DATA CENTRE THREAT REPORT

Global Situational Awareness

March 2026

CONTENTS

Threat Level Matrix

Overall Summary

Threat Summary - Overview

Quarterly Summary Forecast

March 2026 – April 2026 Forecast

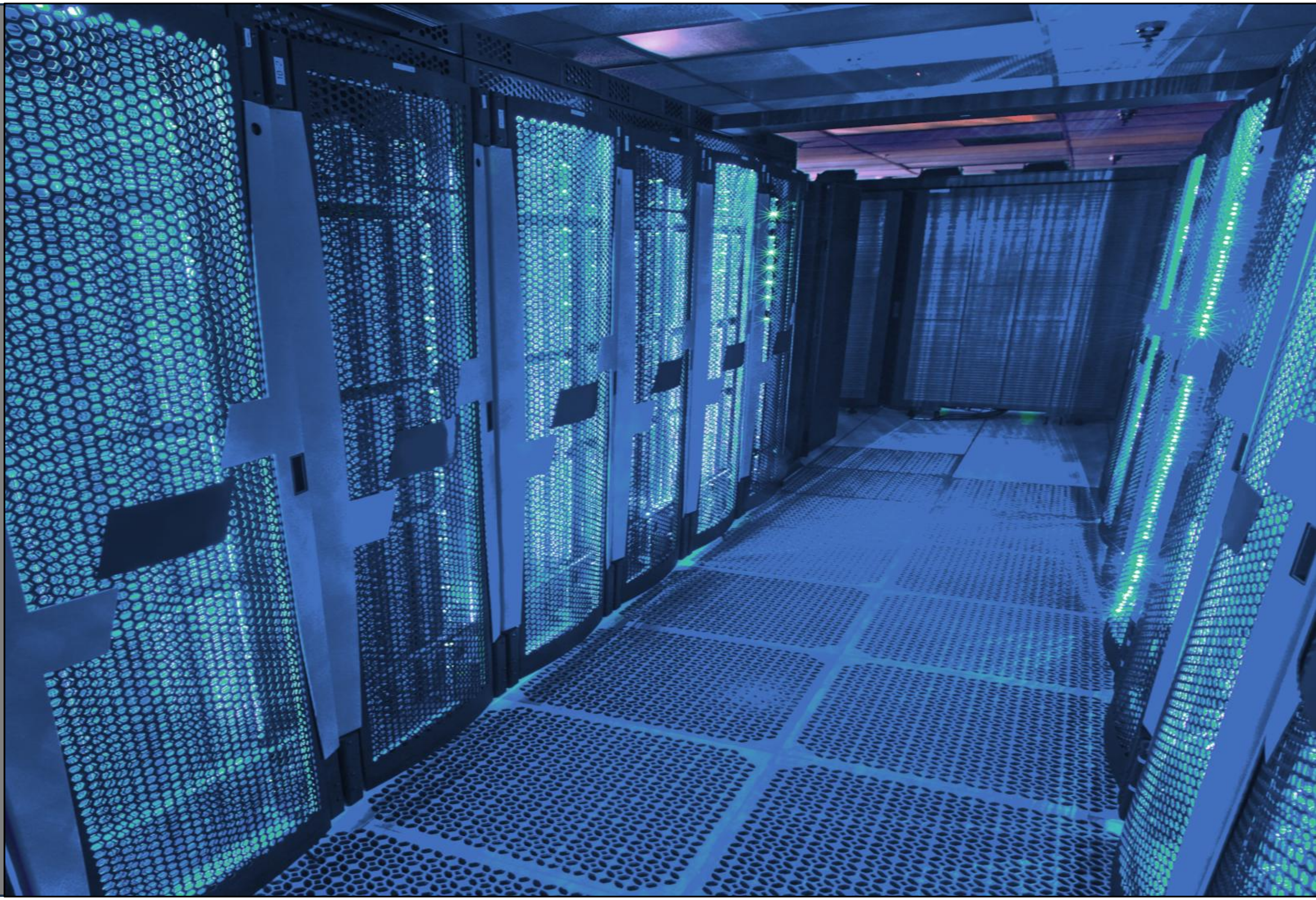
Crime Graphics

Terrorism Graphics

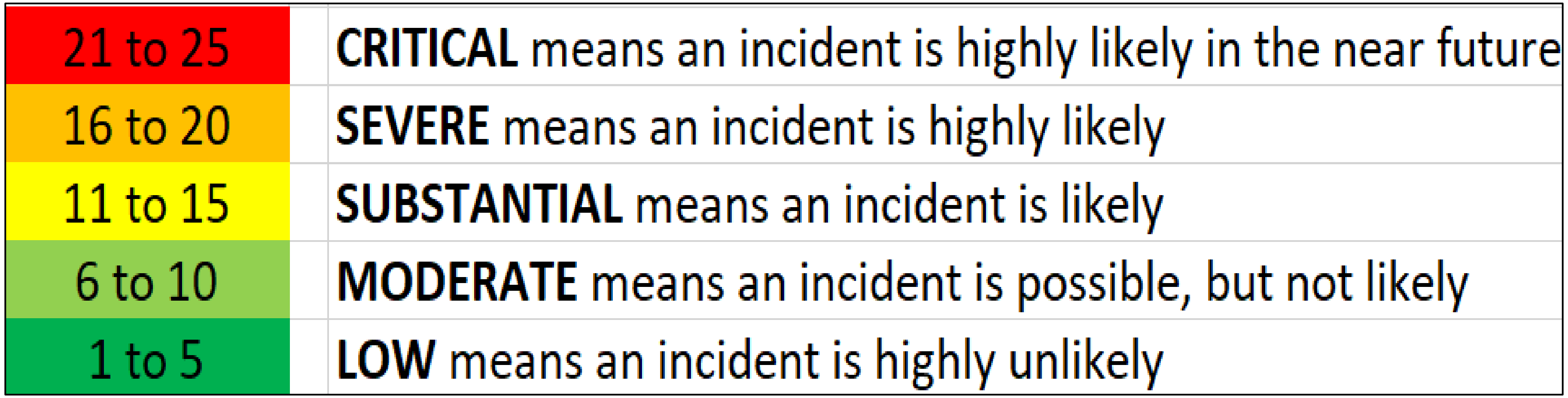
Threat Actor Graphics

Focus Issue – Data Centre Protest

Focus Issue – Middle East Conflict + DC’s

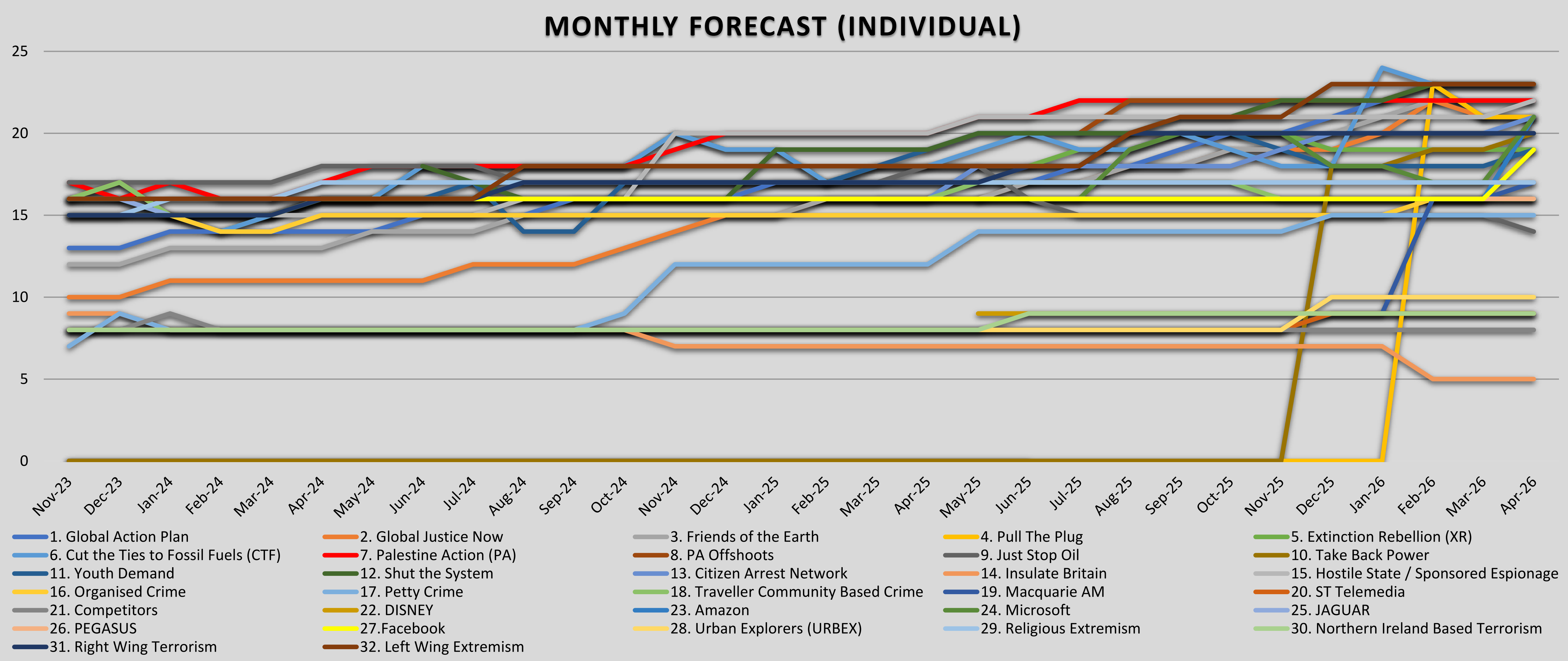


THREAT LEVEL MATRIX



21 to 25		**CRITICAL** means an incident is highly likely in the near future
16 to 20		**SEVERE** means an incident is highly likely
11 to 15		**SUBSTANTIAL** means an incident is likely
6 to 10		**MODERATE** means an incident is possible, but not likely
1 to 5		**LOW** means an incident is highly unlikely

OVERALL SUMMARY



THREAT SUMMARY - OVERVIEW

As of 17 March 2026, the threat environment remains broadly consistent with forecast expectations, with no significant deviation from projected behavioural patterns across monitored categories. Early March activity has largely validated the February outlook, reflecting seasonal operational cycles, and campaign continuation rather than abrupt shifts in intent, capability, or targeting logic.

- **Extinction Rebellion (XR)**: Extinction Rebellion maintained its threat rating of 19 throughout March 2026, fully consistent with forecast expectations and reflecting a continuation of its established seasonal operating posture rather than any escalation in disruptive capability. Activity across the month has been characterised by high frequency but low-intensity mobilisation, centred on reputational pressure campaigns, community outreach, and internal movement consolidation. The group has sustained its pattern of regular demonstrations outside corporations it accuses of contributing to climate change, particularly fossil fuel firms and associated financial or insurance stakeholders. Silent vigils targeting Shell and BP offices in London, coordinated through the Christian Climate Action (CCA) XR affiliate, exemplify this ongoing tactic, prioritising symbolic visibility over operational disruption. Beyond corporate-facing protest, February's activity calendar demonstrates the movement's continued investment in organisational maintenance and capacity-building.

- **Palestine Action (PA)**: Palestine Action retained its CRITICAL (22) threat rating into March 2026, consistent with the February forecast. The group continues to operate in a uniquely catalytic legal environment following the 13 February 2026 High Court ruling, which found the July 2025 proscription under terrorism legislation unlawful on proportionality grounds. While PA remains formally proscribed pending further government appeal, law enforcement posture has shifted to evidence-gathering rather than immediate arrests for low-level expressions of support. March monitoring indicates that PA's ideological influence, narrative mobilisation, and activation of solidarity networks remain strong, demonstrating continued operational continuity despite ongoing legal constraints. Direct-action activity has been limited by judicial pacing, but the broader operational environment remains high-intensity, validating its CRITICAL rating.

- **PA Offshoots (PA–O):** PA–O retained its SEVERE threat rating of 23 in March 2026, confirming forecast expectations, with multiple successor and proxy networks remaining highly active across the UK, demonstrating ongoing capacity for property disruption, symbolic messaging, and reputational impact. Operational pacing remains aligned with legal pressures and campaign timelines, maintaining structural stability and confirming the networks' continued ability to sustain high-intensity, ideologically motivated actions across multiple UK locations.

THREAT SUMMARY - OVERVIEW CONTINUED

Other Threat Categories:

- **Take Back Power**: Take Back Power maintained an increased threat rating of 19 in February 2026, consistent with forecast expectations, reflecting heightened operational visibility and continued mobilisation. Following January's in-person and online launch events, TBP escalated activity with a high-profile nonviolent "locked-on" protest outside Parliament on 06 February 2026, during which two supporters affixed themselves to Carriage Gate while carrying a giant papier-mâché head of Keir Starmer and displaying placards reading "Cut the Corruption." While small in scale, the protest demonstrated the group's continued capacity for highly symbolic, media-amplified interventions designed to generate reputational and political impact.

- **Youth Demand (YD)**: YD maintained a threat score of 18 in February 2026, reflecting continued subdued mobilisation following a temporary deceleration. Public-facing activity remained limited, with no notable campaigns or high-visibility interventions reported.

- **Hostile State/Sponsored Espionage** continued at a SEVERE threat level (21), reflecting sustained cyber and intelligence-gathering activity from persistent threat actors.

- **Organised Crime**, **Petty Crime**, and **Traveller Community-Based Crime** all remained consistent with projections, with threat levels at 16, 15, and 16, aligning with longer-term patterns.

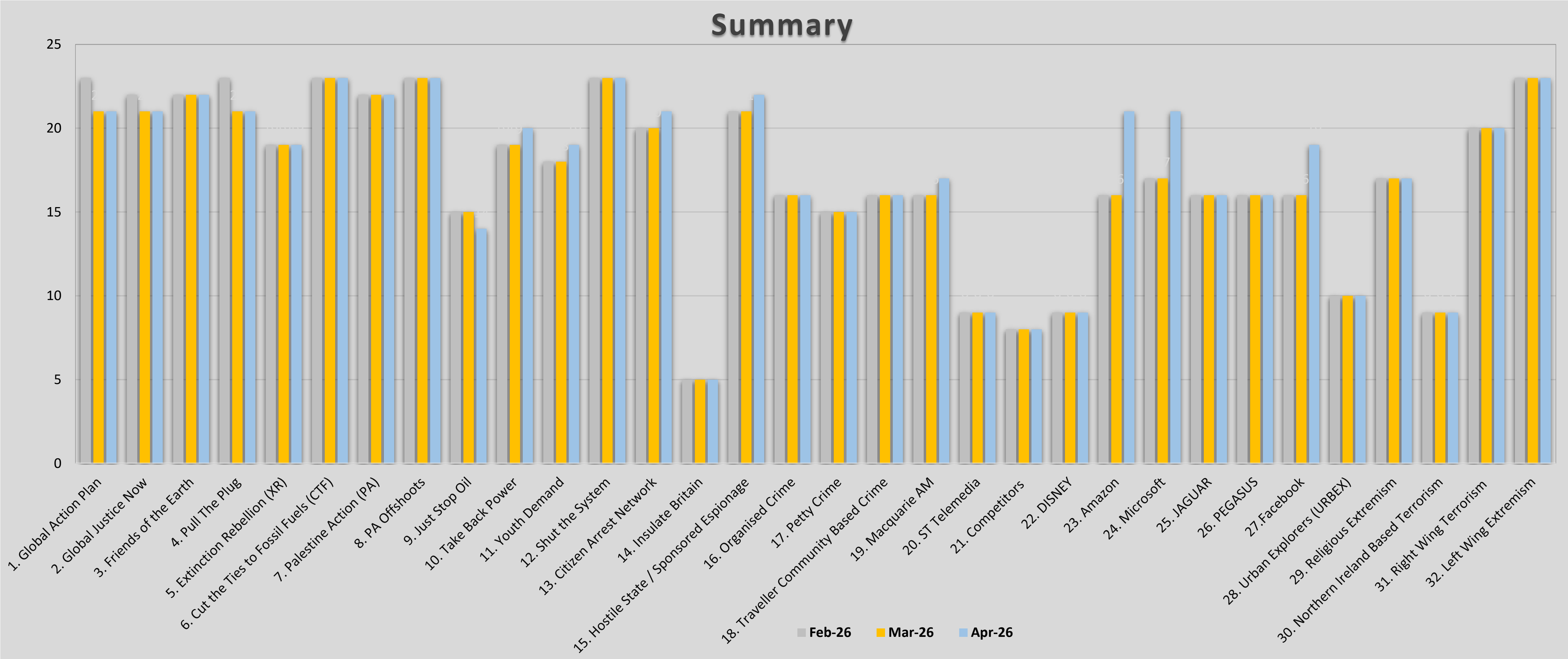
- **Religious Extremism** remained steady at 17, alongside **Northern Ireland–based Terrorism** at 9 and **Right-Wing Terrorism** at 20, all fully consistent with expectations and recent risk behaviour. **Left-Wing Extremism** also remained stable within its assessed threat band during February 2026.

- Threat levels linked to **Citizens Arrest Network**, **Just Stop Oil**, **Insulate Britain**, **Macquarie Asset Management**, **ST Telemedia**, and **Urban Explorers (URBEX)** remained steady, in line with forecast expectations and without incident-based deviations.

- Client-specific risks involving **JAGUAR**, **PEGASUS**, **Facebook, Disney, and Amazon** persisted at expected levels, with no unexpected surges or incident clusters recorded during the October 2025 period.

Overall, March 2026 has presented a stable yet high-intensity threat environment that aligns closely with forecast expectations. High-risk activism continues to be anchored by Palestine Action, PA–O, and Shut The System, while Extinction Rebellion maintained its predicted tempo and Take Back Power increased operational tempo. The recent judicial ruling for PA and the Solidarity Ecosystem, alongside coordinated PA–O activity, highlights a risk landscape dominated by decentralised operations, narrative amplification, and symbolic disruption rather than sudden escalation. The February picture, therefore, confirms the model's predictive accuracy, with ideological continuity and cross-movement alignment shaping the operational environment.

QUARTERLY SUMMARY FORECAST



MAR 2026 – APR 2026 FORECAST

Following the operational activity observed throughout March 2026, the forecast for April 2026 reflects targeted adjustments to threat ratings based on recent events, emergent groups, and geopolitical developments. Seasonal and organisational factors continue to moderate large-scale escalation, while decentralised networks and new entrants contribute to a complex and high-intensity operational landscape.

New Groups Added - Forecast:

Five new groups have been formally integrated into the monitoring dataset this month, now treated as a distinct monitored category. Retrospective assessment across the historical dataset has been conducted, where possible, to ensure analytic continuity:

- **Global Action Plan (GAP)**: forecasted to operate at a CRITICAL rating of 21. An established environmental NGO focused on public engagement, policy advocacy, and systemic change. Operational posture involves anti-data centre campaigns and legal actions against the rise of hyperscale data centres.

- **Global Justice Now (GJN)**: forecasted to operate at a CRITICAL rating of 21. A Long-standing NGO addressing global justice, corporate accountability, and trade justice, with advocacy and campaign networks active nationally and internationally.

- **Friends of the Earth (FoE)**: forecasted to operate at a CRITICAL rating of 21. A UK environmental NGO engaging in policy campaigns, local activism, and sustainable development advocacy.

- **Pull The Plug**: forecasted to operate at a CRITICAL rating of 21. Newly established grassroots coalition addressing AI oversight and hyperscale data centre accountability through public mobilisations and advocacy campaigns.

- **Cut The Ties To Fossil Fuels (CTT)**: forecasted to operate at a CRITICAL rating of 23. Direct-action environmental campaigner targeting fossil fuel infrastructure, including Macquarie AM-linked sites, with high-visibility protests and regulatory engagement.

MAR 2026 – APR 2026 FORECAST

Confirmed Forecast Adjustments:

- **Hostile State / Sponsored Espionage** increases from 21 to 23, reflecting heightened cyber and kinetic threat activity linked to Iran-US–Israel escalation. The adjustment accounts for both state-aligned cyber campaigns and the potential for direct attacks on critical infrastructure, including data centres and communications networks.

- **Amazon** rises from 16 to 21, following the 01 March 2026 drone attacks on AWS facilities in the Middle East, attributed to IRGC-linked actors. The adjustment reflects elevated geopolitical risk, the potential for further infrastructure disruption, and the IRGC's designation of the company as a “legitimate target” for military strikes, with broader implications for American-linked technology providers operating in the region.

- **Microsoft** increases from 17 to 21 due to the 11 March 2026 IRGC designation of the company as a “legitimate target” for military strikes. The adjustment accounts for heightened regional and cyber risk, as well as the potential for attacks on associated data centres and infrastructure.

- **Citizen Arrest Network (CAN)** increases from 20 to 21, reflecting March’s public media interventions targeting water companies and the anticipated near-term continuation of direct-action campaigns. The adjustment accounts for the group’s growing operational visibility and persistent ideological messaging.

- **Take Back Power (TBP)** increases from 19 to 20 for April 2026, reflecting March’s coordinated supermarket redistribution actions, the likelihood of ramped-up direct-action activity as weather improves, and growing public visibility. The adjustment accounts for the group’s tactical escalation from symbolic interventions to materially impactful campaigns, including high-visibility redistribution efforts, narrative amplification, and engagement with civil society audiences.

- **Facebook** rises from 16 to 19, reflecting Iranian threats targeting US-linked technology providers and the associated escalation of geopolitical and operational risk in the Middle East.

- **Youth Demand (YD)** rises from 18 to 19, while maintaining a low-intensity operational posture with continued focus on training and organisational development; historical patterns suggest the potential for small-scale, high-visibility interventions in April, consistent with the group’s previous month-long protest in London, though no confirmed public-facing actions have yet been observed.

- **Macquarie AM** increases from 16 to 17, reflecting ongoing operational and reputational risk following Cut The Ties To Fossil Fuels (CTT) activism targeting energy infrastructure and associated financial actors in March. The adjustment considers potential future escalation and continued monitoring of indirect impacts on linked infrastructure.

MAR 2026 – APR 2026 FORECAST

Confirmed Stability and Sustained Threats (No Changes):

- **Extinction Rebellion (XR)** to maintain a threat rating of 19, reflecting high-frequency but low-intensity mobilisation.

- **Palestine Action (PA)** is to maintain a CRITICAL rating of 22. The 13 February High Court ruling partially invalidating its proscription reinforces ideological momentum, supporter mobilisation, and operational influence through its solidarity ecosystem.

- **PA–O offshoots** forecasted to operate at a CRITICAL rating of 23, with operational capability and ideological persistence remaining high, confirming structural stability and ongoing risk.

- **Shut The System (STS)** to maintain a CRITICAL rating of 23, with previous actions and coordinated campaigns demonstrating sustained capability for symbolic property damage, narrative amplification, and reputational impact.

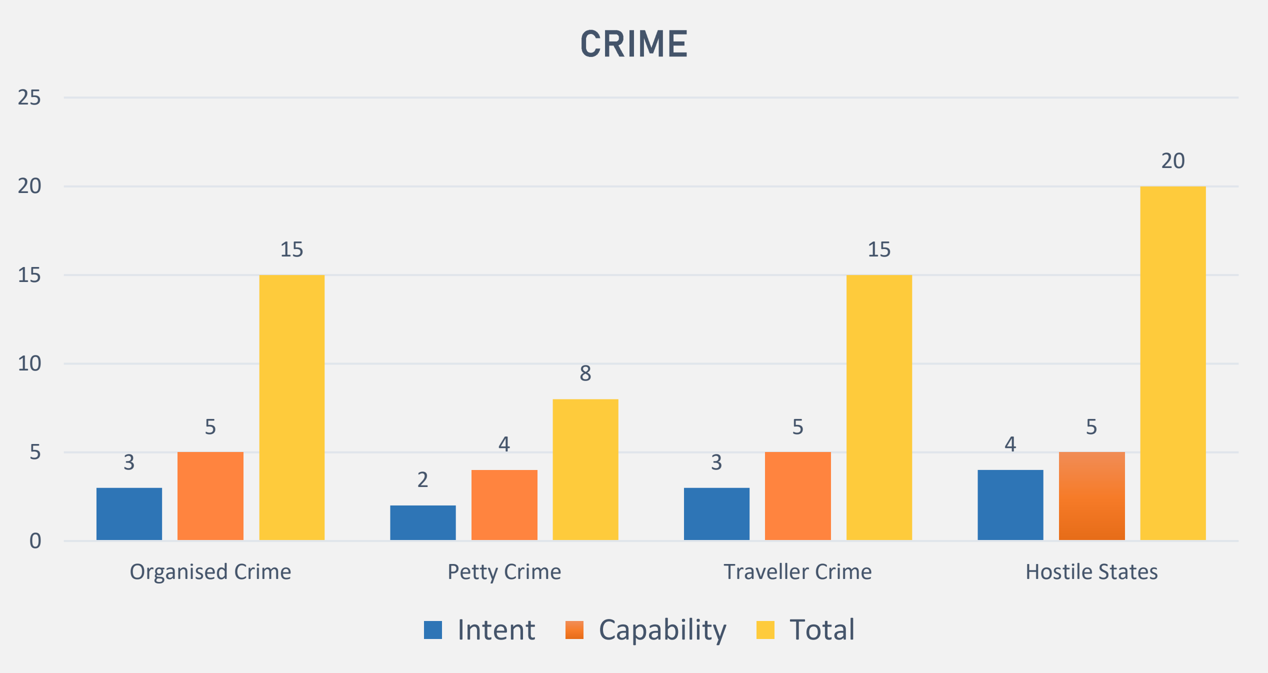
- **Left-Wing Extremism (LWE)** is forecasted to remain at 23 for April 2026, reflecting the continued high operational threat from far-left anarchist and anti-tech extremist networks.

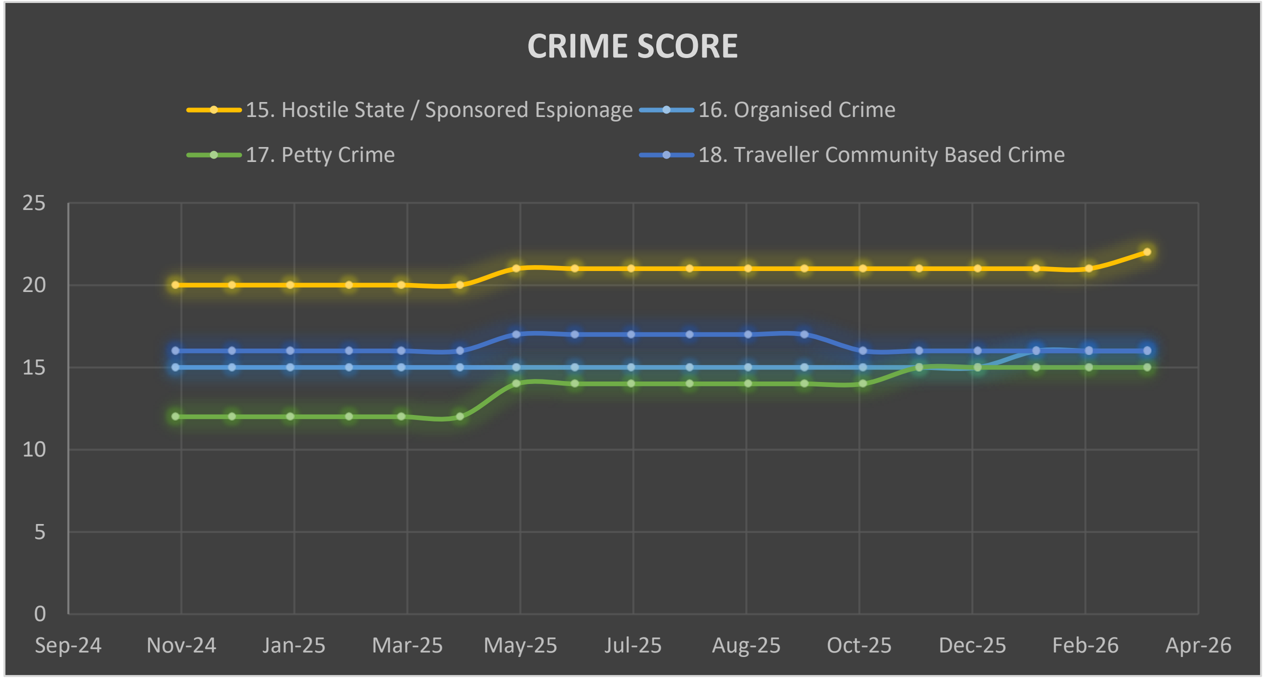
- **Traveller Community-Based Crime**, **Petty Crime**, **Competitors**, and **ST Telemedia, Disney**, **Jaguar**, **Pegasus**, **Religious Extremism**, **Northern Ireland-Based Terrorism and Right-Wing Terrorism** all maintain their current ratings. There is no credible intelligence at this time indicating imminent escalation across these entities.

Outlook:

- April 2026 is assessed as a period of sustained operational intensity across the threat landscape, moderated by seasonal, legal, and organisational factors. High-risk activity is expected from both established networks (PA, PA–O, Shut The System, TBP, Extinction Rebellion) and newly monitored groups (CTT, Pull The Plug, GAP, GJN, FoE). Geopolitical developments in the Middle East have elevated risk to technology and cloud infrastructure, reflected in increased ratings for Amazon, Microsoft, Facebook/Meta, and Hostile State / Sponsored Espionage. Operational risk remains dominated by decentralised, small-cell interventions, narrative amplification, and symbolic disruption, with potential for further escalation in corporate, infrastructure, and socio-political domains.

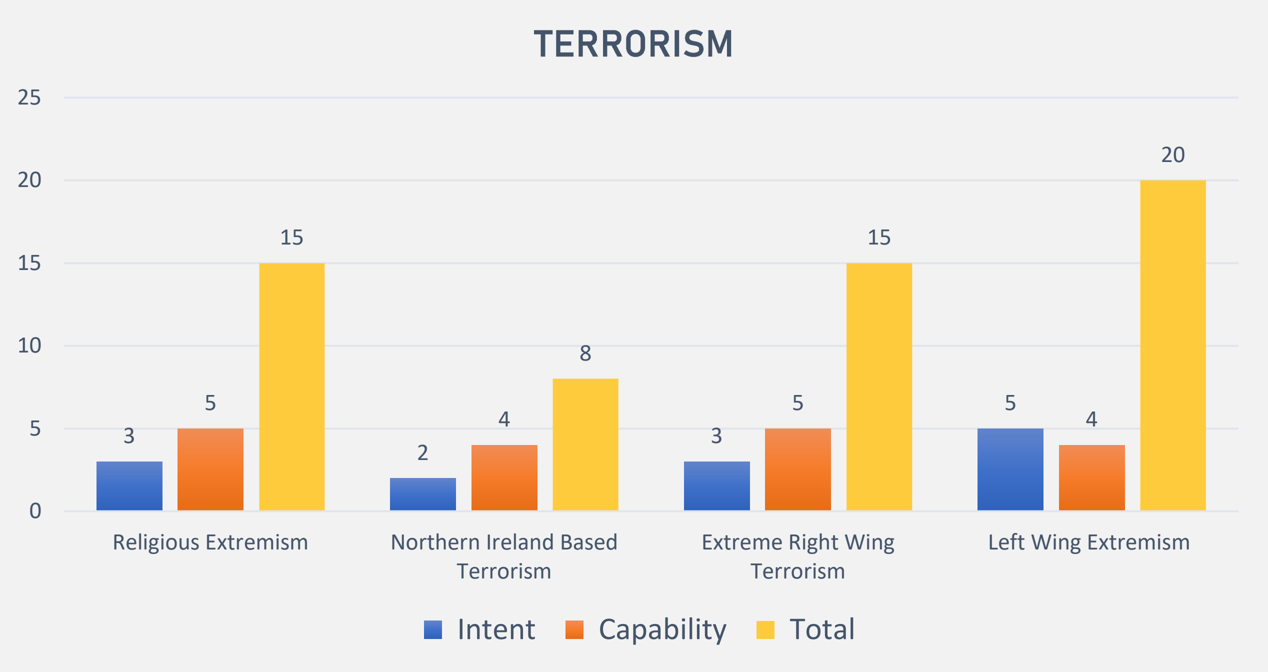
CRIME GRAPHICS

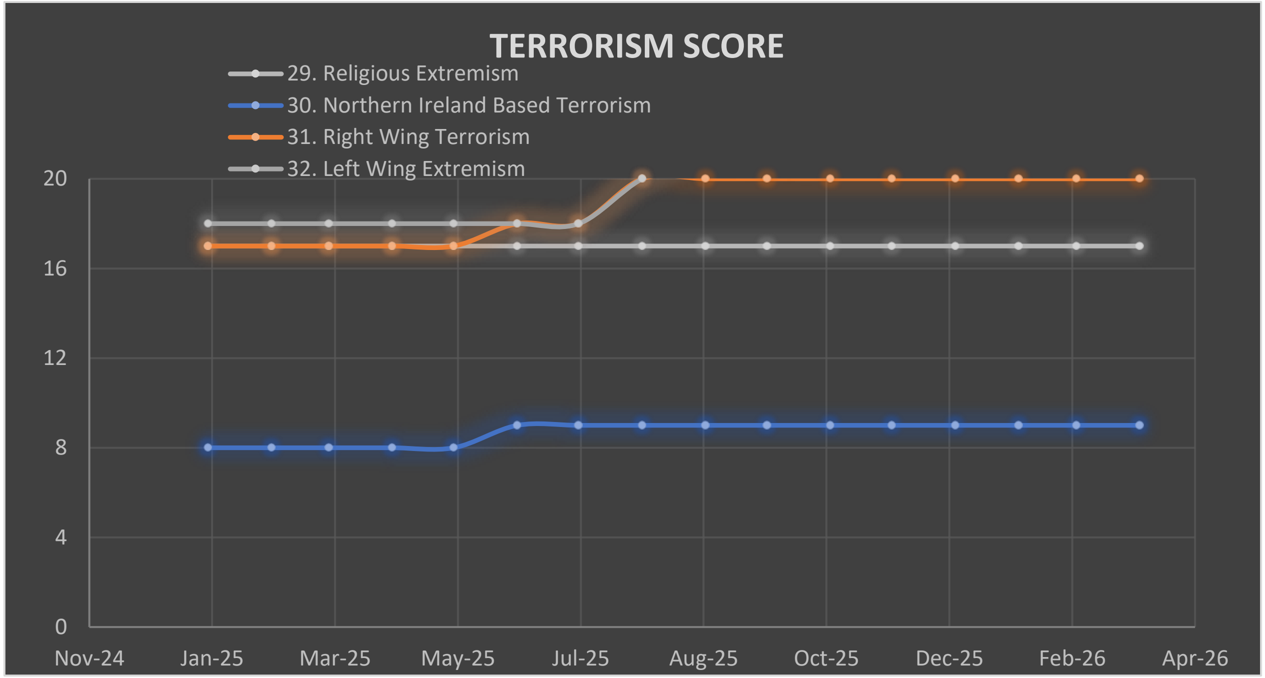




- Organised Crime, Traveller Crime and Hostile States share the highest total threat score (15), indicating significant concern.
- All demonstrate extensive capability (5), suggesting well-established networks and resources.
- Organised Crime and Traveller Community-Based Crime both maintain substantial overall threat scores, with Hostile States maintaining a Severe threat score.

TERRORISM GRAPHICS

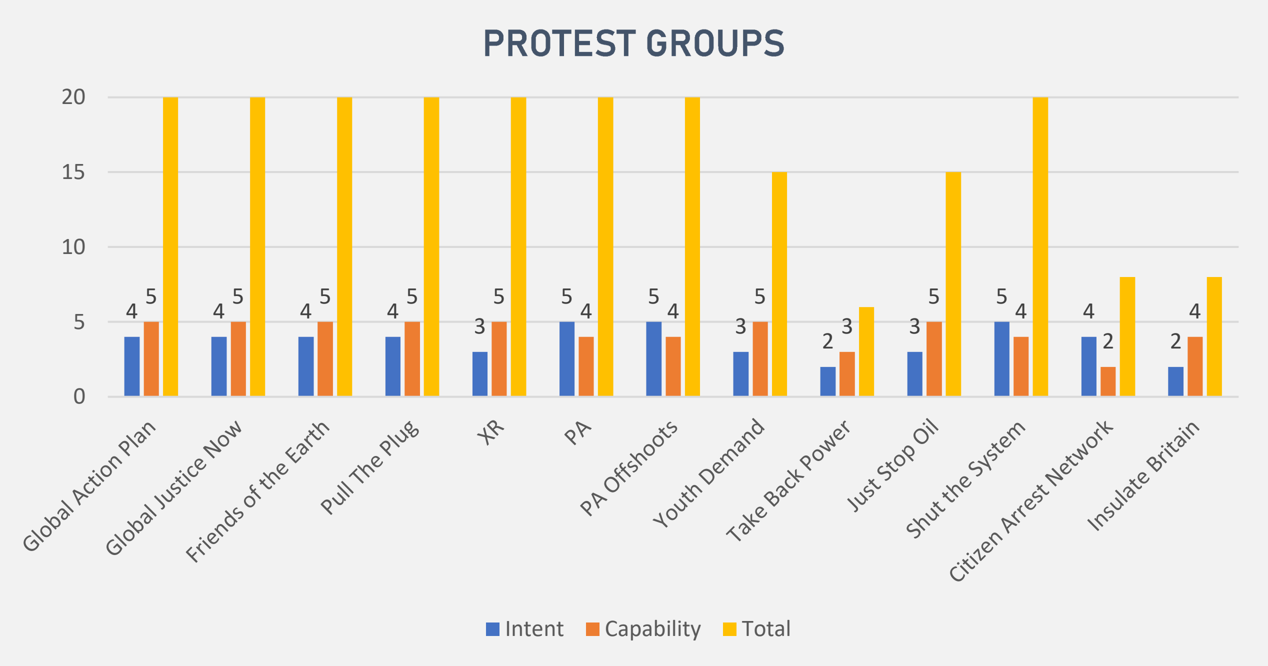


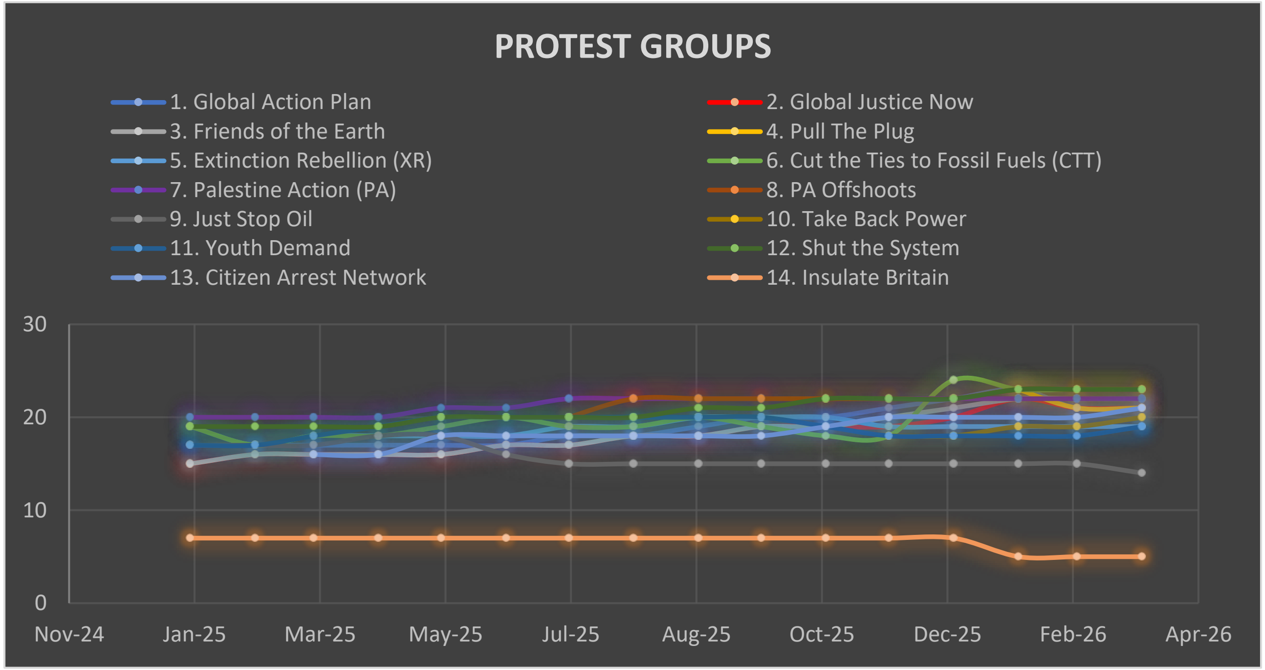


- Both Religious Extremism, Right-Wing Terrorism and Left-Wing Extremism show a concerning upward trend, highlighting the expanding scope and intensity of ideologically driven threats.

- Northern Ireland-based terrorism remains at a MODERATE threat level of 9, indicating a stable but ongoing concern. This aligns with the UK government's assessment and suggests that while not escalating drastically, this threat requires continued vigilance.

THREAT ACTOR GRAPHICS





- Palestine Action (PA), PA Offshoots and Shut the System all score 20 while Extinction Rebellion, Youth Demand, and Just Stop Oil all score 15 (Intent: 3, Capability: 5). These groups demonstrate a high capability to execute their objectives, coupled with a determined intent.

- Most protest groups are forecast to remain stable going into April 2026, with no immediate indicators of significant escalation. While operational output varies across actors, most retain resilient infrastructure and ideological momentum, sustaining the potential for rapid reactivation if strategic or situational triggers emerge.

- Citizen Arrest Network and Insulate Britain both score 8. Overall, all actors demonstrate advanced capabilities, albeit with less pronounced intent.

FOCUS ISSUE – DATA CENTRE PROTESTS

On 27–28 February 2026, the UK witnessed coordinated environmental and technology-focused demonstrations under the banners of #StopDirtyDataCentres and "March Against the Machines." The campaigns represented a significant mobilisation of both established NGOs and grassroots networks, with organisers highlighting concerns over hyperscale data centre expansion, AI governance, and environmental sustainability.

Stop Dirty Data Centres – Nationwide Protests

The environmental charity Global Action Plan (GAP) coordinated the #StopDirtyDataCentres campaign, bringing together local residents' groups and national NGOs including Global Justice Now (GJN), Friends of the Earth (FoE), Biofuel Watch, Corporate Europe Observatory, London Mining Network, and Pull The Plug. Protests focused on the environmental impact of hyperscale data centres, emphasising electricity demand, water usage, greenbelt development, and climate implications.

Confirmed actions included a flash mob and photo call in Iver Heath (Buckinghamshire), engagement outside Dame Alice Owen's School in Potters Bar, a Havering Day of Action, and events in Scotland targeting sites near Edinburgh. Campaigners framed messaging around planning law, environmental protection, and community consultation, highlighting the risks of rapid data centre expansion to UK net-zero commitments. Attendance ranged from small local gatherings to several hundred participants in urban centres, including London, and the events remained largely peaceful, featuring marches, leafleting, and public engagement rather than direct action or property interference.

The protests demonstrated an emerging capacity for national coordination among environmental NGOs and grassroots coalitions, signalling a shift toward integrated activism targeting the environmental footprint of digital infrastructure. While immediate disruption to critical infrastructure was minimal, reputational and planning pressures on developers and local authorities are likely to increase, reinforcing the importance of monitoring these networks in the context of future regulatory and planning challenges.

FOCUS ISSUE – DATA CENTRE PROTESTS

March Against the Machines – London AI Protest

On 28 February 2026, Pull The Plug hosted what they stated was the UK’s first mass AI-focused demonstration, dubbed the “March Against the Machines,” with an estimated attendance of up to 500 participants. The march brought together advocacy groups including Pause AI, Mad Youth Organise, Blaksox, and Assemble, calling for democratically controlled AI development and binding Citizens’ Assemblies to guide policy decisions.

The protest involved a route through Central London, stopping at the offices of OpenAI, DeepMind, Meta, and Google, and culminated in a People’s Assembly deliberation on AI governance. Participants emphasised the societal, environmental, and economic risks of unregulated AI, highlighting threats to mental health, public infrastructure, and employment. Speakers included prominent academics, campaigners, and legal experts, with messaging framed around democratic oversight, corporate accountability, and public participation in AI policy.

The March Against the Machines represents the largest AI-focused demonstration in the UK to date and demonstrates Pull The Plug’s ability to organise large-scale, public-facing mobilisation. Actions were symbolic, highly visible, and media-oriented, emphasising advocacy and public engagement over direct disruption. The event underscores the growing integration of AI governance campaigns with broader environmental and technology activism, reflecting an evolving landscape of protest networks capable of high-visibility national coordination.

FOCUS ISSUE – MIDDLE EAST CONFLICT AND DATA CENTRES

On 11 March 2026, Iranian state-affiliated media, including Tasnim News Agency, reported that the Islamic Revolutionary Guard Corps (IRGC) had designated multiple US technology and cloud infrastructure facilities across Bahrain, Israel, Qatar, and the United Arab Emirates as “legitimate targets” for retaliatory strikes. The announcement follows the 01 March 2026 drone attacks on Amazon Web Services (AWS) facilities in the UAE and Bahrain, which caused structural damage and disrupted regional cloud services. The IRGC framed these sites as “enemy technology infrastructure,” highlighting the strategic importance of cloud and AI facilities to US and Israeli military and intelligence operations.

The targeted facilities include offices, cloud data centres, research laboratories, and AI development hubs belonging to Amazon, Microsoft, IBM, Google, Nvidia, Oracle, and Palantir Technologies. Specific locations cited include Amazon offices and AWS infrastructure in Israel, Bahrain, and the UAE; Microsoft campuses in Israel and Dubai; Google regional offices in Dubai, Doha, and Tel Aviv; Nvidia R&D and operations centres in Haifa, Tel Aviv, and Dubai; Oracle regional hubs in Jerusalem, Abu Dhabi, and Dubai; IBM AI and cybersecurity centres across the Gulf and Israel; and Palantir offices supporting government and defence clients. The targeting explicitly identifies companies perceived as supporting US–Israeli operations, reflecting a shift toward infrastructure-based conflict.

The initial AWS strikes on 01 March 2026 caused extensive disruption, triggering automated fire suppression systems, water damage to servers, and network outages. Regional banking, telecommunications, logistics, and digital services were significantly affected, impacting roughly 11 million users and temporarily halting operations of major banks, including Emirates NBD, FAB, and ADCB. The attacks demonstrate the operational consequences of infrastructure targeting, where even limited physical disruption to cloud facilities can produce cascading effects on critical services.

While data centres outside the Middle East are not physically threatened, the designation of these companies as targets elevates their cyber risk. Threat actors may exploit the situation to conduct cyberattacks, espionage, or ransomware operations, and regional operational disruptions could propagate globally due to reliance on interconnected cloud services. The announcement also serves as a psychological and deterrence measure, pressuring Western technology firms and signalling the strategic relevance of digital infrastructure in modern conflicts.

The escalation exemplifies the growing role of cloud and AI infrastructure as a battlefield, where non-traditional targets can have strategic impact comparable to conventional military strikes. Companies with regional operations are likely to increase security measures, review contingency plans, and shift workloads to alternative regions. Compnaies should monitor both physical and cyber risks, as well as potential indirect effects on global cloud services. Although direct strikes outside the Middle East remain unlikely, the overall cyber and operational threat profile for affected companies, including Amazon, Microsoft, and Facebook/Meta, has been materially elevated in this report.