CORPS RELAY

Prepared by: Mike Bluestone & Neil Shanks

Date: March 2021

CORPS SECURITY

COVID-19: Roadmap to Cautiously Ease Lockdown Restrictions

Towards the end of February, Prime Minister Boris Johnson announced his "roadmap to cautiously ease lockdown restrictions" in England. The roadmap provides the principles for easing, as well as four tests each stage must pass before progressing. England's roadmap would, if each step is taken at the predicted time, lead to the lifting of all restrictions on 21st June 2021.

Wales began the route out of lockdown in February with the return of some pupils to school, but does not yet have an anticipated date for leaving lockdown. Scotland have stated pupils will not return until at least April and have the most cautious roadmap of the three nations that have declared so far. Northern Ireland is yet to declare its roadmap for COVID but an announcement is expected soon.

What are England's Four Tests
The four tests are:

1. The vaccine deployment programme continues successfully.
2. Evidence shows vaccines are sufficiently effective in reducing hospitalisations and deaths in those vaccinated.
3. Infection rates do not risk a surge in hospitalisations which would put unsustainable pressure on the NHS.
4. Our assessment of the risks is not fundamentally changed by new Variants of Concern.

Lockdown Easing in March 2021

Each area has a different plan for easing lockdown, with Wales having already begun with the return to school for pupils aged 3-7 from Monday 22nd February. Here is how the published roadmaps compare in March 2021 (Northern Ireland are absent from this section):

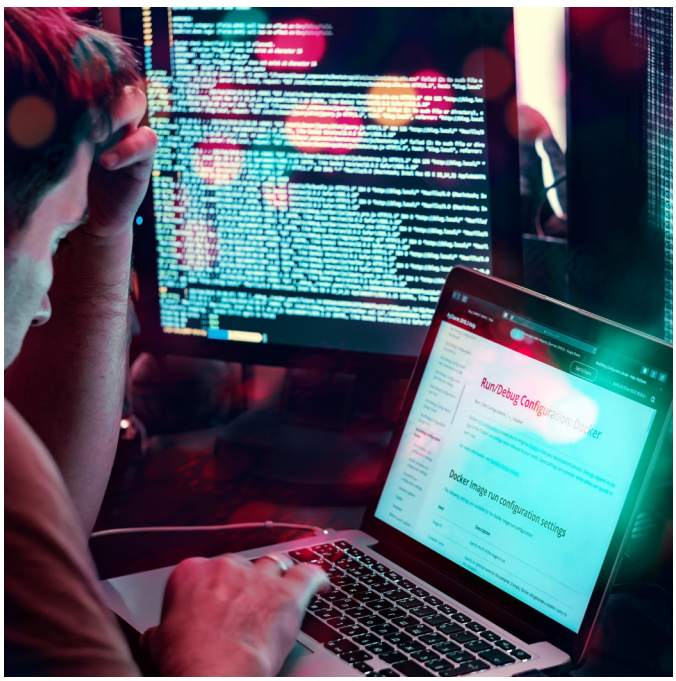
<table>
<tr><th colspan="3">England</th></tr>
<tr><th>8th March</th><th colspan="2">29 March</th></tr>
<tr><td>• Schools and colleges are open for all students including some students on practical higher education courses.
• Recreation or exercise outdoors with household or one other person. No household mixing indoors.
• Wraparound childcare.
• Stay at home.
• Funerals (30), wakes and weddings (6)</td><td colspan="2">• Rule of 6 or two households outdoors. No household mixing indoors.
• Outdoor sport and leisure facilities.
• Organised outdoor sport allowed (children and adults).
• Minimise travel. No holidays.
• Outdoor parent & child groups (up to 15 parents).</td></tr>
<tr><th colspan="3">Scotland</th></tr>
<tr><th colspan="3">15th</th></tr>
<tr><td colspan="3">• Four people from two households will be allowed to meet outdoors</td></tr>
<tr><th colspan="3">Wales</th></tr>
<tr><th>1st</th><th>12th</th><th>15th</th></tr>
<tr><td>• Venues for weddings reopen
• Review guidance for Care Home visits</td><td>• Review stay-at-home rule</td><td>• Non-essential shops may be open again
• Back to school for other primary and some secondary pupils</td></tr>
</table>

Lockdown Easing in April-June 2021

England		
12th April	**17th May**	**June 21st**
• Reopening of all shops • Pubs and restaurants can have outdoor service • Reopening of gyms, spas and close contact services	• Pubs can provide indoor seating • Groups of up to 30 can meet outdoors • Groups of up to 6 can meet indoors	• Lifting of all restrictions
Scotland		
15th April • Four people from two households will be allowed to meet outdoors		
Wales		
Easter (4th April) • Possible limited reopening of tourism • Possible return to school for remaining pupils		

Cyber Criminals Target Utility Providers

As technological advances continue to yield improvements in the workplace, more systems are controlled remotely. This practice is not new to utility providers who have controlled a number of their systems remotely for years. The cyber security of these systems is paramount, as proved by a recent incident in Oldsmar, Florida, U.S. A. A cyber criminal was able to gain access to the city's water treatment system and change the sodium hydroxide levels. They increased the level by 111 times the usual amount, making the water dangerous. Fortunately, one of the workers spotted this and changed it back before it could cause any harm. Complacency was a factor with this attack as a failed attempt to access the system was identified earlier in the day but it was incorrectly assumed to have been the Supervisor. The criminal responsible remains unknown and unapprehended.



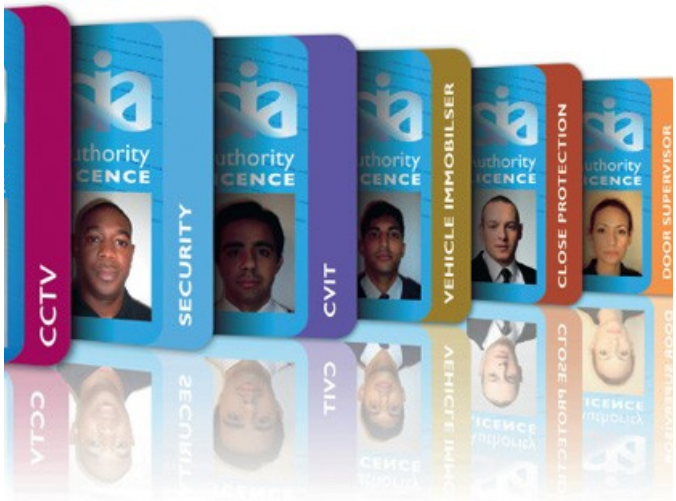
Corps Relay
March 2021

GRU Targets the Bundestag

A 55-year old German man has been charged with giving floor plans of the Bundestag, the German federal parliament, to a Russian agent believed to belong to the GRU. The individual charged was employed by a third-party company to maintain the electrical equipment within the Bundestag. The accused is alleged to have sent a data storage device containing the plans to an individual at the Russian Embassy who mainly worked for the Russian intelligence agency known as the GRU. This is the latest revelation regarding the GRU and the Bundestag. Numerous sources, including Angela Merkel, report that the GRU's Fancy Bear Group were responsible for the cyber-attack on the Bundestag in 2015.

Changes to SIA Training Requirements from April 2021

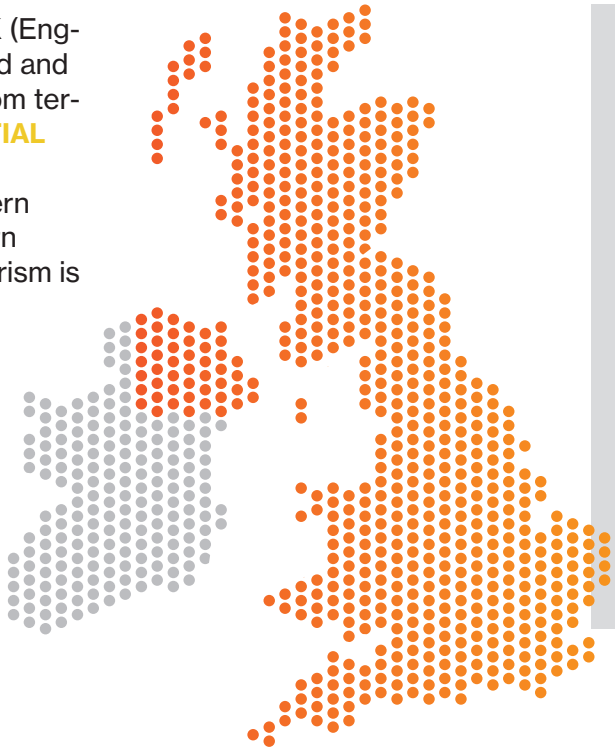
Following a public consultation, the SIA will soon require Door Supervisors and Security Officers to undertake additional training to that previously mandated. The additional requirements come into effect from next month (April 2021) for all new applications, and from October 2021 for licence renewals. Existing licence holders will be required to complete the "Top Up" training before renewing their licences and new licence linked qualifications will become part of the training for new applicants.



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

Anti-COVID Restriction Protests

As COVID-19 restrictions continue across the globe, people continue to attend protests against what they claim is an infringement of their liberties. Whilst the majority of these protests have been peaceful, a minority have descended into violence and destruction. The Netherlands saw anti-COVID rioting in response to the national curfew implemented on 23rd January, with one WhatsApp invitation instructing rioters to bring "Fireworks, dynamite, gasoline, bricks". An anti-lockdown protest in Dublin followed a similar route on the 27th February, with Police preventing hundreds of protesters attempting to gather in St Stephen's Green. The Police were attacked with fireworks and other debris, resulting in 23 arrests.

Shamima Begum Court Ruling

The Supreme Court has ruled that Shamima Begum does not have the right to return to the UK to fight the decision, made by the Home Secretary (which was Sajid Javid at that time), to remove her British nationality in 2019. The original decision to remove Ms Begum's citizenship was based on the grounds of national security. Lord Reed's statements in explaining the judgement made it clear that, in this case, national security was the primary factor, stating the Court of Appeal "had "mistakenly believed that, when an individual's right to have a fair hearing... came into conflict with the requirements of national security, her right to a fair hearing must prevail.". He went on to say that Ms Begum's right to appeal did "...not trump all other considerations, such as the safety of the public...". This case has been very high profile and will undoubtedly continue to attract attention. It will stand as a key moment in the UK's judicial history with regards to national security. Whilst the court challenges have ended, this case is likely to continue and develop within the public arena."

Notable Dates/Events

Key Religious or National CelebrationsKey There are significant days for several religions and nations in March 2021. It is not only important to be mindful of these to celebrate our diverse society, but also because several Terrorist Groups have been known to select the days for their actions based on significant days in either their own or their targets' calendars. For a full list of key dates, events and demonstrations, please view the "Corps Events Calendar" in the Customer Portal or on the "Corps Secure" App.

Notable dates in March 2021 include:

- 1st March – The Feast of St David/St David's Day – Celebration of the patron saint of Wales
- 8th March – Commonwealth Day - An annual celebration observed by people across the Commonwealth nations
- 10th March – Al-Isra' wal-Mi'raj/Isra' and Mi'raj – An Islamic celebration
- 11th March – Maha Shivaratri – A Hindu celebration
- 17th March – The Feast of St Patrick/St Patrick's Day - Celebration of the patron saint of Ireland and a Christian celebration
- 25th March – Feast of the Annunciation/Lady Day/ Conceptio Christi – A Christian celebration
- 28th March – 1st Day of Passover – A Jewish celebration
  – Holi – A Hindu celebration
  – Palm Sunday – A Christian celebration

Anniversary

Anniversary of the 2017 Westminster Bridge Attack

The 22nd March 2021 marks the fourth anniversary of the Westminster Bridge Attack. The incident, which commenced at approximately 14:40, involved Khalid Masood initially mounting the pavement on Westminster Bridge in his hired car. Mr Masood drove the car along the pavement, hitting pedestrians, until he crashed it into the railings outside the Palace of Westminster. Mr Masood then attacked PC Keith Palmer with a knife, killing him, before armed officers arrived and shot Mr Masood. The incident resulted in 6 fatalities (including PC Palmer and Mr Masood) and approximately a further 50 people injured.

Demonstrations

Autonomous Day of Action – Saturday 6th March (International)

The groups calling themselves Full Stop Affinity (FSA), Green Anti-Capitalist Front (GAF), Youth Liberation Front Affinity Group (YLF) and Trans 7 Non-Binary Queer Insurrectionary Anarchists are calling for an "Autonomous Day of Action". There are no locations given, or any indications of what action will take place, other than they will "target capitalism, target the state, paint the streets and squat empty buildings. Keep it quiet. Keep it serious". GAF have also advertised their intention is to "...create solidarity between our communities and destroy those who oppress us. Target the state.". Historic information suggests that the targets could include council offices, government offices and financial institutions, although no targets have been named. It is expected that London will be the main UK city affected, however, as this is part of an international movement, these groups could have identified targets in any major town or city.

Hackers

Corps Focus: Security Issue of the Month

This month's Relay referenced the vulnerability of governments and corporations to Cyber Criminals know as "Hackers". Hacker is a broad term referring to a type of activity conducted by individuals with hugely varied levels of skill and ability. There are a variety of classifications of "Hackers", the first of which can be one of an organisation's best defences against the others.

Types of Hacker:

1. **White Hat** – "Ethical Hacker" – Computer specialists and expert hackers. They are authorised to "hack" the systems they attack as part of a government or organisation's cyber security programme. They try to find weaknesses and loopholes in the cybersecurity of the system they are attacking which, once identified, will be fixed to avoid a Malicious Hacker from exploiting it. They may hold Ethical Hacker certification such as a Certified Ethical Hacker (CEH) Certificate.
2. **Black Hat** – "Malicious Hacker" – Like the White Hat, the Black Hat is also a computer specialist/expert. Unlike the White Hat, the Black Hat hacks into systems they do not have any authorisation to access. They may do so to gain/destroy/amend information, or for any other malicious reason. They gain access (through hacking) to a system without authorisation, with malicious intent, which is a criminal offence.
3. **Grey Hat** – "Not Malicious/Not Always Ethical" – The Grey Hat is the ambiguous middle ground between the Black and White Hats. Grey Hats work both defensively and offensively at different times. As it is the intention of the Hacker that determines whether it is a criminal offence or not, the ambiguity around the Hacker actions determines them as a Grey Hat.

4. **Green Hat – "New Hacker"** – Green Hats are students of hacking. They lack the knowledge to be a Hacker but their intention is to learn enough to become one. They may aspire to be a White, Black Grey or Red Hat.
5. **Blue Hat – "Vengeful Hacker"** – Blue Hats lack the full knowledge of a Hacker and have no intention of pursuing the subject further. Their main intent in hacking is status within a peer group and to use hacking maliciously against others. They are one step up from Script Kiddies.
6. **Red Hat – "Vigilante Hacker"** – The Red Hats are known to pursue a form of vigilante justice. Whilst a White Hat that discovered a Black Hat would aim to identify them and hand them over to the proper authorities, a Red Hat would launch an attack on them. These attacks often result in the destruction of the Black Hat's computer and resources.
7. **Script Kiddies** – These are amateur Hackers that use scripts written by actual Hackers to attempt to get access to systems. They lack the knowledge of a real Hacker and the scripts they use may have properties they are unaware of.
8. **Hacktivist** – These are individuals who promote a political agenda through hacking. They often use tactics involving defacing or disabling websites as an act of protest. They usually target governments or large corporations. They identify their cause as part of the hack, intending to influence the change they seek. Hacktivists can be lone actors or work as a collective, with groups like Anonymous which claim to be Hacktivists.
9. **Suicide Hackers** – These individuals aim to bring down critical infrastructure in the name of a cause, regardless of the personal cost. They differ from Hacktivists as the intent of their hacking is to cause damage, rather than embarrassment or raising awareness. Some members of Anonymous would also fit into this category.
10. **Cyber Terrorist** – These are individuals that use hacking as a medium to spread fear through disrupting systems/networks. They act in accordance with certain political or religious beliefs which influenced them in taking this form of offensive action. It is possible that the individual(s) that hacked into the Oldmar water treatment system fall into this category as their actions could have resulted in significant deaths influencing national fear and panic. However, until the perpetrator(s) are apprehended their actual motives cannot be ascertained and it is the intent, not the outcome, that is the key determiner for this form of hacking.
11. **State/Nation Sponsored** – These are Hackers that have been recruited by a government to gain access to the information of their chosen targets. They will often target the secret information of other governments. The GRU's Fancy Bear Group are an example of State Sponsored Hackers.
12. **Malicious Insider or Whistle-blower** – Insiders within a company have access to confidential information. If they decide to share it with an unauthorised person(s) or place it in the public domain, they become either a Malicious Insider or Whistle-blower. The rationale for their disclosure will determine which they are. Someone that uncovers illegal activity and shares it as they believe it to be in the public interest is known as a Whistle-blower. Someone that sells confidential information to a third-party, such as a competitor of the business they work for, is a Malicious Insider (the German man from the "GRU Targets the Bundestag" section is an example of a Malicious Insider).

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

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