CORPS RELAY

Prepared by: Mike Bluestone & Neil Shanks

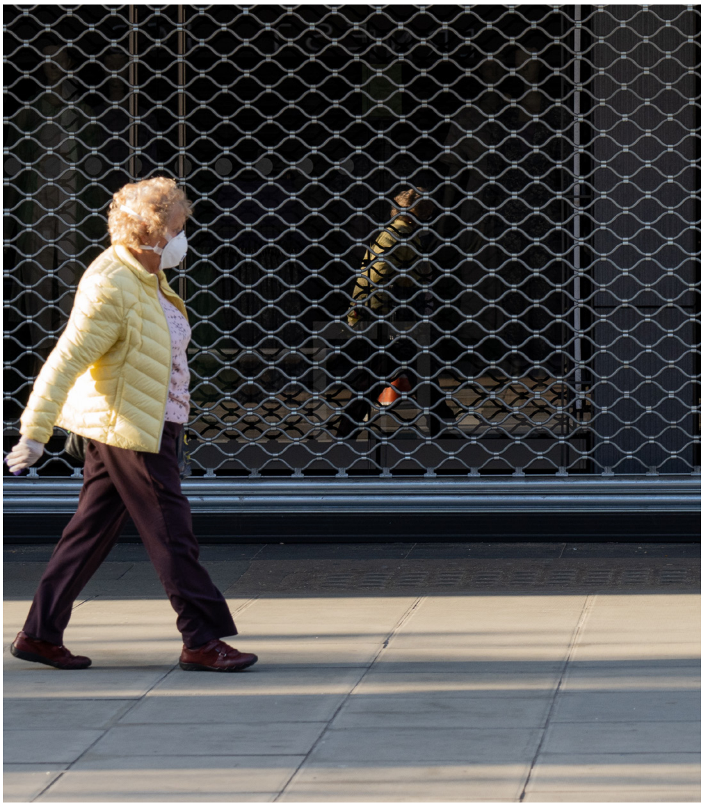
Date: July 2021

CORPS
SECURITY

COVID-19: Lockdown continues into July

The lockdown reductions planned for June did not take place due to the emergence and reproduction of multiple new strains of COVID-19. New infections remained high towards the end of June, with Scotland registering their highest number of infections in one day since the start of the pandemic.

However, despite the increase in infection rates, the levels of fatalities remain significantly lower than during the peaks of the second wave of the pandemic. This has led to newly appointed Health Secretary Sajid Javid announcing that restrictions in England are likely to come to an end on the 19th of July, and that the UK will have to learn to live with the virus. The easing of restrictions in Northern Ireland, Scotland and Wales remains under local control within the devolved powers. Scotland and Northern Ireland are yet to declare an anticipated date for easing lockdown further, whilst Wales have declared their next lockdown review will take place on the 15th of July.



UK's Cybersecurity Plans

The Foreign Secretary, Dominic Raab, has announced that the UK and U.S. are revising the Atlantic Charter to address cybersecurity. The UK and U.S. are also currently taking a number of steps to counter cybersecurity threats ranging from ransomware attacks, to attacks on critical infrastructure. These steps follow a number of high-profile ransomware attacks in the UK that affected numerous businesses and organisations, including a number of educational establishments.

These actions form part of the UKs plans to become a global leader in cybersecurity, which will extend to playing a major role in stopping international cybersecurity organisations. Examples include the recent U.S./Europol operation that resulted in the disruption and seizure of the Slilpp cybercrime marketplace infrastructure.

LinkedIn Deny Data Breach of 92% of Users

There have been numerous reports of a major data breach affecting 92% of LinkedIn users. The reports suggest that the information of approximately 700 million people has been made available, with types of information including: full names, phone numbers, email addresses, physical addresses, geolocation records, username and profile URL's, and associated social media accounts.

LinkedIn deny that any breach has occurred and claim that the breach being reported is actually the result of data scraped from LinkedIn and other sites and is the same data that is included in their April 2021 scraping update. "Scraping", also known as data scraping or web scraping, is the process of extracting human-readable information from a website/program, into a spreadsheet/file, and then saving onto a server/computer. Scraping is a very efficient way to collect data from the internet and can be used to inform other programmes or websites.

Fastly: Internet Outage

The Fastly service, an edge cloud platform, went down on Tuesday 8th June, resulting in a number of websites (including Amazon, eBay, and the .Gov website) becoming unavailable. The function of Fastly, and other providers like Cloudflare and Akamai, is to provide a server known as a Content Distribution Network (CDN). Very simply put, the role of the CDN is to improve webpage load speed and handle high traffic loads, by reducing the physical distance between the user and the server. The existence of widely distributed CDN's allows for websites to function where, without the CDN, the traffic would overwhelm the site and cause the errors that were experienced in June. The impact of one CDN going down resulted in some of the largest websites in the world becoming inaccessible. This emphasises the risks of disorder and disruption that would be caused if, for any reason, multiple CDN's were to be impacted simultaneously. The targeting of CDN's may become a tactic adopted by certain groups, be it terrorist organisations, or civil groups looking to disrupt corporate establishment operations.

Manchester Arena Inquiry

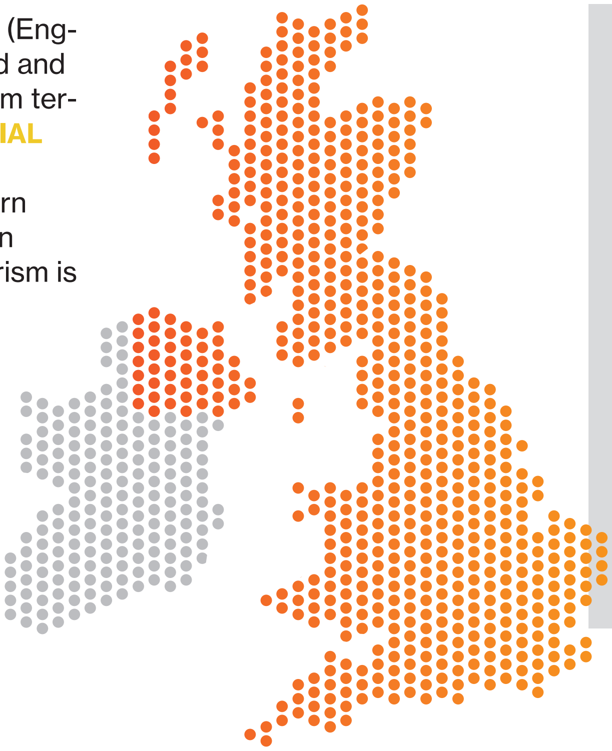
The first of three volumes of the Manchester Arena Inquiry was published in June. Each volume addresses a different area that influenced the outcome of the 2017 attack, and are arranged as follows:

- Volume One – addresses the security arrangements of the concert, including missed opportunities for detecting and preventing perpetrator Salman Abedi, or reducing the harm that was caused in the attack. This volume was published to coincide with the government's consultation on a "Protect Duty" as there are several areas that are highly relevant.
- Volume Two – will address the response to the emergency including the planning and preparedness of the responders to the attack. It will examine every element of the response after the bomb had detonated and seek to determine what could have been done to reduce the harm that was caused. The report will also explore the circumstances of the death of each of the twenty-two victims of the attack.
- Volume Three – will examine the roles of the security services and Counter-Terrorism Police and ask whether they should have prevented the attack from occurring. It will explore whether Mr Abadi was radicalised, and if so, how, as well as how he came to be at the concert on that day. Within this assessment it will also explore whether there were opportunities that would have allowed the incident to be averted had the correct actions been taken.

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 **SEVERE**



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

Recent Developments

Increasing Threat from Daesh in Africa

The Global Coalition against Daesh met in late June to discuss concerns about the growing threat of the terrorist group in Africa. Not only has there been recent violence in north-east Syria, but the group continues to pose an increasing threat across many areas of Africa including Nigeria, Cameroon, Niger, and Chad. The UK Government has committed £12.6m to support local efforts to counter the growing threat of Daesh. They are also engaged in discussions with ministers from 45 other countries, regarding strategy to combat the terrorist group. The UKs contribution will fund a new Conflict, Stability and Security Fund programme for the Lake Chad Basin region of West Africa, where a group known as Islamic State West Africa (ISWA), an affiliate of Daesh, have been responsible for spreading terror through serious violence. Despite reduced media coverage of Daesh, and their defeats in Syria and Iraq, they remain a genuine threat to those that do not share their ideologies.

Recent Developments

Northern Ireland: Improvised Explosive Device Defused in Portadown, County Armagh

On Monday 14th June, homes in Glanroy Avenue, Portadown, were evacuated after an explosive device was found in the vicinity. The device was discovered by a member of public on the roadside during the time parents travel to school to collect their children. Army bomb disposal experts were called to the scene, where they defused the device and took it away for forensic investigation.

One in Eight Terror Suspects in the UK are Children

One in eight terrorism suspects arrested in the past year were children, according to figures revealed recently by the Home Office. This equates to 13% and is the highest level on record. The Home Office has stated that the high proportion of children arrested for terrorism offences was largely due to falls in the arrests of those in older age groups (overall arrests for terrorism-related offences decreased by approximately 38% compared to the previous twelve-month figures). However, this only serves to make the increase of 75% in the number of under-18's arrested for terrorism-related activity more alarming, as it clearly goes against the overall trend. Whilst the percentages are high, the overall figures remain low, with the number of under-18's arrested increasing by only nine individuals from the previous 12-month figure of twelve.

The increasing risks of isolation leading to radicalisation through the internet is not new, and the potential of the pandemic increasing this risk was identified early on in lockdown. This may also be compounded by the likelihood that many individuals may be having less face-to-face interaction with positive role models that could have identified signs of radicalisation and alerted the authorities, which would have increased the chances of early intervention.

Notable Dates/Events

Key Religious or National Celebrations

There are significant days for several religions and nations throughout July. It is not only important to be mindful of these dates to celebrate our diverse society, but also because several terrorist groups have been known to select these days to carry out their actions.

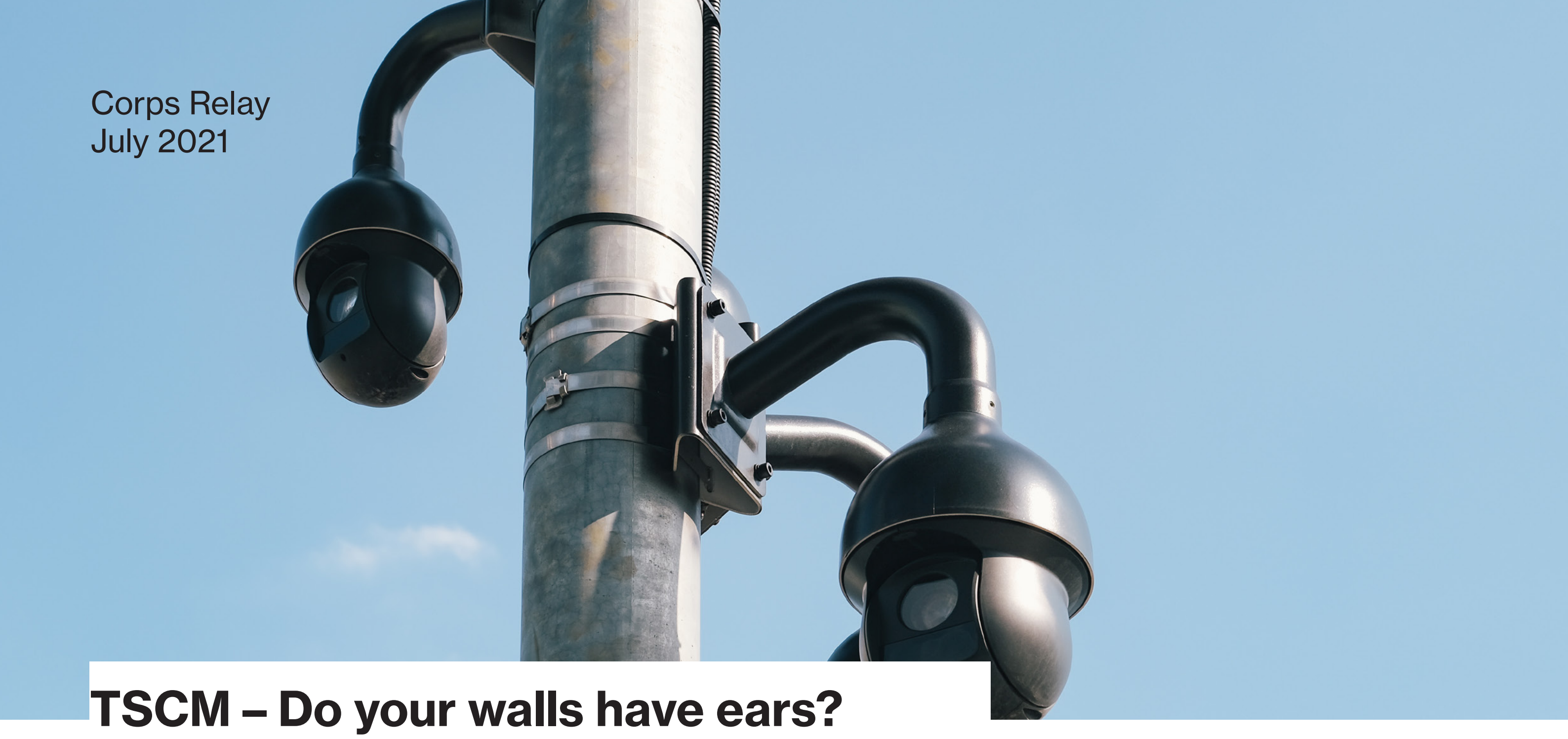
For a full list of key dates, events and demonstrations, please view the "Corps Events Calendar" in CorpsSecure, our online customer portal or app.

Notable dates in July include:

- 7th July – 16 year anniversary of the 7/7 bombings – key event anniversary
- 12th July – bank holiday – bank holiday in Northern Ireland
- 12th July – eight-year anniversary of Pavlo Lapshyn's attempt to blow up Mosques in Wolverhampton and Tipton – key event anniversary
- 18th July – Tisha B'Av – a Jewish celebration
- 19th July – fourth anniversary of the Finsbury Park attack– key event anniversary
- 20h July – Eid-al-Adha - Islamic celebration

Demonstrations

- 26th June - 03rd July – anti HS2 protests “Truth Trail – Stop HS2”. Walking route from Lichfield to Wigan via Rugeley, Stafford, Stone, Madley, Crewe, Middlewich, Glazebrook and Wigan.
- 3rd July – animal rights protest in Leeds, Leicester Square (Westminster), Swansea and Yeovil.
- 3rd July – reclaim the streets protest to remember the death of Sarah Everard – Chester, Sheffield City Centre (Devonshire Green, Devonshire Street).
- 3rd July – Liverpool Fight Racism Fight Imperialism (FRFI) open-mic event on Church Street as part of an anti-racism demonstration.
- 3rd July – anti-lockdown protests being held in Glasgow and Edinburgh.
- 3rd July – “Rally for Cecil” – Worldwide Rally Against Trophy Hunting (WRATH) annual march in Birmingham. Initial meeting point is Centenary Square.
- 5th-10th July – pro-Palestinian protest camp “mass-action camp” by Palestinian Action Group (PAG) as part of their “Shut Elbit Down” campaign.
- 6th July – pro-Palestinian protest by Palestine Action, Palestine Solidarity Campaign and Oldham Peace and Justice outside Elbit Ferranti (Cairo House, Oldham). This has been advertised as a repeat event taking place every Tuesday.
- 9th July – pro-Palestinian protest organised by the Palestine Solidarity Campaign UK, who are calling for the end to international support for Israel. The meeting point is advertised as outside the School of Oriental and African Studies (SOAS) (Mallet Street, Bloomsbury), followed by an unknown march route.
- 10th July – animal rights protest in Cambridge, Bridgend, Leicester Square (Westminster) and Taunton.
- 10th July – pro-Palestinian Protest outside Puma’s head office (22 Sea Containers, Upper Ground, Southwark) due to their continued sponsorship of the Israeli national football team.



TSCM – Do your walls have ears?

Corps Focus: Security Issue of the Month

Technical Surveillance Counter Measures, also known as TSCM, is the process of conducting a systematic physical and technical inspection of a designated area to locate and remove/deactivate any covert surveillance devices. Within popular media this process is also known as bug sweeping. These devices can take many forms and fulfil a variety of duties, from collecting audio and video footage from the area, to recording keystrokes and computer access, as well as a range of other functions.

Every business should be mindful of the risks posed by technical surveillance and ensure that there are policies and processes in place to reduce the likelihood that it can take place. The more confidential the data that the company is working with, the more valuable that information is likely to be to criminals and/or state actors. Technical surveillance can be used by criminals/state actors as a remote way to steel intellectual property and confidential information that can then be used against the company in question.

Whilst most businesses ensure that their cybersecurity is robust enough to defend against external attack, and that their server rooms are secure, far fewer take the same steps to ensure access to their servers from within their offices has the same level of security.

Office items that seem perfectly normal can, and are, adapted by criminals to provide technical surveillance. Examples include inanimate objects, and even cables. In 2013 Andy Davis, a UK based Black Hat Hacker and Research Director for the NCC Group, demonstrated how easy it is to adapt a laptop docking station into a technical surveillance tool using a Raspberry Pi insert that can "sniff" traffic to and from the machine. Packet sniffing is the process of gathering/collecting packets of data that pass through that point. The ability of Mr Davis insert (dubbed the "Spy-Pi") to gather packets amounted to the potential to steal sensitive information transmitted to/from the laptop. In reality the systems used by criminals and state actors are far more discrete and powerful that Mr Davis's Spy-Pi.

If there is not already a programme of regular TSCM in place within a workplace then the answer to the question "do your walls have ears?" cannot be confidently answered. Instead, the questions that need to be answered are what is the potential cost to the business if key areas were being monitored, be that via audio, video, or transmissions through the information communication technology (ICT) networks? Does technical surveillance fall between the lines of the existing approach to security and what can be done to address this? Is it time to engage a specialist TSCM partner?

If you have any questions about TSCM for your site, or would like guidance in how to engage a TSCM provider, please contact Corps Consult by phone on 020 7566 0516, or by email at Intel@corpsconsult.co.uk

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

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