeys recorded between April 2024 and March 2025. However, following a noticeable rise in robbery offences in 2023, BTP has prioritized operations to tackle this crime type. Intelligence-driven patrols and operations have been ramped up, particularly during the festive period and into the new year, with dozens of operations across London involving hundreds of plain clothes and uniformed officers on trains and in stations. These efforts have resulted in the identification and prosecution of prolific offenders, the removal of weapons from the transport network, and a 17% reduction in robbery offences year-on-year.

The survey also revealed that nearly half of all respondents avoid holding or using their phones on station platforms and trains out of fear of theft, highlighting the impact of this crime type on passenger confidence. BTP Superintendent John Loveless has reassured the public that officers are working around the clock to keep families safe, investigating every robbery report regardless of whether victims can provide specific location details. The force has extensive CCTV coverage across the network, which is used to trace offenders rapidly. However, only half of commuters are aware that they can text BTP on 61016 to report crimes or concerns, a service that the force is actively promoting.

For organisations in the Cambridge-London-Oxford corridor, particularly those with staff or students who rely on rail travel, this intelligence underscores the importance of travel safety awareness. Employers and educational institutions should ensure that staff and students are aware of BTP's reporting mechanisms, encourage vigilance

during peak travel times, and consider providing guidance on personal security while using public transport. The ongoing industrial action affecting bus services in Cambridge, combined with severe weather warnings, may increase reliance on rail travel, making this intelligence particularly timely.

## Section 5: Protest Intelligence & Four-Week Horizon Scan (8 Jan - 4 Feb 2026)

The following table details planned protest activity with potential to impact business operations. This is not an exhaustive list. A dual-rating system has been applied based on **Risk Level** (Low/Medium/High/Critical) and **Impact Level** (Minimal/Moderate/Significant/Severe).

### Color Coding:

Date	Event	Organiser(s)	Location(s)	Risk	Impact	Considerations
17 Jan 2026	Intersectional Uprising March	Intersectional Uprising	25+ UK cities including London, Cambridge, Oxford, Manchester, Birmingham	**High**	**Significant**	High disruption. Coordinated nature implies significant disruption to transport, retail, and business operations in city centres. Review staffing levels, monitor police announcements for march routes, and prepare for access control challenges. Brief staff on de-escalation for peaceful protest engagement.
18 Jan 2026	Barclays Nationwide Action	Palestine Solidarity Campaign	Nationwide, including London, Manchester, Cambridge	**Medium**	**Moderate**	Targeted disruption. Focus on Barclays branches. Expect sit-ins and leafleting. Financial sector clients should review physical security at branch locations. Estate managers with Barclays tenants must coordinate security planning. Potential for isolated direct action.
28 Jan 2026	Windrush Rally	Roland Houslin	House of Commons, London	**Low**	**Minimal**	Localised disruption. Primarily affecting access to the Parliamentary Estate. Low risk of wider public disorder, but monitor for potential counter-protests.
31 Jan 2026	National Palestine March	Stop the War, PSC, CND UK	Central London	**Critical**	**Severe**	Severe disruption. Expected attendance of 80,000-100,000. Will cause major transport disruption across central London. Businesses should consider remote working for staff. High potential for counter-protests and public order incidents.
15 Jan 2026	Battle of Cable Street Workshop	Stand Up To Racism, Ella Baker School	Online (Zoom)	**Low**	**Minimal**	Online educational workshop on defeating narratives of division. No physical disruption to business operations. No operational impact expected.
31 Jan 2026	Keep Racist UKIP Out of Whitechapel	Stand Up To Racism	Whitechapel Station, London	**Medium**	**Moderate**	Counter-demonstration with potential for confrontation between opposing groups. Businesses in Whitechapel area should monitor for disruption. Transport delays likely around Whitechapel Station and surrounding streets.
Ongoing Jan 2026	Venezuela Solidarity Protests	Various solidarity groups	US Embassy, 10 Downing Street, London	**Low**	**Minimal**	Protests against US intervention in Venezuela. Localized to embassy and government areas. Minimal business disruption expected. Peaceful gatherings with no significant public order concerns.
Ongoing Jan 2026	Iran Solidarity Demonstrations	Iranian diaspora groups	10 Downing Street, Iranian Embassy, London	**Low**	**Minimal**	Support for anti-regime protesters in Iran. Peaceful gatherings localized to government and embassy areas. No significant business disruption anticipated.

Date	Event	Organiser(s)	Location(s)	Risk	Impact	Considerations
Ongoing Jan 2026	Palestine Action Solidarity Events	Palestine solidar ity groups	Various UK cities	**Medium**	**Moderate**	Vigils and solidarity actions supporting jailed activists on hunger strike. Some potential for direct action targeting defense contractors. Businesses in defense supply chain should review security posture.

**Note:** Additional protests scheduled after 4 February 2026 (including events on 6, 7, 11, and 21 February) are tracked separately and will be included in future horizon scans. All protest intelligence is subject to continuous monitoring and reassessment.

## Section 6: Sector-Specific Analysis & Operational Resilience

**Retail & Night-Time Economy:** The combination of organised acquisitive crime and high-impact protest activity presents a significant challenge. A review of physical security, staff training on conflict management, and robust business continuity plans for transport disruption are essential. The upcoming SIA licensing changes will require proactive engagement with security providers.

**Life Sciences & Technology:** The strategic importance of this sector, highlighted by recent partnerships, increases its attractiveness as a target for state-sponsored espionage. A holistic security approach covering physical, personnel, and cyber domains is critical. Intellectual property protection must be a board-level priority.

**University/Academia:** The need to balance an open, collaborative environment with robust security measures is paramount. Foreign interference in research and the potential for on-campus protest activity require clear policies and well-rehearsed incident management plans. The changes to hate incident recording will also require updates to internal policies and procedures.

**Property/Real Estate:** Managers of commercial properties, particularly those with high-profile tenants (e.g., financial institutions, defence contractors), must coordinate security planning in response to targeted protest threats. The findings from rural crime operations also necessitate a review of security for outlying estates.

**Professional Services & Financial Sector:** Geopolitical instability and the associated risk of retaliatory cyber-attacks are the primary concerns. A review of business continuity plans, particularly in relation to market shocks and cyber incidents, is strongly advised. The Barclays-focused protests highlight the potential for direct disruption to client operations.

## Section 7: Featured Advertisement - Fortiscan<sup>SM</sup>



### ILLuminating Security, Defining Precision

In an era of complex threats and increasing regulatory demands, traditional security solutions are no longer sufficient. The forthcoming implementation of Martyn's Law will place a significant new responsibility on

organisations to demonstrate proactive, intelligence-led security planning. **Fortiscan<sup>SM</sup>** is a next-generation security vulnerability and risk assessment service designed to meet this challenge.

Developed by Rittel Consulting, Fortiscan integrates advanced aerial survey technology with expert-led physical security analysis to provide an unparalleled, data-driven understanding of your organisation's risk landscape. Our methodology moves beyond traditional 'pen and paper' assessments, delivering a comprehensive, auditable, and actionable intelligence product.

## Key Capabilities

**Aerial Intelligence & 3D Modelling:** We utilise state-of-the-art drones to capture high-resolution imagery and create precise 3D digital twins of your assets. This allows for a comprehensive analysis of physical security measures, lines of sight, and potential vulnerabilities that are impossible to identify from the ground.

**Data-Driven Risk Analysis:** Our proprietary methodology analyses thousands of data points to identify, assess, and prioritise risks. We provide clear, evidence-based recommendations to enhance your security posture and ensure compliance with emerging standards such as Martyn's Law.

**Actionable Intelligence:** The Fortiscan output is not just a report; it is a dynamic intelligence product. We provide detailed vulnerability assessments, clear recommendations for mitigation, and a robust evidence base to support your security decision-making and demonstrate regulatory compliance.

**Operational Resilience:** By identifying and mitigating vulnerabilities before they can be exploited, Fortiscan provides a foundational layer of operational resilience, protecting your people, assets, and reputation.

## Prepare for Martyn's Law

Fortiscan is the definitive tool for organisations seeking to meet and exceed the requirements of Martyn's Law. Our service provides the evidence-based risk assessment and mitigation planning that will be essential for demonstrating compliance.

**To learn more about how Fortiscan can illuminate your security and define precision for your organisation, contact Rittel Consulting for a confidential briefing.**

*Disclaimer: Rittel Consulting Limited is not liable for the featured products or services. This advertisement is for informational purposes only.*

## Section 8: References

1. Anderson, S.R. et al. (2026) 'Making sense of the US military operation in Venezuela', Brookings Institution, 5 January.
2. Chatham House (2026) 'US intentions towards Greenland threaten NATO's future. But European countries are not helpless', 6 January.
3. National Interest (2026) 'Maduro's Capture Won't Disrupt Global Oil Markets', 6 January.
4. ABC News (2026) 'US military is 'always an option' for Trump to ...', 6 January.
5. Fox News (2026) 'Trump Greenland takeover would end NATO, Denmark ...', 6 January.
6. UK Government (2026) 'PM remarks after Coalition of the Willing meeting', gov.uk, 6 January.
7. Home Office (2025) Consultation Options Assessment: Manchester Arena Inquiry Monitored Recommendations 7 and 8. HO COA 1026.
8. Easterbrook, P. (2025) 'Protecting public safety: our latest action against training malpractice', Security Industry Authority Blog, 8 December.

9. Security Industry Authority (2025) 'A message to the private security industry for Christmas 2025', gov.uk, 19 December.
10. Thames Valley Police (2026) 'Operation Gate tackles rural crime', tvp.police.uk, 5 January.
11. Cambridgeshire Constabulary (2026) 'County lines network disrupted in city raids', cambs.police.uk, 6 January.

## Disclaimer

This intelligence briefing is provided for informational purposes only and represents the analysis and opinion of Rittel Consulting Limited. The content should not be construed as specific security advice tailored to individual circumstances. Organisations should conduct their own risk assessments and consult with qualified security professionals before implementing any security measures. Rittel Consulting Limited accepts no liability for actions taken based on the information contained in this briefing. All information is believed to be accurate at the time of publication but is subject to change.

## Copyright

**© 2026 Rittel Consulting Limited. All rights reserved.**

This document is intended for general distribution and may be shared freely for educational and informational purposes. Unauthorised commercial use or modification of this document is strictly prohibited.

*Published by Rittel Consulting | [www.rittelconsulting.com](http://www.rittelconsulting.com)*