

CORPS RELAY

Prepared by:

Mike Bluestone CSyP, Neil Shanks CSyP,
Keith Denton MSyL, Nick Jones, MSyL &
Sophie Purdy, MSyL

Date:

December 2025

CORPS
— Est. 1859 —
SECURITY

Keyless Car Theft Devices

According to the BBC, criminal groups have been using electronic devices to steal keyless vehicles, with these tools being sold on the black market for up to £20,000. These gadgets function by relaying the signal from a key inside a property, enabling unauthorised access and ignition of the vehicle from outside. Experienced criminals can gain entry and steal a car in under two minutes.

At present, mere possession of such devices is not an offence; prosecution is only possible if it is proven that the tool was used in the commission of a specific crime (such as theft), or if the person intended to use it to commit a crime, requiring evidence of criminal intent. Legislation is currently before parliament which will criminalise the sale, use, or possession of these devices. Under the proposed law, individuals found in possession would need to demonstrate a legitimate reason, such as being an authorised vehicle mechanic, for doing so. In the past 12 months, over 100,000 vehicles have been stolen in the UK, with an estimated 60-70% being keyless models. Organised crime syndicates are reportedly deploying these devices themselves or providing them to others, often concealing them as Bluetooth speakers. Some of these

tools are also capable of disabling vehicle tracking systems through signal jamming technology, meaning that once stolen, the vehicle can no longer be traced.

The Master Locksmith Association gives the following steps for preventative measures:

- Keeping car keys away from the front door and in a signal blocking pouch, such as a faraday bag to prevent such a device from gaining a signal.
- Wireless signals on some key fobs can be switched off – look at your user manual to see if this can be done on a keyless vehicle.
- Steering wheel lock – many modern car thieves do not carry heavy duty equipment for mechanical devices such as a steering wheel lock which can physically prevent the removal of the vehicle.
- Blocking a keyless vehicle behind a physical barrier, such as another car, if driveways allow.

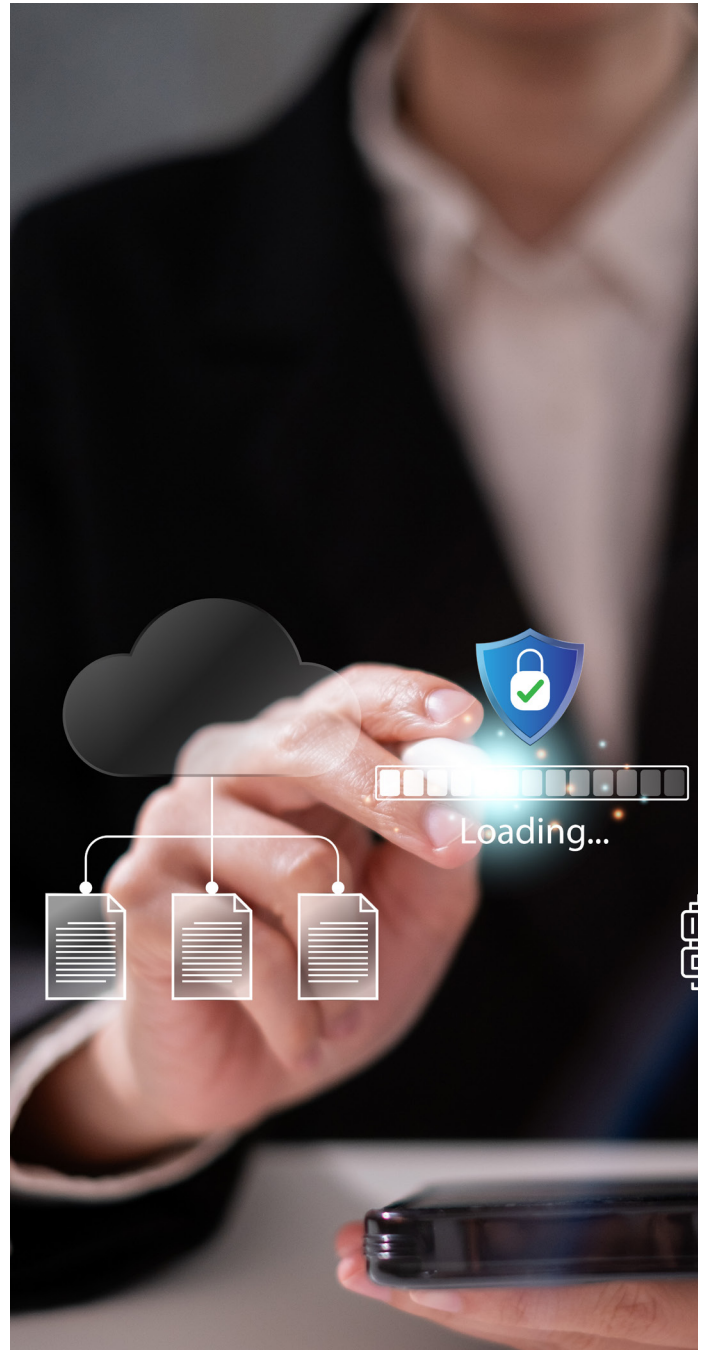


Investigation reveals that X favours right wing algorithms

A recent Sky News investigation examined the political discourse present on the social media platform X, using nine newly created neutral accounts to analyse the platform's algorithm. The investigation noted that X now charges approximately £3,800 per month for access to its API, a tool allowing large-scale data downloads, which was previously available at no cost.

The accounts established for the investigation were designed to equally represent left-leaning, right-leaning, and neutral perspectives, without any specific political affiliation. Over a two-week period, more than 87,000 posts were reviewed. An AI tool classified these posts by political leaning and level of extremism; its accuracy was validated through sample checks conducted by human experts. The tool achieved a 93% success rate in determining left or right political orientation and a 97% rate in identifying whether a post was political. Of the posts evaluated, about 60% were categorised as right-wing, 32% as left-wing, and 6% as neutral, with the rest uncategorised. The investigation suggested that following Elon Musk's acquisition of the platform, who is widely perceived as having right-leaning views, many users with left-leaning perspectives may have migrated to alternative platforms such as Bluesky, therefore there was less overall left leaning engagement from users. Furthermore, the study highlighted that although left-leaning politicians tended to post more frequently, their content appeared less often in the algorithmic feed compared to right-leaning politicians, who were overrepresented.

While the UK Online Safety Act empowers Ofcom to investigate illegal content, it does not require enforcement of political balance. The analysis concluded that even without active engagement, users with varying political perspectives are likely to be disproportionately exposed to right-wing content on the platform.



Independent commission finds UK's Prevent Counter-Terrorism Strategy is 'no longer keeping the country safe'

A summary of findings from an independent commission into the UK's counter-terrorism measures has concluded that the current Prevent strategy 'is no longer keeping the country safe'.

The commission's findings – based on a three-year review – also added that the strategy is 'not fit for purpose' and needs a 'radical overhaul'. It said that 90% of those referred to the scheme are turned away because they have no obvious ideology, despite some going on to commit violent crimes. More than 58,000 people have been referred to Prevent since 2015, but more than 90% of these had no counter-terrorism concerns, the remaining 10% showing no evidence of criminal activity. The commission also reports that most referrals are children and young people, despite only comprising 21% of the UK population.

The recent case of Axel Rudakubana – the Southport murderer who stabbed three young girls to death and attacked several others in July last year – was cited as a prime example of the scheme's inadequacy. Mr Rudakubana had previously been referred to the Prevent scheme three times, but had his case closed in 2021 due to no evidence being found of a 'fixed' ideology - he subsequently went on to commit the atrocities in Southport only three years later.

The commission, chaired by Sir Declan Morgan, a former chief justice of Northern Ireland, has subsequently made several wide-ranging recommendations to the government, including:

- Narrowing the definition of what constitutes terrorism in order to provide greater clarity – stating "Terrorism should be defined narrowly as acts intended to

coerce, compel, or subvert government or public institutions, and the threshold for property damage should apply only to conduct causing serious risk to life, national security, or public safety, or involving arson, explosives, or firearms methods inherently capable of causing unpredictable harm".

- Proscription reviews - decisions made by the government to proscribe organisations (such as the recent proscription of pro-Palestine activist group Palestine Action) to be reviewed every five years to ensure proportionality.
- A radical overhaul of Prevent to "make it part of a broader initiative dealing with violence and no longer based on a flawed radicalisation model" – after finding that there is no evidence that radicalisation is a predictor of whether a person will become a terrorist. "Prevent needs a major overhaul and integration into a wider system to which all those susceptible of being drawn into violence can be referred," it said. This was described as a 'single access point' that would be the first step for concerns about the susceptibility of individuals to being drawn into violence. Those at risk of involvement in terrorist violence would then be passed to Prevent, while others would be dealt with by different agencies.

Full details of the commission's findings were unveiled at the Royal United Services Institute (RUSI) think tank in London on Tuesday 11th November.

MI5 warns MPs over Chinese espionage attempts via LinkedIn

MI5 has issued a warning to MPs, peers, and parliamentary staff about Chinese intelligence services attempting to infiltrate UK political circles via LinkedIn. The alert explained that LinkedIn accounts often in the guise of networking, are likely to target junior staff members who might not recognise the threat or consider themselves likely targets. These contacts aim to gather small pieces of information to assemble a larger intelligence picture - a long-term approach. Two LinkedIn accounts tied to Chinese security services were identified.

This incident spurred concerns in the House of Commons regarding China, particularly around a reliance on Chinese built technology. Investigations in Norway and Denmark found that Chinese made buses could theoretically be shut down remotely by the manufacturer due to an installed "kill switch". In response, the UK's National Cyber Security Centre (NCSC) is working with the Department of Transport to evaluate the risk domestically, and the use of these buses within the UK. Furthermore, the Ministry of Defence has banned Chinese electric vehicles from sensitive military locations, and defence companies like BAE Systems and Lockheed Martin have advised employees not to connect their phones to Chinese EVs.

While embedded Chinese technology is a significant concern for the government, quick mitigations for technical espionage can be used, like those highlighted by the MOD, although easier said than done.

What the findings do underscore is the increasing use of social engineering for espionage. While not a new tactic, social engineering remains effective because, despite efforts to secure social media and fortify systems through cybersecurity, apps like LinkedIn exploit the human element as a point of vulnerability. LinkedIn, unlike Facebook or Instagram, encourages users to connect with strangers, making unsolicited messages seem normal. Many profiles, including those belonging to senior executives, often reveal details people would not typically share elsewhere, such as location, travel plans, professional relationships, emails and phone numbers. Even seemingly trivial bits of information can contribute to a broader intelligence-gathering effort.

State-sponsored espionage is methodical and patient, often unfolding over years, with foreign intelligence services collecting minor details before making overt approaches. When networking on such platforms, it is crucial to verify the identity of your contacts and ensure their legitimacy before sharing any information, however harmless it may appear.

M&S Profits significantly affected due to Cyber Attack

A major cyber-attack that forced M&S to suspend online orders for nearly two months and click-and-collect for almost four over the summer, has cost the company an estimated £300 million. Although the company expects to return to profitability by Christmas, the incident demonstrated how vulnerable even established organisations are to cyber threats. The company was forced to increase IT spending and staffing, while in-store sales declined due to customer uncertainty. Meanwhile, competitors like Next benefited, seeing a 10% increase in sales during the disruption. This event underscores the substantial risks cyber-attacks pose to businesses and again the use of social engineering and technical know-how to infiltrate a business. Hackers first called the IT help desk pretending to be legitimate support staff, successfully

deceiving third-party contractors into resetting passwords. Once granted access to internal systems, they deployed ransomware. This incident highlights the real threat organisations face not only from espionage but also from criminals who exploit human behaviour to gain trust. Passwords should never be reset or access given solely based on a phone call or email - additional verification is essential. It's important to watch out for urgent requests and pressure tactics, as criminals may use knowledge of company executives' identities (often sourced from LinkedIn) to intimidate and pressure employees into releasing information.

Action Fraud replaced by Report Fraud

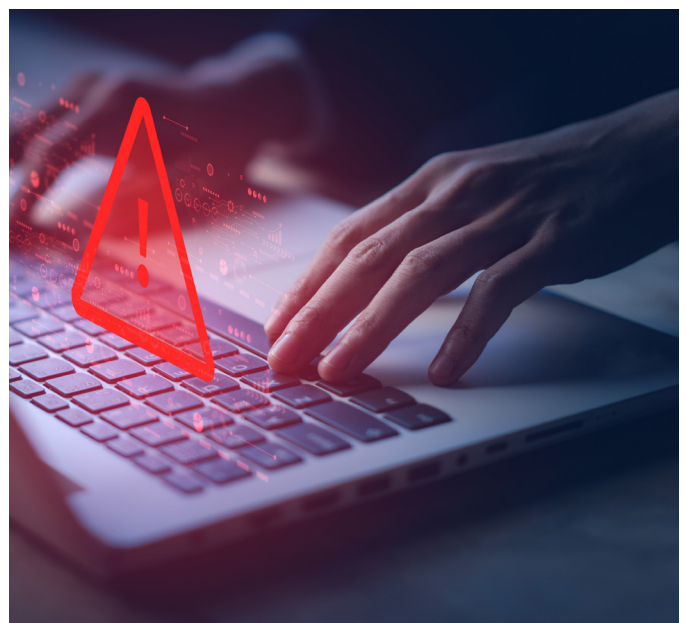
The City of London Police has launched a new way to report fraud, with the new service aimed at improving experience for victims and to provide fast and more efficient intelligence to police. The new system will aim to:

- Speed up analysis and sharing of reports.
- Improve victim support.
- Provide police with better quality data.

Action Fraud previously faced criticism for its poor user experience and delay in passing police intelligence. Over the next few months, traffic reported to the old Action Fraud site will be automatically redirected while data is migrated over.

Victims can report cybercrime and fraud via:

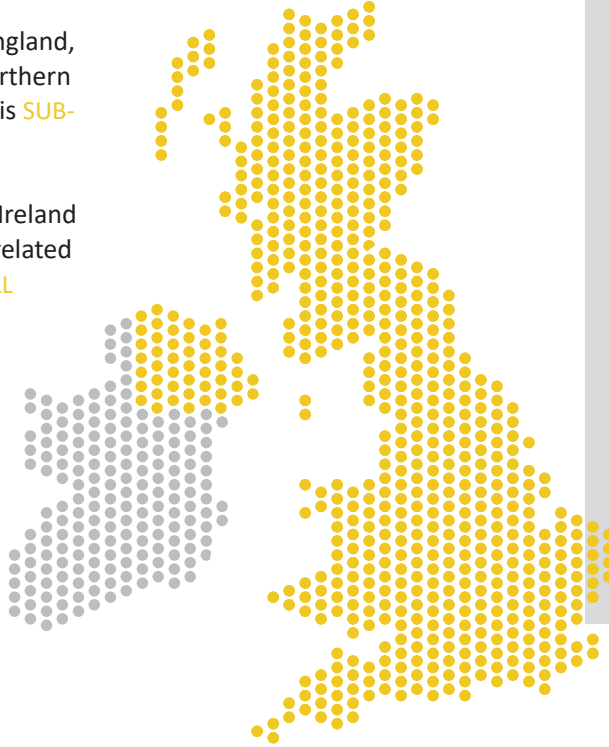
- Website: reportfraud.police.uk
- Phone: 0300 123 2040 (same number as before)



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

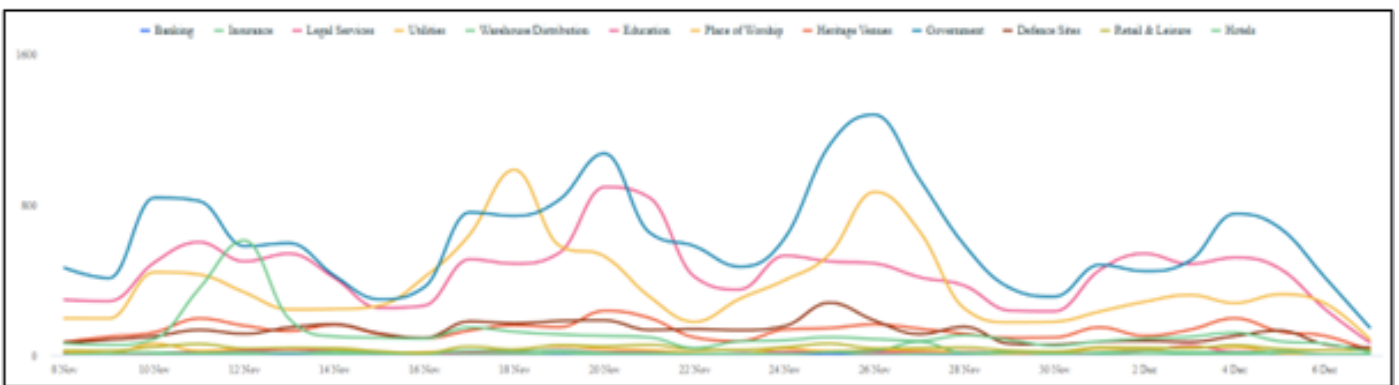
CRITICAL means an attack is highly likely in the near future

Social Media Monitoring

Industries & Activism

The Defend Our Juries: Lift the Ban movement, active throughout November, attracted significant public discussion about the government, especially during the high court's judicial review of the ban on Palestine Action. Throughout the month, many activists visibly supported Palestine Action physically at demonstrations, leading to further mass arrests across the country. Those engaging

with this content continue to express strong anger toward the government, largely supporting the demonstrations themselves rather than Palestine Action itself. Additionally, social media users are frustrated with police responses, questioning why some forces have not arrested supporters of Palestine Action while others enforce a zero-tolerance policy. This disparity has fuelled further online resentment toward the government.

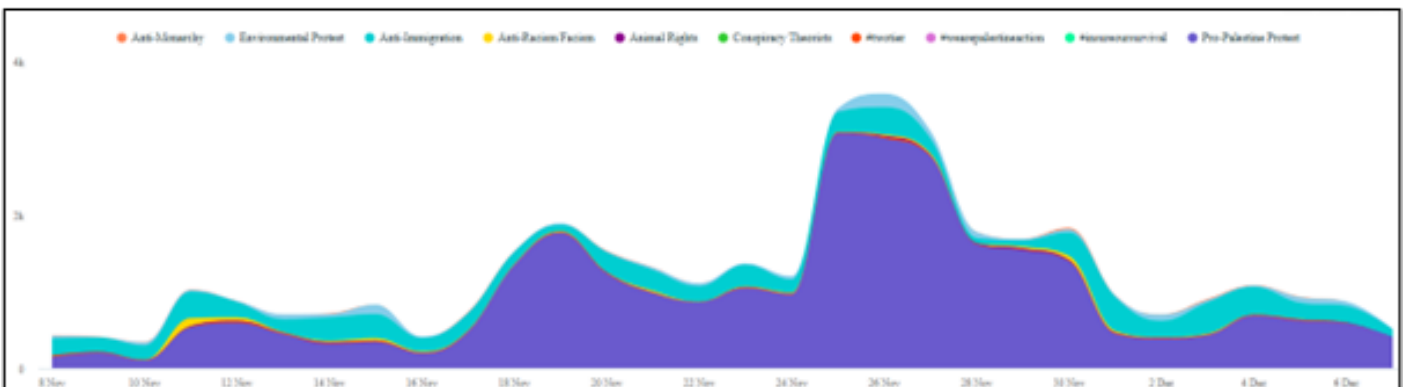


Activism Events and Movements

During the past month, activism has predominantly focused on Pro-Palestine protests. Much social media activity has concentrated on the Defend Our Juries: Lift the Ban demonstrations. The most significant spike in the volume of online discussions increased during the High Court judicial review. Over the last 30 days, content related to mass Pro-Palestine demonstrations supporting Defend Our Juries has been the reason for engagement. Individuals interacting with this material have frequently voiced concerns regarding government and police actions surrounding the arrests of demonstrators. Much of the content that is being engaged with is highlighting the arrest of activists, often depicting them as innocent or vulnerable, seemingly to elicit an emotional response and further increase engagement. The overwhelming

sentiment online is that of anger directed to the government when these arrests are shown.

While anti-immigration discussions continue to attract engagement, the volume is considerably lower than pro-Palestine conversations over the past 30 days. There is also noticeably less discourse related to hotel protests, with there being seemingly fewer of these protests outside migrant hotels as winter approaches. Unlike previous months, there is no dominant or singular topic within anti-immigration conversation; instead, the conversation covers various issues such as ongoing criticism of the government for perceived two-tier policing and general opposition toward those supporting refugees, but no subject stands out significantly.





Market House
85 Cowcross St
London
EC1M 6PF



07890 590352
Neil Shanks



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