SECURITY INTELLIGENCE UPDATE
MAY 2020

CONTENT

About Us

Sentinel Group Security (SGS) was formed in July 2005 and became a fast-growing security services provider within United Kingdom and Ireland. We first partnered with our customers to provide specialised and effective security solutions including open source intelligence reporting, security vulnerability assessments and training. Our capability is defined by our employees and the high level of skills and experience they possess and the procedures they adopt.

Intelligence led security

With a 360° approach to threat detection and intelligence service provision. Outside of dealing with major incidents, the SGS National Operations Centre proactively assesses the various security threats that your business, people, assets and brand might face by monitoring social and conventional media to identify:

- On-going threats
- Specific industry threats
- Future trends
- Best practice

Disclaimer

In compiling this report SGS has relied on the veracity of public information available at the time of publication. SGS accepts no legal, equitable or other liability whatsoever for any actual or consequent loss incurred by the client in relation to this report or for the accuracy of any statement herein.

United Kingdom's National Security Threat

Introduction

The main threats to national security are terrorism, espionage, cyber threats and the proliferation of weapons of mass destruction, many of which impact on the UK's national infrastructure.

National infrastructure sectors represent core strategic interests for foreign intelligence services, whose targeting against the sectors is likely to include espionage for economic, political, military or commercial gain.

While the threat from terrorism to the UK as a whole is high, and historically both international and Northern Ireland terrorist groups have targeted UK infrastructure, the current terrorist threat to the national infrastructure can be characterised as generally limited and often aspirational.

The exception is transport which continues to face enduringly high levels of threat from international terrorism. In addition, the emergency services and defence sectors, specifically police and military personnel, also face a high level of threat from both international terrorism and dissident republic groups in Northern Ireland, for whom they are a priority target for attack.

Generally higher levels of effective and visible protective security at national infrastructure sites are likely to act as a deterrent to terrorists, who increasingly favour 'soft' targets which allow them to achieve their aims with greater chance of success. Nevertheless, with the continual diversification of the threat, the ambition and capability of terrorist groups to target UK infrastructure is likely to continue to evolve. https://www.cpni.gov.uk/national-security-threats

United Kingdom's Threat Definitions

International terrorism

International terrorism from groups such as the Islamic State in Iraq and the Levant (ISIL) and

Al Qaida present a threat from many others. They hold territory in places without functioning governments, making it easier for them to train recruits and plan complex, sophisticated attacks. Drawing on extreme interpretations of Islam to justify their actions, these groups often have the desire and capability to direct terrorist attacks against the West, and to inspire those already living there to carry out attacks of their own.

Northern Ireland-related terrorism

Northern Ireland-related terrorism continues to pose a serious threat to British interests. Although the Provisional Irish Republican Army (PIRA) has ceased its terrorist campaign and is now committed to the political process, some dissident republican groups continue to mount terrorist attacks, primarily against the security forces.

Domestic extremism

Domestic extremism mainly refers to individuals or groups that carry out criminal acts in pursuit of a larger agenda, such as "right-wing extremists". They may seek to change legislation or influence domestic policy and try to achieve this outside of the normal democratic process. https://www.mi5.gov.uk/counter-terrorism

Cyber

"Cyberspace" is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.

Cyberspace lies at the heart of modern society; it impacts our personal lives, our businesses and our essential services. A secure online environment is essential to HM Government, which is providing an ever-increasing number of online services to UK citizens and businesses as part of a major digital services transformation programme. The ability to conduct online transactions securely is central to the delivery of public and commercial services and communications. However, some individuals and groups use cyberspace for malicious purposes. We call these people 'hostile actors' and they exploit cyberspace to conduct espionage operations or launch damaging computer network attacks.

Cyber security affects both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or state and industrial espionage. https://www.cpni.gov.uk/cyber

Espionage

The potential impact of successful State-sponsored espionage against the UK is both wide reaching and significant. The threat of espionage (spying) did not end with the collapse of Soviet communism in the early 1990s. Espionage against UK interests continues and is potentially very damaging. Several foreign intelligence services (FIS) seek to gather intelligence on a broad range of subjects, including foreign policy, defence, financial, technological, industrial and commercial interests. https://www.cpni.gov.uk/espionage

Serious and Organised Crime

Serious and organised crime is defined in the 2018 Serious and Organised Crime Strategy as individuals planning, coordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks.

The main categories of serious offences covered by the term are:

- child sexual abuse
- modern slavery and human trafficking
- organised immigration crime
- illegal drugs
- illegal firearms
- organised acquisitive crime
- cybercrime
- fraud
- money laundering, bribery, corruption and sanctions evasion.

    https://www.nationalcrimeagency.gov.uk/

United Kingdom Current Threat Levels

Introduction

Members of the public should always remain alert to the danger of terrorism and report any suspicious activity to the police on 999 or the anti-terrorist hotline: 0800 789 321. If your information does not relate to an imminent threat, you can also contact them at https://www.mi5.gov.uk/contact-us

> **To report an imminent threat call <u>999</u> or ring,**
>
> **the Anti-Terrorist Hotline on <u>0800 789 321</u>**

What the threat levels mean

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

LOW
- Means an attack is unlikely

MODERATE
- Means an attack is possible, but not likely

SUBSTANTIAL
- Means an attack is likely

SEVERE
- Means an attack is highly likely

CRITITCAL
- Means an attack is highly likely in the near future

How are threat levels decided?

The threat level for the UK from international terrorism is set by the Joint Terrorism Analysis Centre (JTAC). MI5 is responsible for setting the threat levels from Irish and other domestic terrorism both in Northern Ireland and in Great Britain.

In reaching a judgement on the appropriate threat level in any given circumstance several factors need to be considered. These include:

- **Available intelligence.** It is rare that specific threat information is available and can be relied upon. More often, judgements about the threat will be based on a wide range of information, which is often fragmentary, including the level and nature of current terrorist activity, comparison with events in other countries and previous attacks. Intelligence is only ever likely to reveal part of the picture.

- **Terrorist capability.** An examination of what is known about the capabilities of the terrorists in question and the method they may use based on previous attacks or from intelligence. This would also analyse the potential scale of the attack.

- **Terrorist intentions.** Using intelligence and publicly available information to examine the overall aims of the terrorists and the ways they may achieve them including what sort of targets they would consider attacking.

- **Timescale.** The threat level expresses the likelihood of an attack in the near term. We know from past incidents that some attacks take years to plan, while others are put together more quickly. In the absence of specific intelligence, a judgement will need to be made about how close an attack might be to fruition. Threat levels do not have any set expiry date but are regularly subject to review to ensure that they remain current. https://www.mi5.gov.uk/threat-levels

Current national terrorism threat level

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

SUBSTANTIAL

Northern Ireland terrorism threat level

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

SEVERE

Open Source Security Incident News

Convicted terrorists less likely to reoffend than other criminals – study

Convicted terrorists are extremely unlikely to reoffend compared with other prisoners, research by academics and security services in Europe has found. The research shows that less than 5% of convicted terrorists commit a second terrorist offence after leaving prison. In England and Wales, around 45% of all prisoners will reoffend within a year of release. The research was conducted in Belgium, which has faced Islamist terrorism since the early 1990s and became one of the centres of the Islamic State campaign in Europe in 2015 and 2016. The forthcoming release of thousands of extremists imprisoned for terrorist offences has worried security services in the UK and elsewhere.

UK government told not to use Zoom because of China fears

Government and parliament were told by the intelligence agencies last week not to use the videoconferencing service Zoom for confidential business, due to fears it could be vulnerable to Chinese surveillance. The quiet warnings to limit the technology came after the cabinet had used Zoom to hold a well-publicised meeting at the end of March, a decision that was defended at the time as necessary in "unprecedented circumstances".

Parliament was advised last week by the National Cyber Security Centre, part of intelligence agency GCHQ, that Zoom should only be used for public business.
https://www.theguardian.com/uk/uksecurity

## Four arrested and gun seized in firearms investigation

Officers from the National Crime Agency's Armed Operations Unit have arrested four men as part of a major investigation into the criminal supply of firearms to the north of England.

Three men were detained as armed officers moved in to stop a car in the Beech Street area of Tingley, West Yorkshire at around 3pm on Wednesday 22 April, A handgun and ammunition were recovered from the scene. Just after midnight a fourth man was held in the Redfearn

Wood area of Rochdale, Greater Manchester. The operation was assisted by officers from West Yorkshire Police and Greater Manchester Police. All four men are now in custody and are being questioned by NCA investigators on suspicion of being concerned in the supply of firearms.

Armed individual opens fire in Chatham

An armed man opened fire from a balcony in the dockside area of Chatham, Kent. Armed police responded to the incident and arrested the suspect. Details of the incident are still emerging, but no casualties were immediately reported. Indiscriminate acts involving firearms are rare in the UK.
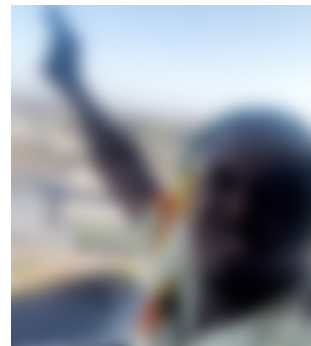
Customs officials discover 190kg of cocaine at Dover port

Customs officials seized 190 kg of cocaine from lorries in two separate seizures at the port of Dover. They found 140 kg of drugs in a consignment of paper and card and arrested the Dutch driver. Later officials found 40 kg in a lorry and arrested two Czech nationals who were later released. The two seizures are not thought to be connected, the National Crime Agency said.

Fears of rise in UK terrorist recruits as anti-radicalisation referrals collapse

Counter-terrorism officials fear a rise in terrorist recruits after a collapse in referrals to the UK's main anti-radicalisation scheme during the lockdown, as extremists pump out propaganda urging British attacks. The Guardian understands referrals to Prevent are down by more than 50% since the lockdown started on 23 March, according to official figures yet to be made public. Counter-terrorism officials fear a crucial defence is being weakened with young people spending more time online alone and unsupervised since schools and colleges closed. https://www.theguardian.com/uk/uksecurity

GCHQ calls on public to report coronavirus-related phishing emails

GCHQ is asking members of the public to report suspicious emails they have received amid a wave of scams and hacking attacks that seek to exploit fear of Covid-19 to enrich cybercriminals.

The National Cyber Security Centre, a branch of the intelligence agency, has launched the suspicious email reporting service with a simple request of the public: forward any dubious emails to: report@phishing.gov.uk

The NCSC's automated scanning system will check for scam emails and immediately remove criminal sites. https://www.theguardian.com/uk/uksecurity

Authorities seize 14kg of cocaine at Channel Tunnel checkpoint

Customs officers seized 14 kg of cocaine hidden in a consignment of face masks at a customs checkpoint in the Channel Tunnel. Authorities discovered the narcotics in a polish-registered van. Police detained a Polish national. The contraband had a street value of around GBP 1 Mn. The seizure demonstrates that criminal gangs are attempting to exploit the disruption caused by the COVID-19 pandemic by using new methods to smuggle contraband into the UK.

Opportunity or threat? How Islamic extremists are reacting to coronavirus

Groups such as Isis plan to exploit pandemic, but even it has acknowledged danger posed by virus. Islamic extremists hope to exploit the Covid-19 pandemic to launch new attacks, motivate followers and reinforce their credentials as alternative rulers of swaths of unstable countries across the Middle East, Asia and Africa. But the responses of different extremist groups have differed. While Islamic State has told its members to launch attacks against weakened and distracted western nations. https://www.theguardian.com/uk/uksecurity

Pharmacist and surveyor arrested over coronavirus testing kits

A pharmacist and a surveyor have been arrested on suspicion of illegally selling coronavirus testing kits in two National Crime Agency investigations. NCA officers searching chemists as part of the agency's proactive response against criminals trying to exploit the Covid-19 pandemic, the NCA also took down a website trying to fool victims into buying suspected non-existent personal protective equipment (PPE) through phishing emails. NCA officers arrested the 46-year-old pharmacist from Cr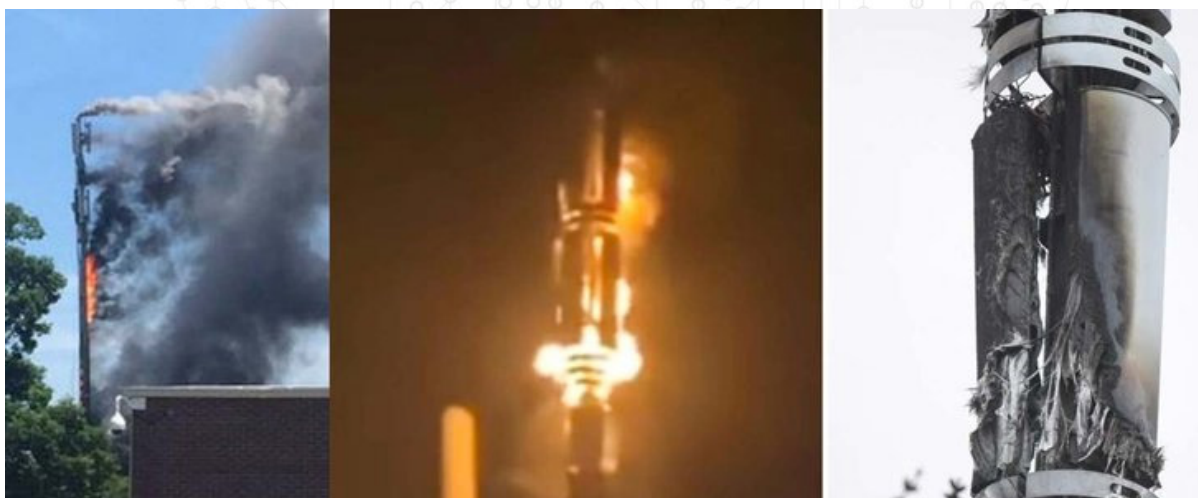oydon, south London, and seized around £20,000. He was arrested under the Fraud Act 2006 after making false and misleading claims about the tests' capability.

Two properties and a car linked to the suspect were searched. He was released on conditional bail. In a separate investigation, a 39-year-old surveyor from Uxbridge, west London, was stopped while driving his car. Inside the vehicle were 250 Covid-19 testing kits. Like the first suspect, he was arrested under the Fraud Act 2006 after making false and misleading claims about the capability of the tests.

Suspected arsonists target phone mast in London

A fire broke out at a phone mast in Dagenham, east London. Around 25 firefighters extinguished the blaze and nearby properties were evacuated. Police are investigating the incident. Mobile phone networks reported 20 further cases of phone masts being targeted by suspected arsonists during the Easter weekend. Vandalism of phone masts

has been prompted by fears that the 5G mobile network system is responsible for the spread of coronavirus (COVID-19).

UK spy agencies urge China rethink once Covid-19 crisis is over

Britain's intelligence community believes the UK needs to reassess its relationship with China after the coronavirus crisis subsides and consider if tighter controls are needed over high-tech and other strategic industries. Issues being aired are whether the UK wants to restrict takeovers of key companies in high-tech areas such as digital communications and artificial intelligence, and whether it should reduce Chinese students' access to research at universities and elsewhere. MI6, the foreign intelligence service, and MI5, its domestic equivalent, still believe it was correct to allow Huawei access to Britain's 5G network, capped at 35%. https://www.theguardian.com/uk/uksecurity

Weapons seized in Organised Crime Partnership raid in Glasgow

Officers from the joint NCA and Police Scotland Organised Crime Partnership have arrested a man from Glasgow in connection with the alleged importation of firearms. OCP investigators executed a warrant in Bishopsgate Gardens, Colston, this morning, where they detained the 53-year-old. Their investigation follows the seizure of a disguised stun gun by Border Force officers carrying out checks on incoming mail. A search of the property in Colston identified a further two stun guns, and three other weapons which have now been sent away for forensic analysis. The man was later charged with firearms offences and released on an undertaking to appear at Glasgow Sheriff Court on 8 July 2020.

Border Force intercept 52 migrants off Dover

Border Force discovered at least 52 migrants attempting to cross the English Channel in four inflatable boats, the Home Office confirmed. The 52 individuals were Iraqi, Iranian and Afghan nationals. Authorities brought the migrants ashore at Dover. There has been an uptick in migrants attempting to cross the English Channel in small vessels in recent months.

Security Industry News

Access to online counter terrorism training made easier for home users

As the ACT (Action Counters Terrorism) Awareness e-Learning course marks its second anniversary, police are launching an updated version, with the latest advice from security experts and a simplified registration system so anyone wanting to take part can help keep the UK safe. Over 400,000 people have taken part in the award-winning programme since its launch in April 2018, together completing nearly 2.5 million modules. Nine out of ten participants said they would recommend the package.

It takes just 45 minutes to work through the six sections and can be done on a personal or work computer, laptop or tablet – all in one session or one module at a time. The course has prompted interest from police forces across the globe. It explains how to spot the signs of suspicious behaviour and what to do to help yourself, others and the emergency responders if an attack should take place. https://ct.highfieldelearning.com/

National Strategic Assessment of Serious and Organised Crime 2020

The National Crime Agency has published the National Strategic Assessment of Serious and Organised Crime 2020. It provides a single authoritative picture of the threat to the UK from serious and organised crime. It shows that we are confronted with a rapidly evolving threat that is becoming increasingly complex as criminals exploit the fast expansion of technology to engage in illicit activity.

Download the pdf National Strategic Assessment of Serious and Organised Crime 2020 (19.30 MB)
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020

NATIONAL CYBER SECURITY CENTRE (NCSC)

The NCSC supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future. Please see the links to this month's NCSC weekly threat reports.

https://www.ncsc.gov.uk/report/weekly-threat-report-3rd-april-2020

https://www.ncsc.gov.uk/report/weekly-threat-report-10th-april-2020

https://www.ncsc.gov.uk/report/weekly-threat-report-17th-april-2020

https://www.ncsc.gov.uk/report/weekly-threat-report-24th-april-2020

Demonstrations held / planned

Extinction Rebellion (ER) Poster campaign

On the 30th of April, ER announced the start of the No Going Back campaign. They will be fly posting over the doors of the most ruinous industries and businesses in our society to make clear that they cannot reopen for business as usual if we want to rebuild a better world; with a sustainable future that cares and respects everyone equally.

Two arrested after anti-lockdown protesters in stand-off with police on roof of Shrewsbury College

Two men have been arrested after staging a protest on the roof of Shrewsbury College against the coronavirus lockdown. They posed on the roof of one of the college's London Road buildings for more than five hours with a banner that said, "No more lockdown". One of the men was wearing white overalls and what looked like a gas mask, while the banner also had a logo very similar to that of independent girl's school Shrewsbury High. Police officers were called to the scene to attempt to talk the protesters down. https://www.shropshirestar.com/

5G and coronavirus: thousands of conspiracy theorists gather in Facebook groups to plot 'silent' protests


Thousands of people are assembling online to plot protests promoting the dangerous and baseless conspiracy theory that the coronavirus pandemic is somehow linked to 5G technology. More than 10,000 so-called 'truthers' have gathered in one Facebook group to plan a global protest for Easter Monday aimed at preventing the roll out of the next-generation cellular technology. The 'Worldwide Unified Protest Against 5G – Easter Uprising' group made a call-for-action despite Covid-19 containment measures preventing more than half of the world's population from assembling en mass.

The Facebook groups promoting the conspiracy typically cite unscientific and unverified research from second or third hand sources, yet it gains far more traction than peer-reviewed studies. The groups have proved so effective in stoking fears that some conspiracy theorists have begun to act in the real world, with at least 20 UK phone masts vandalised since last week by suspected arsonists. https://www.independent.co.uk/

UK phone masts attacked amid 5G-coronavirus conspiracy theory

Three recent mobile phone mast fires around the UK are being investigated as possible arson, amid concerns that people are attacking telecoms infrastructure because of a conspiracy theory linking 5G technology to the spread of coronavirus.
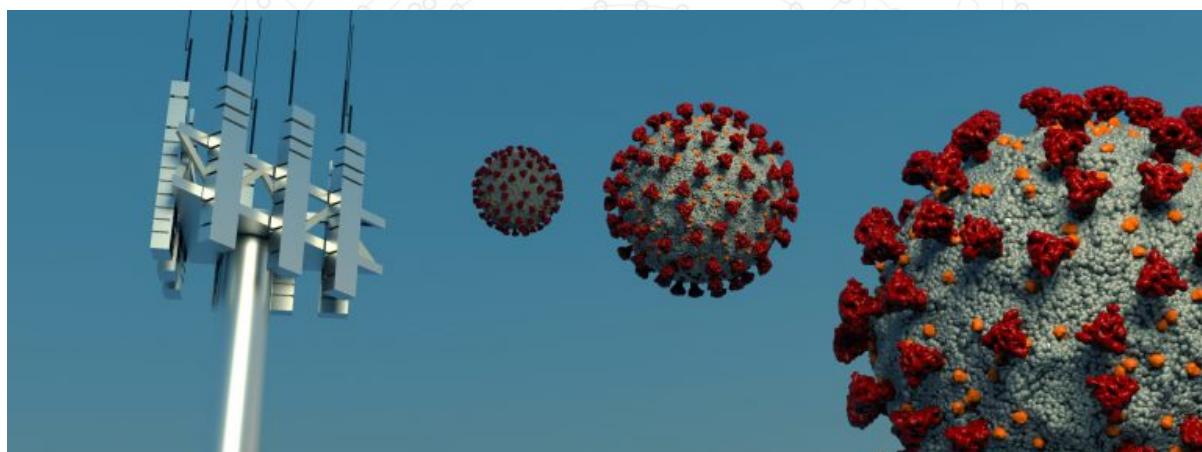
Emergency services were called to reports that a 5G mast was on fire in Liverpool shortly before 11pm. Police confirmed they were investigating the blaze at Spencer's Lane, Aintree, close to the M57 motorway.

Police in Belfast appealed for information after a mobile phone mast was damaged in an arson attack, with online footage suggesting the motive was opposition to 5G networks. The video clip shows an incident on the Antrim Road in north Belfast on Thursday night, in which flames can be seen at the base of a mobile telephone mast.

Facebook removed one anti-5G group in which members were being encouraged to supply footage of them destroying mobile phone equipment. Video footage of a 70ft (20m) telephone mast on fire in Birmingham has also circulated widely alongside claims it was targeted by anti-5G protesters.

Metropolitan Police Service Advice for Businesses

The Metropolitan Police Service advice for businesses relating to crime prevention and advised on practical steps to reduce the chances form becoming a victim of crime in the event of protests near your premises.

Protests on public land

The Metropolitan Police Service (MPS) is fully aware of the potential impact of any demonstrations on the local community and is well-equipped to deal with events should it be required.

The majority of protests are peaceful and under Human Rights legislation they are to be facilitated on public land unless certain exceptions apply. The core role of the police in this situation is to:

- Minimise and detect crime
- Prevent or stop breaches of the peace
- Regulate traffic if required
- Activate a contingency plan where there is an immediate threat to life and co-ordination of resultant emergency service activities.

Protests within private property

If a protest takes place on private property then the primary responsibility for the security of the property and the management of any trespass within the premise's rests with the landowner or company.

The venue being open to the public implies an invitation to all persons, but the landowner, manager or representative of the company can withdraw this invitation at any time if required.

Should there be an incursion onto your premises that is not disorderly and police are requested to attend, it should be stressed that the officers attending will expect a representative of the premises to request those trespassing to leave, whilst in the presence and hearing of the officer.

If the police are asked to assist in the ejection of trespassers, then they are acting as an agent of the company or premises and have no more powers and privileges than that of an ordinary member of the public. They would look to stand by to prevent a breach of the peace whilst the persons are encouraged to leave and escorted onto public land by shop/security staff.

If there are criminal offences apparent then officers will deal with these as they would in any normal situation.

Section 68 Criminal Justice and Public Order Act 1994 (Aggravated Trespass)
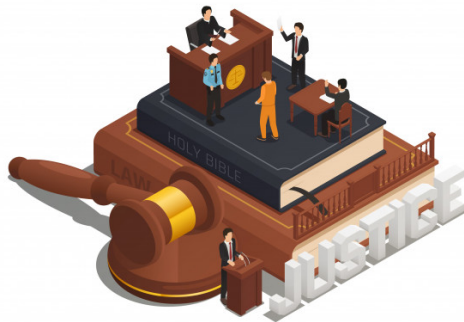
With reference to alternative legislation, 'mass action to disrupt the normal operation of the premises', the senior officer present may seek to use the above-mentioned powers. They would look to the land manager to support this process by providing confirmation of the way the business is being affected and that they are willing to provide a statement and attend court if necessary. Any CCTV in relation to the incursion would also need to be provided to the police at the earliest opportunity.

The practical aspect of this would be that a person in a position of decision-making ability in the company is willing and able to state, in the presence of the person(s), that they reasonably believe that the person(s) have trespassed on private property and that they have acted/are acting in a manner which is disruptive to the normal business of the store.

Protecting your businesses from protests and trespass

You can help to protect your business by taking a few sensible precautions. The following is a list of things to consider and is by no means exhaustive:

- Premises should be adequately staffed with prominent management present who can make themselves identifiable to police in the event of an incursion.

- Where possible security officers should have a visible presence on the premises.

- Ensure that all staff are fully briefed in the days leading up to a planned event.

- All staff should remain vigilant and report any suspicious activity to security and/or police.

- Consider minimising the number of entry points to your building.

- Ensure building perimeters are clear of any debris, dustbins, ladders or loose tools and equipment that could assist entry.

- Check that your emergency equipment/grab bags/ first aid supplies and radio communications systems are stocked and fully operational.

- Check and test your building security and emergency systems.

- Ensure all members of staff are fully aware of any emergency evacuation procedures.

- Ensure CCTV coverage is fully operational and can provide the highest recording resolution possible.

- If your building has scaffolding erected, or is in close proximity to scaffolding, then security staff should be aware of its potential for aiding access.

Coronavirus Covid-19 Related News

Coronavirus Covid-19 Advice from the Security Industry Authority (SIA)

A message from our Chief Executive SIA

This month we have introduced changes to the rules for the issue of Licence Dispensation Notices (LDN) - a facility for approved contractors. We have also taken steps to reduce the need for those renewing their licence to have to go to the Post Office. Details of these changes are outlined below.

To make it easier for approved contractors to quickly deploy staff in the current crisis:

A Licence Dispensation Notice (LDN) may be issued to an operative whose application is at Next Steps and has been paid for, rather than waiting until it reaches Checks in Progress.

The duration of LDNs has been extended from 10 to 20 weeks before needing to be renewed. This applies to both first and subsequent LDNs. We will keep these arrangements under review. More information on this change and guidance on the use of LDNs is available on our website.

Key developments include:

Remote training pilot-A key area of concern has been around training. We are piloting, under very carefully controlled conditions, remote training for some licence linked qualifications. We will be evaluating the pilot with a view to rolling this out more widely. This will be done only when we have assured ourselves that the systems of assessment are robust.

Approved contractor scheme assessments-In response to concerns raised by approved contractors, we have extended all annual assessments by an initial 3 months. We will review the extension at the end of this period.

Approved contractor fee payment extension-Approved contractors due to pay fees in the next three months will be given up to three months to pay instead of the normal 21 days. Any approved contractors wishing to take advantage of this should contact us via their business account.

Disclosure Scotland electronic applications-For individuals in Scotland applying for a licence, I am pleased to advise that Disclosure Scotland have created an electronic application process to allow for disclosure applications to proceed. This allows licence applications to progress and decisions to be made as normal.

https://www.sia.homeoffice.gov.uk/Documents/sia-covid-19-faq.pdf

https://www.sia.homeoffice.gov.uk/Documents/sia-advice-to-retailers.pdf

The Centre for the Protection of National Infrastructure (CPNI) has issued guidance on good personnel security practices during the COVID-19 pandemic.

This is intended to remind businesses to continue to address risks, even when usual security practices may be suspended or changed. Sadly, the threat to security from sophisticated hostile intelligence actors through to low-level criminals continues, and could even increase in the current environment

View guidance **HERE**

COVID-19 related assaults

Emergency and essential workers are facing assaults and aggression, say the authorities. Dorset Police report that between March 16 and April 14 – that is, the first month of the lockdown – Dorset had 40 occurrences of assault on police officers and emergency workers in the county. These have included being coughed and sneezed at with the threat of infection and physical attacks. Not all victims' occupations are recorded. However, Dorset had a further five reports of COVID-19-related assaults involving several occupations.

https://www.professionalsecurity.co.uk/news/case-xstudies/covid-19-related-assaults/

Government Guidance on Right to Work Checks and Visa Extensions during COVID-19 Crisis

The Government has published guidance for employers carrying out Right to Work checks for immigration status during the COVID-19 pandemic and have instigated temporary changes which employers may take advantage of to make processing easier during the pandemic crisis.

Checks can now be carried out over video calls

Job applicants and existing workers can send scanned documents or a photo of documents for checks using email or a mobile app, rather than sending originals

Employers should use the Employer Checking Service if a prospective or existing employee cannot provide any of the accepted documents

Read the Government guidance on Right to Work checks for immigration status https://www.gov.uk/government/collections/coronavirus-covid-19-immigration-and-borders

CO-VID 19 Mandate Fraud Advice

The threat from mandate fraud has increased during the COVID-19 response. This could result in organisations losing substantial amounts of money that will be difficult to recover. However, whilst mandate fraud is becoming more sophisticated, it is entirely preventable if your organisation is aware and takes the threat seriously. Current risks:

- Payment diversion / mandate fraud

- Identity fraud

- Misinformation campaigns (esp. 'cure'-related)

- Malware attached to coronavirus trackers

- Online shopping fraud

- Investment fraud

- Pension liberation fraud

- Data breaches (esp. unsecure video conferencing systems and failing PCI DSS)

- CEO fraud

- Phishing emails (generally)

Please find attached an HM Government Counter Fraud Function - 'Mandate Fraud' guidance document issued - 30 April 2020.

Please find attached the Fraud Advisory Panel-Bulletin 1 May 2020