CORPS RELAY

Prepared by: Mike Bluestone CSyP, Neil Shanks CSyP
James Henderson CSyP & Keith Denton Msyl
Date: January 2025

CORPS
Est. 1859
SECURITY

Terrorist Uses Smart Tech Whilst Planning

On 1st January Shamsud-Din Jabbar, a 42-year-old American man from Houston, Texas, carried out a terrorist attack killing 14 people and injuring a further 57. Jabbar, who had proclaimed his support for ISIS in social media posts before the attack, targeted pedestrians in New Orleans where he drove a rented pickup truck into a crowd on Bourbon Street. Jabbar then engaged in a shootout with police after the vehicle attack and was killed in the exchange. During the FBI's investigation into the attack, which they are treating as an act of domestic terrorism, they have revealed Jabbar had used Meta smart glasses to scout the location weeks before the attack.

Meta and Ray-Ban began their collaboration on a range of smart glasses in 2021, with the devices having only a few visible distinctions from a standard pair of Ray-Bans. The functionality of the glasses allows the wearer to not only take photographs and videos, but also to livestream their camera on specific social media platforms. The wearer can also ask questions of the glasses using the camera or microphone as the focal point to target their search.

Whilst Jabbar did not use the glasses to livestream the attack, he was wearing them throughout. The FBI were able to recover evidence of Jabbar using the glasses to take video of the hostile reconnaissance he conducted of the area in October last year.

This is another example of advancements in technology being utilised by threat actors. Security teams and businesses should be aware of the potential threat of emerging and uncommon technology, such as the Meta glasses and other wearable technology, and its potential to be used in a series of threat activities. There are a range of covert technical surveillance devices available to those that know where to get them, however, the risk from mainstream technology such as glasses and watches that have photographic capabilities can extend beyond hostile reconnaissance, and may include risks of IP theft, or the potential for the collection of other inappropriate images without the subject being aware.

Corps Relay
January 2025

Ministers Reject Call to Broaden Extremism Definition in the wake of the Southport Attack

The attack in Southport stimulated debate in the UK around whether the definition of extremism should be broadened. It was questioned whether the established definition of "vocal or active opposition to fundamental British values," is sufficient to tackle emerging threats. This followed the leaking of sections of a report commissioned by the Home Office last summer (2024) to a Policy Exchange 'think tank' which criticised the recommendations within the report.

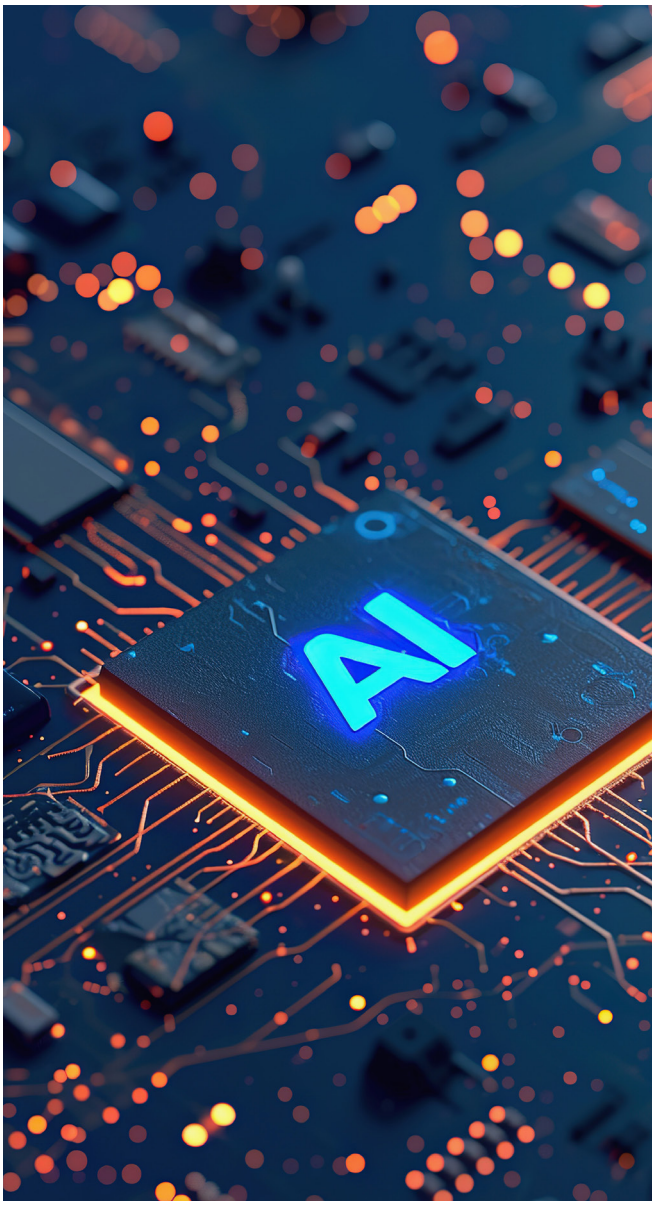
Those in favour of expanding the definition argue that the rise of far-right extremism, online radicalisation, and other evolving threats are not adequately addressed by the government's current strategy, known as 'Contest', which does not favour or target any particular ideology or belief system. Instead, it focuses on tackling extremism and terrorism regardless of the ideological background of the individuals or groups involved. Those calling for change suggest that a broader definition would provide authorities with the tools and resources needed to combat these dangers more effectively. The report urges expanding the definition of extremism to cover, alongside Islamists and extreme right-wing; extreme misogyny, pro-Khalistan extremism, advocating for an independent Sikh state, Hindu nationalist extremism, environmental extremism, left-wing, anarchist and single-issue extremism (LASI), violence fascination, and conspiracy theories.

The Government has rejected the necessity to expand the definition, with critics of the proposal warning that expanding the scope could lead to the suppression of free speech and unjustly label individuals or groups as extremists without clear evidence. This concern highlights the delicate balance between protecting national security and safeguarding individual rights.

Corps Relay
January 2025

DeepSeek – The New Chinese-made Artificial Intelligence (AI) Powered Chatbot

DeepSeek is a Chinese artificial intelligence company that develops open-source large language models (LLM) akin to that of ChatGPT and Gemini. High-Flyer, a Hangzhou based company, were previously known for their use of AI for quantitative trading, the practice of using AI to analyse financial data to inform investment decisions and became the first quant hedge fund in China to raise over 100 billion yuan ($13m) in 2019.



DeepSeek performs tasks at the same level as ChatGPT and Google's Gemini, and the release of the first free DeepSeek chatbot app has significantly disrupted Nvidia's market position. DeepSeek surpassed ChatGPT as the most downloaded free app on the iOS App Store in the United States by 27th January this year leading to a to drop in Nvidia's share price of 18%.

The rise of publicly available AI LLMs pose a number of interesting challenges for the world and businesses. The potential for commercially sensitive information to be compromised by users unwittingly inputting it into the chatbot is very real. Whilst these tools can be very useful for specific purposes, users must remain conscious that any information input into the chatbot is then compromised and accessible to the company providing the chatbot, and in High-Flyer's case, this may also include this information being available to the Chinese Government. If the data should not be shared outside of your business, it should not be input into a chatbot.

"Shut the System" Target Fibreoptic Cables

On 20th January, environmental activist group "Shut the System" conducted co-ordinated attacks across the UK, severing fibre-optic cables to pressure insurance companies into ceasing support for fossil fuel projects.

The London based action was carried out between 06:30-07:00 and reportedly affected:

- Lloyd's of London
- 20 Fenchurch Street (the Walkie Talkie building), the office of Ascot, Hardy, Kiln, Lancashire Syndicate, Tokio Marine, and Markel
- Talbot AIG, 60 Threadneedle Street
- 52 Lime Street – WR Berkley, and Chaucer
- Chubb – 100 Leadenhall street
- AIG – Fenchurch Street

The targets outside London included:

- AIG – 60 Church Street (Birmingham)
- AXA – 21 Queen Street (Leeds)
- Markel - Ecclesall Road South (Sheffield)Who are Shut the System?

Shut the System are a relatively new environmental activist group, having first come into the public eye in the summer of 2024. There are reports from June 2024 of "Shut the System" supporting "Palestine Action" to commit criminal damage (red paint attacks and smashing of windows) at a number of Barclays bank branches across the UK. This was followed in July with similar criminal damage (smashing windows and spray painting) at the premises of Lloyd's of London, Tokio Marine, Chubb, Markel, and QBE, many of which were targeted in the January 2025 incident.

They target banks and insurance companies which they state enable fossil fuel expansion.

Methodology
Sources report that the London based incident involved two activists, attempting to disguise themselves as telecommunications engineers by wearing hi-visibility vests, hooded jackets, facial coverings and gloves, lifted two cable access slabs in the street and cut at least two fibre-optic cables.

It's unknown if the activists had specific knowledge of which cables to cut or simply cut the nearest cables likely to be connected to each target building.

A letter from the group, addressed to the targeted insurer, was also deposited in at least one of the cable access points and has been held by the Police for further investigation.

It's highly likely that the activists conducted some form of hostile reconnaissance in the weeks and days leading up to these actions to establish which cables were most likely connected to the target sites and how vulnerable these areas were to such action.

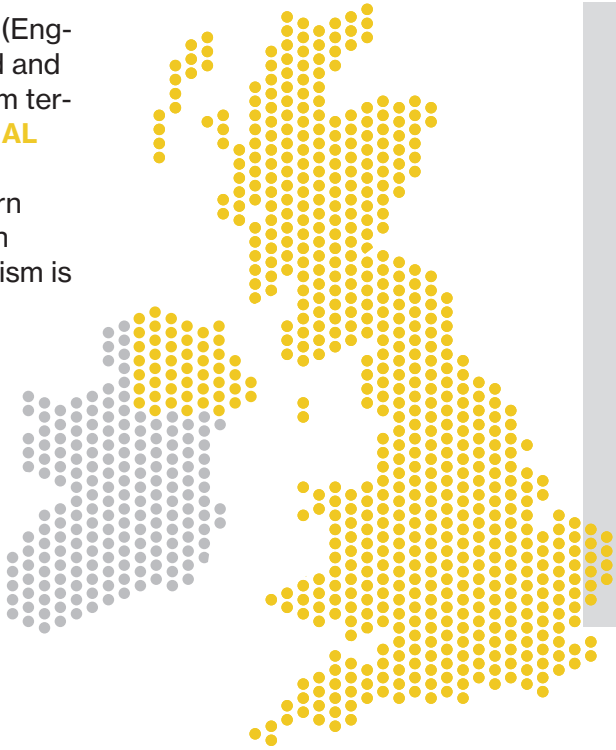
Post Incident
Following the incident, the group then widely publicised their actions to various activist related social media outlets, to achieve optimum exposure to their cause.

These actions reinforce the importance of vigilance from organisations and their security teams with regards to identifying, questioning, and reporting suspicious behaviour externally to their premises. The importance of having adequately secured utilities, including plant equipment and communications access points, is clearly demonstrated. It is possible other groups will now adopt a similar tactic as the potential for an individual(s) to cause significant disruption to a business through targeting their connectivity has now been widely publicised.

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

3D Printing Firearms Manuals

Abdiwahid Abdulkadir Mohamed (33), from Neasden, London was found guilty of six counts of possessing documents likely to be useful for committing or preparing an act of terrorism (contrary to section 58 of the Terrorism Act 2000). Mohamed used a social media app to send himself documents on how to make 3D-printed weapons. Mohamed was found to have attempted to conceal his actions through the use of two proxy accounts and storing the documents on the encrypted app's servers. Mohamed was sentenced to seven years in prison with a further year on extended licence.

Man Sentenced to Prison for a Terrorist Attack on Asylum Hotel

Callum Parslow (32), from Worcester, was sentenced to life with a minimum term of 22 years and eight months for the attempted murder of a 25-year-old man in the Pear Tree Inn, Smite, Worcester. Evidence of Parslow planning an attack included the discovery of research into hotels housing asylum seekers, the purchase and importation of a knife from the US, and his prepared manifesto. Parslow was arrested shortly after the attack in the Pear Tree Inn and before he was able to publish his manifesto or cause further harm. During the search of his address detectives found extreme right-wing material and several weapons, including an axe, knife, and a baseball bat.

19-Year-Old Far-Right Extremist Sentenced

Cameron Finnigan (19), from Horsham, West Sussex, is the latest in a line of radicalised teenagers to be convicted of terror related offences. Finnigan, who was a member of an extreme satanic group, was sentenced to a nine-year extended sentence for possessing a terrorist document and encouraging someone online to take her own life. As part of the investigation, detectives seized his digital devices and established that Finnigan had become involved with a satanic extremist group named ‘764’ which has a militant accelerationist (extreme right wing) ideology.

Finnigan pleaded guilty to six charges, including doing an act capable of encouraging or assisting suicide, contrary to the Suicide Act 1961, possession of a document or record containing information of a kind likely to be useful to a person committing or preparing an act of terrorism, contrary to section 58 of the Terrorism Act 2000, and Possession of indecent images of children, contrary to section 160(1) of the Criminal Justice Act 1988; relating to six category A images and one category A video file.

Security Awareness & Familiarisation - Drone use in the UK

Corps Focus: Security Issue of the Month

Drones, also known as 'unmanned aerial vehicles' (UAV) and more recently 'uncrewed aerial systems' (UAS) have gained significant popularity in the UK, serving both recreational and commercial purposes.

Whilst previously, drones were used mostly by hobbyists to assist with high quality photography and video capture, they have evolved exponentially over the past few years into highly sophisticated systems, transforming multiple industry sectors such as agriculture, construction, delivery services and even emergency services.

Whether it's a single rotor, multi rotor drone, or even a fixed wing model, it's safe to say that drones are no longer just for social media 'influencers' and photographers. Within minutes of unboxing, any member of the public is in control of one of these devices.

UK Drone Regulations
The Civil Aviation Authority (CAA) regulates drone operations in the UK to ensure public safety, airspace security, and compliance with aviation laws. The regulations cover various aspects, including registration, operational guidelines, and restricted zones, the following are key regulations relevant to security teams:

- Drones cannot be flown outside of the pilots visual line of sight.
- Drones cannot be flown more than 120m (400ft) from the closest point on the earth's surface.
- Drones over 2kg must keep at least 150m away from residential, recreational commercial and industrial areas.
- Although drones can be flown over people, they cannot be flown over crowds / large assemblies without prior authorisation.
- Drones cannot fly within restricted airspace or flight restriction zones (FRZ) without prior permission. This includes built up city areas, airports, military zones, prisons and nuclear sites.
- Drone pilots must comply with the UK Data Protection Act when capturing images or videos. This includes informing people that they are being recorded and avoiding intrusive surveillance.
- Drones weighing between 250g and 25kg require both a registered 'Operator ID' and a 'Flyer ID' from the CAA. This registration needs to be renewed annually and is a registration of the operator, not the drone.
- Drones weighing under 250g require a registered 'Operator ID' from the CAA but not a 'Flyer ID'.
- Sanctions such as heavy fines, and even imprisonment may be issued for failure to comply with the regulations set out by the CAA.

Security Threats Associated with Drone Use
The rise in drone usage has introduced several security concerns that businesses and security teams must be aware of. These challenges include threats to public safety, privacy violations, and potential misuse by malicious actors. Below are key security issues associated with drone use:

- Unauthorised surveillance and privacy violations – Drones equipped with cameras can be used for surveillance, capturing images, footage or sensitive information without consent.
- Trespassing / unauthorised access – Drones may be flown over private businesses or restricted airspace, resulting in significant disruption. In 2019, climate activist group Extinction Rebellion threatened to shut down Heathrow Airport by flying drones close to flight paths.
- Smuggling / contraband delivery - Drones have been used to smuggle illegal goods such as drugs, weapons, and mobile devices across borders or into prisons.
- • Weaponisation and Terrorism – Although

Security Awareness & Familiarisation - Drone use in the UK

not yet witnessed in the UK, drones can be weaponised with explosives or firearms, creating potential threats to public gatherings or high-net worth individuals. Extremist groups have utilised drones for reconnaissance and attacks in conflict zones, raising concerns about their use in urban settings, particularly since smart devices such as Meta glasses are now being used by attackers to conduct hostile reconnaissance (New Orleans attack, New Years Day 2025).

- Cybersecurity vulnerabilities - Drones rely on GPS and communication links that can be hacked or jammed, allowing attackers to take control of the device or access sensitive / classified information.
- 'Swarm' technique – This involves the coordination of multiple drones operating as a unified system. These can be used as an effective distraction method or to gather intelligence over a large area in a shorter space of time, compared with a single drone.
- Notice of intent – This involves utilising the drone to display messages, taking advantage of the unit's inaccessibility, and is likely to be used by protest groups to display banners / group messages etc.
- 'Crop Spraying' – Another not yet witnessed in the UK, this involves modifying the drone and enabling it to drop all manner of liquid substances directly over a large crowd or event.

Security Response to Potential Drone Threats
Security teams and organisations should familiarise themselves fully with the threats associated with drone use for malicious purposes, as well as the current regulations around their use in the UK, full details can be found on the CAA website: https://www.caa.co.uk/drones/

- Drone use should form part of documented security strategies, with a clearly defined response and escalation procedure.
- Patrolling security officers should remain vigilant to 'threats from above' whilst conducting external patrols, incorporating checks for drone activity as standard. Remember, a drone is effectively a mobile camera in the sky and the response should be the same as if a suspicious person was spotted filming around your premises.
- Police services request that they are contacted immediately if unannounced drone activity is observed, particularly if it appears to have an object attached to it as this could potentially be an IED or have CBRN (Chemical, Biological, Radiological, and Nuclear) implications. Whether in flight or static on the ground, the drone could pose a risk to those around it.

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

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