CORPS RELAY

Prepared by: Mike Bluestone CSyP, Neil Shanks CSyP, Keith Denton MSyl, Nick Jones, MSyL & Sophie Purdy, MSyL

Date: April 2026

CORPS INTEL

NSSC warns Russians are targeting messaging apps

Security officials have issued warnings about a rise in malicious activity on popular messaging apps like WhatsApp, Facebook Messenger, and Signal. The UK's National Cyber Security Centre (NCSC) has reported an increase in attempts by Russian-based malicious actors to exploit these platforms, especially targeting people who have access to sensitive information or influential networks.

The NCSC has cautioned that messaging apps are increasingly being used for impersonation and social engineering to obtain information. This approach is favoured as it is usually inexpensive, hard to detect, and especially effective when targeting people who have access to sensitive information or who are key decision makers. Professional networking sites like LinkedIn often expose company organisational structures, making it easier for threat actors to carry out social engineering attacks.

The NCSC has previously attributed this activity to China-linked APT31, the Russian Federal Security Service (FSB), and Iran's Islamic Revolutionary Guard Corps (IRGC), or proxies of these organisations.

Those deemed most at risk and face a greater likelihood of attack include:
Senior leaders and executives

- Government officials and advisers
- Security, intelligence and law enforcement professionals
- Individuals supporting critical national infrastructure or major public events

Common Approach Methods

- Tricking users into sharing login or account recovery codes
- Adding controlled devices to an account without the user noticing
- Joining group chats covertly to monitor conversations
- Impersonating trusted contacts to gain credibility
- Using malicious links or QR codes to harvest credentials

Recommended Protective Measures

While no single action can eliminate risk, the NCSC stresses that practical steps used in conjunction with one another can significantly reduce risk. These measures are:

- Avoid sharing sensitive or operational information via messaging apps on personal devices
- Using approved devices and messaging services for work related communications, in line with organisational policy
- Never sharing verification codes or scan unexpected QR codes
- Enabling two step verification
- Enabling passkeys where available
- Regularly reviewing linked devices, group memberships and contacts, and remove or independently verify anything unfamiliar
- Be alert to duplicate or impersonated contacts.
- On personal accounts, use disappearing messages to limit what an attacker could access if an account is compromised, while remaining mindful of any record keeping obligation.

Spike in Fuel Theft

Petrol thefts in the UK have increased by 62% over the past year, according to BBC data. Higher prices at petrol stations have also led to more staff abuse and a rise in drive offs, with Pay My Fuel (an automated security platform used by UK petrol stations to detect fuel theft) reporting an increase from 2.1 to 3.4 incidents per station between March 2025 and March 2026.

The term “drive off” includes individuals who depart the forecourt without paying but intend to return, such as those who inadvertently forget their payment methods, as well as incidents of deliberate theft, commonly referred to as making off without payment or “bilking.” Retailers across various petrol forecourts have reported a substantial increase in fuel theft since the onset of the conflict in Iran.

Although geographical data is limited, industry reports and information from Pay My Fuel indicate that east and southeast London, Glasgow, Manchester, Leeds, and Birmingham are particularly affected areas, with drive-offs occurring three to four times more frequently in less affluent regions.

M&S Retail Director “retail crime is out of control”

Marks & Spencer’s Retail Director, Thinus Keeve, has publicly stated that retail crime in the UK is essentially “out of control.” He described a significant rise both in the number of incidents and the severity of crimes impacting the company’s stores and staff.

This follows recent incidents of large-scale disorder and retail crime in Clapham, South London, where groups of young people mobilised through social media and participated in extensive looting across multiple shops in the area, including M&S. Several arrests were made in connection with two separate incidents occurring on different days. Social media trends on platforms such as TikTok and Snapchat reportedly encouraged young people to attend, with police noting that what may have begun as an attempt at entertainment quickly escalated into significant unrest. The situation required a substantial police response, including the implementation of dispersal orders to restore order.

Although Mr. Keeve’s comments were directed at M&S, they underscore a wider sentiment within the broader retail sector, with senior leaders characterising the current situation as unsustainable.

Mr. Keeve has mentioned recent cases showing that criminals today are not just acting opportunistically but shops are being deliberately targeted by organised gangs who efficiently clear shelves of products in one single visit, feeling free from consequence. Staff feel intimidated, as previous attempts to intervene have resulted in injuries.

Although retailers, such as M&S, have allocated resources to security, technology, and information-sharing platforms, concerns remain that these efforts may not sufficiently address the extent of retail crime. The company has advocated for enhanced and consistent enforcement by police, as well as improved collaboration between police and retailers to more effectively target repeat offenders.

Plans to expand on Blitz Courts

The UK government has announced plans to expand Blitz Courts, which are designed to handle many hearings in a single day to address significant court backlogs. Blitz Courts are focused sessions where similar cases are grouped and decided over a short, concentrated period. By scheduling comparable cases consecutively, resources are used more efficiently, allowing cases to be resolved much faster.

The backlog of Crown Court cases has reportedly doubled compared to pre-pandemic levels and is expected to continue rising without intervention, with about 80,000 cases currently pending and some crime victims may not have their cases scheduled until 2030. If no action is taken, projections suggest the backlog could reach as high as 200,000 by 2035.

Under this model:

- Similar offences are grouped together, enabling judges, prosecutors, and defence teams to handle cases more efficiently
- Court sessions occur over shorter periods, which minimises delays from rescheduling and last-minute adjournments
- The approach promotes early guilty pleas, allowing cases to be resolved faster
- Prosecutors must quickly assess whether a conviction is likely, resulting in cases being either amended or discontinued

Another benefit is that Blitz Courts may encourage offenders to change their behaviour. With cases being heard more frequently, offenders can no longer rely on waiting out their court dates in hopes that victims lose interest and withdraw, resulting in collapsed cases. This shift ideally signals to offenders that there are genuine consequences for their actions, which could help deter repeat offences.

Widespread reports of broken CCTV in UK

Although the UK possesses one of Europe's most extensive CCTV networks, research suggests a significant amount of this infrastructure is non-functional or outdated, reducing the effectiveness of police investigations. As a result, these limitations are likely affecting the deterrent effect on criminal activity and behaviour.

A report from The Telegraph, showcases broader national concerns surrounding CCTV coverage. Up-to-date statistics on faulty CCTV systems are difficult to obtain, as faults are likely often unreported. However, an investigation conducted in February identified major shortcomings in CCTV operation and coverage across infrastructure such as the UK rail network. It found that hundreds of allegations of sexual harassment or assault could not be properly investigated due to CCTV failures.

The government's Biometrics and Surveillance Camera Commissioner pointed out that many current systems have been in use for decades, and the footage collected often fails to meet evidential standards required for court cases. Although CCTV technology has advanced, irregular maintenance, limited monitoring, and budget constraints faced by local authorities mean that many cameras are probably creating an unrealistic sense of security.

When information like this enters the public domain, it can be used by those who argue that CCTV systems infringe upon citizens' civil liberties. Such individuals may present this as proof that mass surveillance is no longer an effective deterrent against crime and therefore should not be deployed.

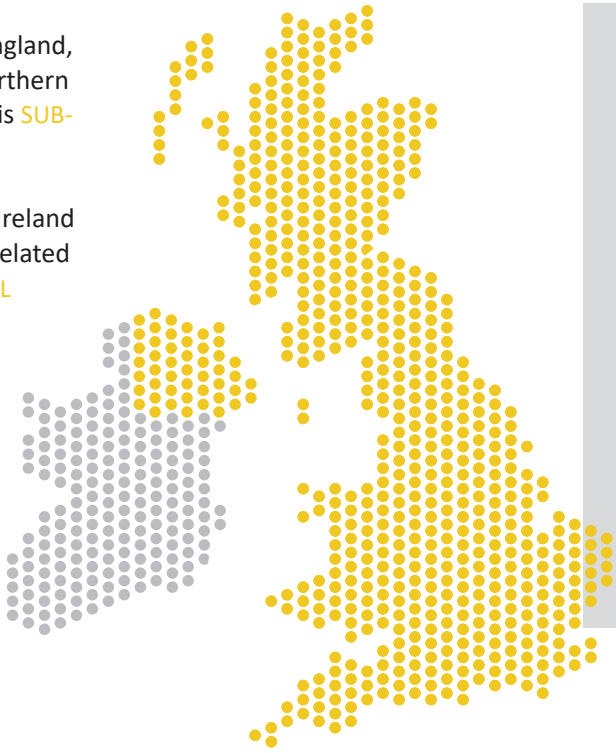
Industry and security professionals, including those in academia, still widely support the implementation of CCTV for the prevention and detection of criminal activity. However, CCTV infrastructure seemingly only acts as an effective deterrent only if cameras are operational and actively monitored. Simply having CCTV systems in place does not constitute a significant deterrent unless they remain in good working condition and are monitored effectively.

Corps Relay
April 2026

Current National Threat Level

The threat to the UK (England, Wales, Scotland and Northern Ireland) from terrorism is SUBSTANTIAL

The threat to Northern Ireland from Northern Ireland-related terrorism is SUBSTANTIAL



NOTE:

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack

LOW means an attack is highly unlikely

MODERATE means an attack is possible, but not likely

SUBSTANTIAL means an attack is likely

SEVERE means an attack is highly likely

CRITICAL means an attack is highly likely in the near future

SIA launches consultation following Section 27 of the Terrorism (Protection of Premises) Act 2025 statutory guidance publication.

The Home Office has released official guidance detailing the implementation of the Terrorism (Protection of Premises) Act 2025, also referred to as Martyn's Law.

The guidance explains:

- Which premises and events are covered
- Who is responsible
- What those responsible will be expected to do

It is designed to be accessible and straightforward, requiring no specialist security knowledge, and includes practical examples illustrating legal requirements and good practices.

In addition to publishing the Section 27 guidance, the SIA has started a consultation on its Section 12 statutory guidance, which details how the SIA plans to function as the regulator under the act. This consultation will remain open until 12th June.

The draft intends to set out:

- How the SIA plans to monitor compliance
- How it will take enforcement if required
- How it will use discretion if appropriate, to ensure a supportive and risk-based approach

Martyn's Law received Royal Assent on 3rd April 2025, with an implementation period of at least 24 months until the Act comes into force. Organisations and individuals who are likely to fall within the scope are advised to familiarise themselves with the guidance so they can consider their requirements in advance.

For Section 27 guidance under the Terrorism (Protection of Premises) Act 2025, see: https://www.protectuk.police.uk/news-views/martyns-law-statutory-guidance-published-home-office?mtm_campaign=Martyn%27s%20Law%20Statutory%20Guidance&mtm_kwd=Email.

For SIA section 12 consultation details, visit: https://www.gov.uk/government/news/sia-launches-consultation-on-section-12-guidance-for-martyns-law.

Guide, Shelter, Report Guidance Issued by NaCTSO

The National Counter Terrorism Security Office (NaCTSO) has updated its Crime Prevention Toolkit issuing the principles of Guide, Shelter, Report (GSR), a set of dynamic response principles developed to support business and organisations in responding effectively to a terrorist attack. The guidance is intended for a wide range of businesses that operate within public venues and spaces, including small and micro business.

GSR is intended for organisations located in areas accessible to the public, such as retail outlets, hospitality venues, leisure centres, transport hubs, educational institutions, healthcare facilities, and places of worship. This guidance is distributed to all staff working within any organisation. It is designed to complement the Run, Hide, Tell (RHT) guidance provided to individuals, which offers life-saving advice to members of the public during a terrorist attack. However, RHT was not created for use by organisations as their main incident response plan in the event of an attack.

The core principles applied within GSR are:

- **Guide** people away from danger
- **Shelter** people to keep them safe
- **Report** the incident to police when safe to do so

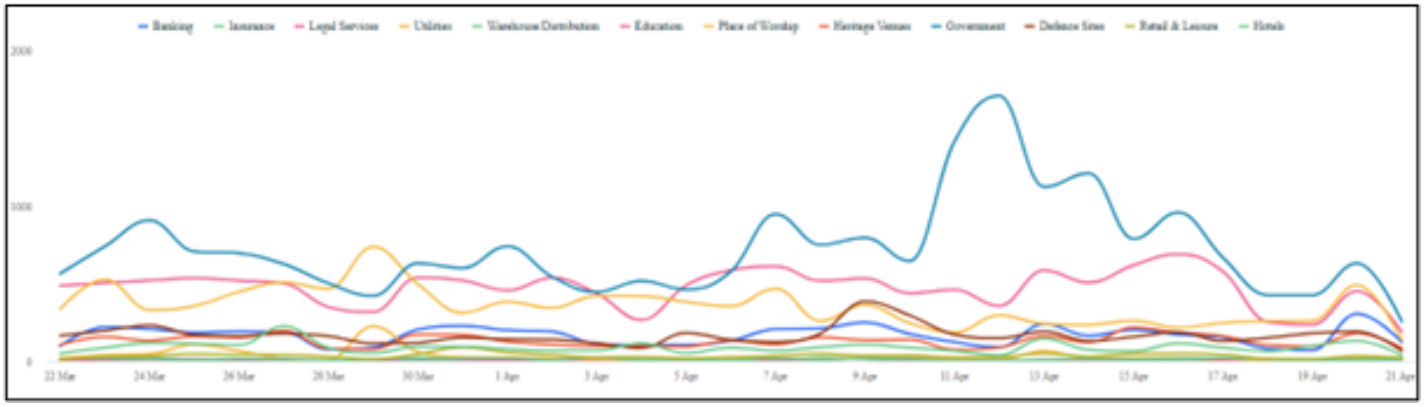
These principles are not sequential and can be applied in different orders or simultaneously depending on circumstance.

The purpose of this guidance is to assist organisations in fulfilling their duty of care obligations by facilitating a structured and coordinated response to an attack, thereby complementing the RHT personnel guidance. NaCTSO states that terrorist attacks are unpredictable, and may occur at any location, with GSR designed to help organisations prepare staff to take decisive action that may help protect life during an incident.

The full published guidance can be found here: https://www.protectuk.police.uk/gsr

Social media activism last 30 days

Activism by Sector - During the past month, social media activity related to sector activism has centred on government policy, especially after the Metropolitan Police began arresting supporters of Palestine Action again while the government appeals a high court ruling on the ban. Reports indicate that more than 500 people have been detained since these arrests resumed, with online discussions largely voicing anger at the government and disapproval of the police actions. While these opinions do not reflect everyone's views, data reveals significant online advocacy for the right to support Palestine Action following the court's decision, rather than widespread backing for the prohibited organisation itself.

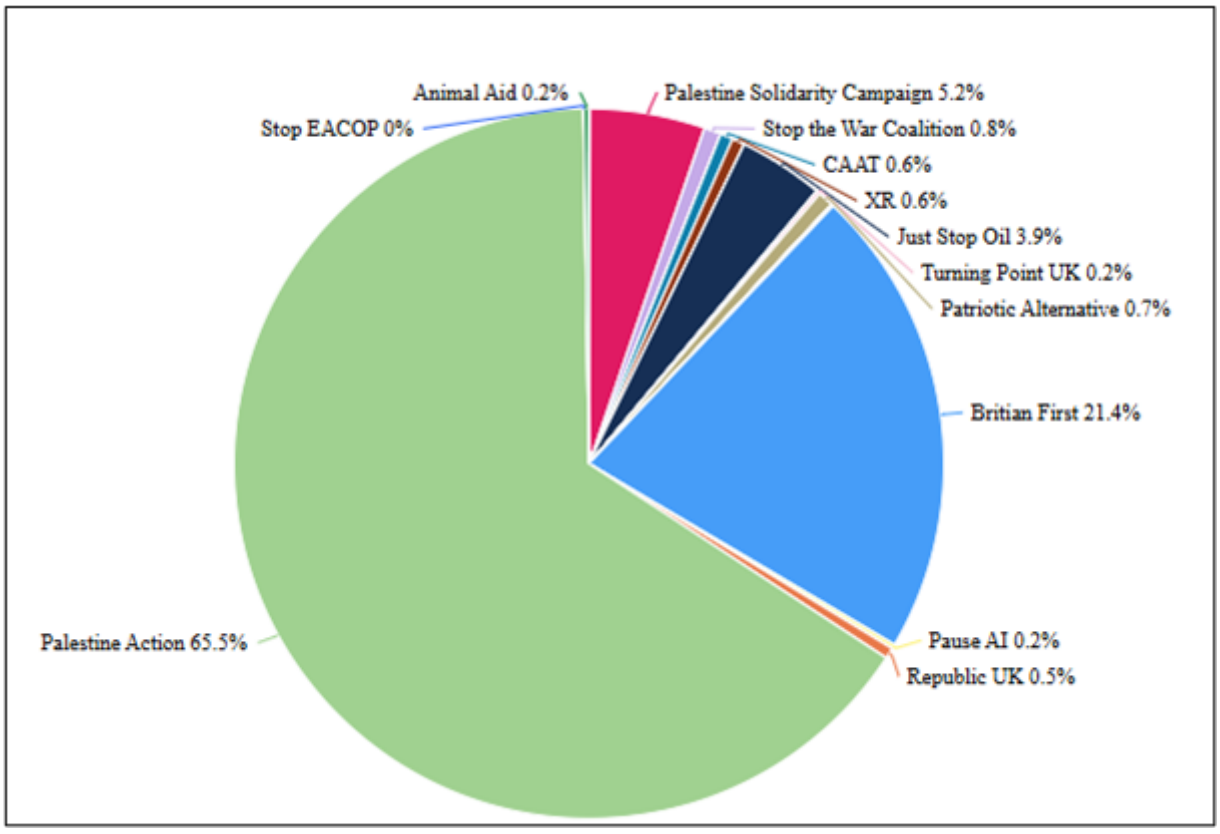


Corps Relay
April 2026

Social media activism last 30 days

Activist Groups - Following the high court ruling and the MET's decision to resume arrests of people openly supporting Palestine Action, it's not surprising that over half of social media discussions are focused on this topic. The discussions themselves don't necessarily support Palestine Action directly; instead, they mainly criticise the central government and police, often seen as one entity, for not adhering to the high court's decision. Most of the sentiment expressed is anger directed at the government rather than outright backing of Palestine Action.

Britain First continues to attract significant online engagement following its planned marches in central Manchester during the weekend of April 18th. Reactions on social media remain highly polarised. Although a larger majority of people expressed support for the organisation and its activities in Manchester, a smaller yet influential contingent voiced criticism of both the group and its demonstration. Consequently, much of the discourse surrounding Britain First has focused on critiques of its actions and public gatherings.



Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

intel@corpssecurity.co.uk
www.corpssecurity.co.uk