CORPS RELAY

Prepared by: Mike Bluestone CSyP, Neil Shanks CSyP
James Henderson CSyP & Keith Denton Msyl
Date: November 2024

CORPS
Est. 1859
SECURITY

Russia/Ukraine Conflict – US and UK can now be targeted according to Putin

President Putin has made a public statement that military facilities of the United States and United Kingdom can now be targeted, as these nations allowed the use of US Army Tactical Missile Systems and UK-supplied Storm Shadow Missiles to target areas within Russia. Putin asserts that Russia is entitled to use their weapons against the military facilities of any countries that allow their weapons to be used against Russian facilities. The impact of this within the UK is more likely to involve the use of cyber attacks and dis/misinformation campaigns against targets including UK businesses. The threat of cyber attacks on UK and US businesses has been identified by several politicians, including the Chancellor of the Duchy of Lancaster, Pat McFadden, and the Work and Pensions Secretary, Liz Kendall.

Businesses should take steps to ensure they have adequate cyber security measures in place, including the delivery of appropriate cyber security awareness training and testing. Businesses should be aware of their online presence and those of their employees, including the use of both personal and professional social media platforms (information on this can be found on the NPSA website within their Think before you Link guidance).

CT Police Winter Vigilance Campaign

The winter brings with it a calendar full of festive and seasonal events, such as increased shopping, festive markets, pantomimes, concerts, and of course the New Year. These types of events can attract a range of threat actors and criminals looking to take advantage of the busy crowds and potentially busy or distracted people. The Winter Vigilance Campaign is about encouraging people to remain aware and alert as they enjoy the season with family and friends and enabling them to do this safely.

Whilst there is a necessity to remain aware of a range of criminality, including opportunistic thieves and pick pockets, it is also vital to remember that the terror threat remains. The threat to the UK from terrorism is currently at substantial, which means an attack is likely. This campaign seeks to remind the public of potential threats, encourage people to report anything that “doesn’t feel right”, and ultimately to help people enjoy the winter season safely.

Protect UK are promoting the scheme nationally, however, many local forces have their own Winter Vigilance Campaigns so please check what is happening in your local area.

Pro-Palestinian Protestors that targeted Elbit arrested on Terror Charges

The incident in August 2024 at the Elbit Systems site, which involved a van driving through the fence of the arms manufacturers site in Filton, near Bristol, initially resulted in the arrest of seven people on charges of criminal damage. Once inside the facility, the group engaged in further acts of property destruction and were said to be equipped with axes, sledgehammers, and “homemade weapons”. One of the group also received an assault charge. November saw a further ten individuals being charged with terror related offences linked to the incident in August. Nine have been charged on suspicion of the commission, preparation and instigation of acts of terrorism, contrary to Section 41 of the Terrorism Act 2000, with the tenth being arrested on suspicion of preparation of terrorist acts under Section 5 of the Terrorism Act 2006.

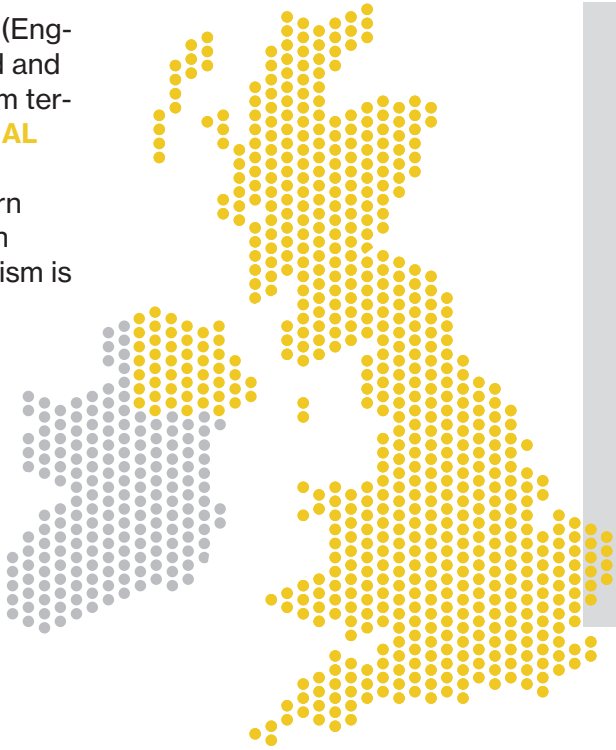
Gatwick South Terminal Evacuation

The South Terminal at Gatwick Airport was evacuated on the morning of Friday 22nd November due to a suspect package being identified. Sussex Police responded to the site at 08:20am and imposed a cordon around the area to ensure the safety of the public. The incident disrupted over 600 flights in and out of the airport. The evacuation was eventually lifted in the afternoon of the same day following an explosive ordinance disposal team making the package safe. Two individuals were detained by the Police in relation to the incident but were subsequently allowed to continue their journeys.

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

Guidance to Social Media Auditors (Article of the Month)

It is a common occurrence to see citizen journalists or social media (YouTube) auditors on site these days, especially those with access from public highways. These individuals may be seen as a nuisance to many of the sites they target, however, they generally act lawfully. Many within the Photography is not a Crime (PINAC) movement believe they are providing a public service in highlighting the rights of individuals against unlawful restrictions to individual rights within the UK.

Many Auditors make money from the upload of their content to social media and video streaming sites, and it has been suggested that some seek to provoke reaction from their subjects to capture more interesting content and increase their viewership. This has been countered recently as some auditors have been making a greater effort to be nice to their subjects and engage more people with their content.

Any person has a lawful right to film and photograph anything they can see from a public (or publicly accessible) space. They do not require permission for this, even if they intend to publish or share any of the recorded content. Auditors are often well versed in their rights and may attempt to embarrass the person they engage with if they are able to identify any gaps in their knowledge or if they make statements that contradict an individual's legal/civil rights. Some of the more popular auditors have over 150k subscribers and get half a million views on a single video over the time it is posted.

Good practice in managing a social media auditor on/at site:

- Educate the site staff in individuals rights. This includes all staff, not just security and front of house teams. Colleagues in key roles should complete regular training and table top exercises to ensure they know how to deal with any occurrences.

Guidance to Social Media Auditors (Article of the Month) Cont.

- Be clear on the legal boundary of the site and which areas are publicly accessible or private - the access gates/barriers are logical and will save time and discussion, which in turn will limit the content created.
- If you have publicly accessible areas, including public receptions, be clear on the expectations for members of the public accessing them. There is an implied right to enter such areas, which can be expressly revoked at any time by the site manager or their agents, and it is advisable that any privately owned places that allow the public to enter include signage to show it is private property. Businesses with publicly accessible spaces, such as shopping centres or venues, may elect to include signage informing visitors of any rules or restrictions in place such as no photography without written permission from the management. Auditors can be directed to this signage if they question being asked to stop recording or leave the area.
- If an auditor is clearly on the premises and you want them to leave, be polite, and take the time to explain your policy. They will expect you to revoke access and ask them to leave or they will likely remain in place to build their content.
- Do not engage with auditors any longer than necessary. This approach limits the content available to them and reduces the time they will spend at your site, as well as the chances of it being upload onto social media. If there is nothing of interest it is unlikely to get posted as social media auditors do not want to post boring content.
- If you must engage with an auditor, keep it brief and factual, and do not attempt to restrict or limit their movements outside the site boundaries (fence line/perimeter). It is imperative to understand where the sites jurisdiction ends.
- Closed-Circuit Television (CCTV) can monitor auditors from a distance without engaging with them. Once you have confirmed they have no hostile intent monitor them from a distance.
- You cannot demand (legally or otherwise) for them to stop filming or that they delete their recordings/images. Furthermore, do not attempt to confiscate or touch their recording devices.
- Recording vehicles in a car park or persons on the site is not breaching GDPR/Data Protection but you can ask the auditor politely to respect people's privacy and to blur these out. They are not required to do so, but many will if asked polity.
- If you film or photograph an auditor whilst at work, then you are subject to GDPR/Data Protection as you will be acting for an employer. The auditor can apply for any information as per site policies and procedures.
- If you suspect the person is suspicious inform the Police immediately.

It is recommended that staff view a selection of online audits, to see both good and bad practices.

National Protective Security Authority (NPSA) Guideline for Social Media Auditor Activity

The NPSA have published their guidance on Social Media Auditor activity on their website. This includes a range of awareness posters and guidance for employers to use.

It is possible that the actions of an auditor and a threat actor could appear very similar. It is important to ensure the person(s) on site is not a threat actor(s) e.g. conducting hostile reconnaissance (further information can be found in both the ACT and SCaN training). Once this is confirmed and it is established that the person(s) is/are a social media auditor, NPSA recommend the use of the CALM approach – Chat, Assess, Limit, Monitor.:

CHAT - First, engage suspected auditors in a friendly manner. A professional greeting will often work better than a more confrontational approach. Remember that the goal of auditing is often to generate controversial content. A friendly opening will minimise the risk of this happening while ensuring you remain vigilant and maintain a strong security culture.

ASSESS - Next, confirm the suspected auditor's intent while continuing to evaluate for other potential threats they might pose, or may provide a distraction for. Auditors will often either identify themselves as a social media auditor, or state that they do not need to provide a reason to film. If the auditor provides a name of the social media account, this could be noted down to check at a later point. If you feel the auditor's behaviour may represent a genuine security risk or feel there is a risk for the personal information of staff to be misused, call the Police. The Police will assess whether they need to attend based on the information provided. The incident record will also assist in building an intelligence picture around such activity.

LIMIT - Thirdly, aim to keep interactions with auditors as short as you can while maintaining your security presence. Auditor activities rely on generating and maintaining negative encounters, so by limiting interactions you minimise the scope for negative content from video or audio recordings. Everyone interacting with auditors should be particularly mindful of avoiding the use of inappropriate or offensive language. Remember: the goal for auditors is often to provoke such reactions in order to generate online engagement.

MONITOR - Lastly, you should continue to monitor auditors to ensure they don't escalate into a threat, such as attempting to breach a perimeter. Such monitoring can be done from a distance to avoid unnecessary encounters, if you are able to do so effectively. If escalation does occur, or you have other concerns, you should notify the police.

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

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