Monthly *Threat* Update

February 2021

Pool Re SOLUTIONS
Building resilience against terrorism risk

Threat overview

	Critical: an attack is highly likely in the near future	**Severe:** an attack is highly likely	**Substantial:** an attack is likely	**Moderate:** an attack is possible but not likely	**Low:** an attack is highly unlikely
Threat from terrorism to the UK:			●		
Threat from Northern Ireland related terrorism to Northern Ireland:		●			

Threat Overview

There were no significant terrorist attacks in the UK or Europe in February. Despite a recent decline in terrorist activity and the reduction of the UK threat level to 'SUBSTANTIAL' from 'SEVERE', the threat of a terrorist attack occurring remains likely.

February witnessed the UK's youngest terrorist conviction and the deployment of increasingly sophisticated cyber and drone capabilities, evidenced by recent attacks in the US and Saudi Arabia. Both attacks showcased the growing intent and capability of violent groups to weaponise and utilise novel technologies to execute their attacks.

New methodologies were also the subject of recent warnings from Ben Wallace, the UK Defence Secretary, who warned of the growing threat of international chemical and biological attacks. On the domestic front, following the release of the government roadmap on the lifting of COVID-19 restrictions, opportunities for mass casualty attacks will increase and planned attacks, deferred due to the pandemic, may now materialise. Further afield, an attack in the Democratic Republic of the Congo on a United Nations convoy which killed the Italian Ambassador to the DRC, was condemned as a 'terrorist attack' by the DRC president Felix Tshisekedi.

Cyber-attack in Florida highlights vulnerability of Critical National Infrastructure

On 5 February, unidentified hackers remotely accessed a water treatment plan in Oldsmar, Florida, and changed the levels of lye in the drinking water. Lye is often used in the treatment process of water to adjust the pH value and can be dangerous in large quantities. The levels were altered from 100 to 11,100 parts per million. A worker noticed the attack before it could cause harm to the public. The hackers allegedly gained access to the computer architecture through a remote access tool that workers used to troubleshoot problems from other locations.

Whilst it is unlikely that a terrorist group was behind this attack, it illustrates the potential vulnerabilities of critical national infrastructure to cyber-attacks. Had the plant's systems been completely automated, it is possible the attack would have gone unnoticed and caused a localised public health crisis. Furthermore, as an increasing number of CNI facilities now utilise remote access tools as a response to work from home orders due to the coronavirus pandemic, a potentially large number of CNI facilities may be vulnerable to cyber-attacks.

Oldsmar, Florida, USA. 9th Feb, 2021. The Bruce T. Haddock Water Treatment Plant. Local and federal authorities are investigating after an attempt Friday to poison the city of Oldsmar's water supply. Photo: Chris Urso/Tampa Bay Times/ZUMA Wire/Alamy Live News

Certain CNI installations, such as nuclear and power plants, are obligated to have sophisticated cyber-security systems. However, water treatment plants, sewerage treatment, and similar infrastructure may not have such robust systems, processes and procedures in place. As a result of the pandemic, these vulnerabilities may be more acute as industries often prioritise business continuity, for example by relying on vulnerable remote access software, at the expense of cyber-security, thus increasing the risk of cyber-attack.

In further cyber news Conrad Prince, Senior Cyber Advisor to Pool Re, examined cyber supply chain security challenges in a blog in February 2021, which can be read here.

Italian Ambassador killed in potential terrorist attack in DR Congo

The coffins containing the bodies of the Italian ambassador Luca Attanasio and his bodyguard Vittorio Iacovacci, who were killed in an attack in the Democratic Republic of Congo. Photo: REUTERS/Yara Nardi.

At 08:39 on Monday, 22 February, the Italian Ambassador to the Democratic Republic of Congo and two of his security staff were killed in an ambush outside of the city of Goma in the east of the country, whilst travelling as part of a World Food Programme convoy. The Ambassador was shot during an attempted kidnapping, according to local sources. This attack marks the first murder of a sitting Western ambassador since the murder of Christopher Stevens in Benghazi, Libya, in 2012.

No group has claimed responsibility for the attack yet, although the Congolese authorities have blamed the Democratic Forces of the Liberation of Rwanda (FLDR), a Hutu militia. The FLDR has denied responsibility. It is possible the Allied Democratic Forces (ADF), a rebel group affiliated with Daesh's Central Africa Province, was behind the attack. Even if it was not the perpetrator, there is a chance that Daesh may claim responsibility, given the high-profile nature of the murder.

Other potential perpetrators include various Mai-Mai rebel groups, who have previously attacked NGOs in the region. The murder of the Ambassador highlights the strategic importance placed on Western diplomatic staff and interests to armed groups in the more restive regions of the world. Western interests abroad will likely remain a target for Daesh and other Islamist groups in the coming months. Local employees of Western businesses operating in more volatile emerging markets are also vulnerable, particularly to Kidnap for Ransom.

Attacks still likely despite lower threat level

On Monday, 8 February, the Joint Terrorism Analysis Centre (JTAC) lowered the UK threat level from international terrorism from 'SEVERE' to 'SUBSTANTIAL'. This change indicates that an attack is likely, rather than highly likely to occur. The lowering of the threat level reflects a reduction in the momentum of attacks in Europe. The threat level had been increased to 'SEVERE' following an increase in the tempo of attacks in France and Austria between September and November 2020.

Although the threat level has changed, the corresponding Government response level remains the same, at 'HEIGHTENED'. A 'HEIGHTENED' response level suggests implementing "additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk." The recent change in the national threat level to 'SUBSTANTIAL' does not indicate that the threat has dissipated, but instead suggests that the pace and scope of attack planning has slackened, and that the UK is better prepared to respond to threats.

For more on the threat level change, see here.

Defence Secretary Ben Wallace (left), during a visit on Friday to the Forth Valley Health Board's Vaccination Centre, at Forth Valley College in Stirling, where he spoke to military and NHS personnel. Photo: PA Images

Defence Secretary highlights growing threat of CBRN attacks

Ben Wallace MP, the Secretary of State for Defence, has warned of a growing threat of chemical, biological, radiological or nuclear (CBRN) attacks. The Secretary of State attributed this increase to a 'breakdown of world order' as states ignore conventional international laws on CBRN. He also affirmed that the internet has acted as a catalyst for terrorist groups or nation states to research and develop CBRN weapons. Wallace later highlighted that non-state actors are more easily able to utilise online instructions to create chemical weapons.

CBRN weapons can have a devastating impact on both people and the economy, as evidenced by the 2018 Salisbury poisonings, with the total cost estimated at around £150m. Terrorist actors in the UK have shown little capability in mounting CBRN attacks. However, actors across the threat spectrum have demonstrated some intent in developing CBRN weapons in both the UK and the rest of Western Europe. Several plots involving the biological agent ricin have been disrupted in France and Germany since 2017. Other agents of concern include anthrax, sarin and various nerve agents, all of which have been used in CBRN attacks since the 1990s. However, as the Secretary of State highlighted, as chemical weapons in particular become easier for terrorist groups to develop due to increasing availability of schematics and sophisticated technology, the capability of UK-based terrorist actors to employ chemical weapons in attacks may increase in the medium term.

Pool Re is at the forefront of terrorist use of CBRN research and modelling. As part of our commitment to increasing the understanding of the threat, Pool Re and the Biosecurity Research Initiative at St. Catherine's College, Cambridge (BioRISC) are hosting a conference of biological terrorism on 24-25 March 2021. For more on this and to register for the event, see here.

Concern over new terrorist methodologies following drone attack at Saudi airport

Houthi rebels in Yemen claimed responsibility for an explosive drone attack on a civilian airliner in Abha, Saudi Arabia on 10 February. The attack has raised fears over the increasing capabilities of terrorist groups to conduct destructive drone attacks. Four unmanned aerial vehicles (UAVs) were launched into Saudi Arabia, one of which hit a stationary plane at Abha airport. The fuselage of the airliner was lightly damaged in the incident. No injuries were reported from the incident. Three days later, Saudi air defences intercepted and destroyed another explosive drone launched by the Houthis against Abha airport.

New UAV technology capabilities pose an increased threat to the Middle East but also demonstrate the potential for new methodologies to be effectively deployed by terrorist groups. Terrorists have long had the intent, but now increasingly have the capability to use drones in attacks. The proliferation of cheap, commercially available drones has significantly increased the likelihood of them being used in attacks.

Disruptive drone incidents have been seen previously in the UK. The most notable incident in recent years was at Gatwick airport, which impacted 140,000 passengers, closing the airport runway for two days in the lead up to Christmas in 2018. Some estimates put the total loss as high as £200m.

A Saudi security officer walks past the Saudi Arabia's Abha airport. Photo: REUTERS/Faisal al Nasser.

The transfer of drone technology from the battlefields of the Middle East to Britain is a cause for concern, as UK-based threat actors and returning foreign terrorist fighters may emulate the methodologies of Islamist groups overseas. There have been no destructive drone attacks in the UK, although there have been 447 near misses involving drones at airports since 2010, peaking at 125 near misses in 2018, although it is doubtful terrorists were behind these incidents. The attack on Abha airport further demonstrates the vulnerability of the aviation sector to terrorist attacks. This attack was unusual as the targeted aircraft was stationary as opposed to an attempt during take-off or landing. As sophisticated drones become more readily available on the commercial market, the challenges of disrupting drones and the increasing intent of terrorist actors to use drones in their attacks will require security practitioners to mitigate the risk of attacks using UAVs, particularly in and around airports.

For more on the terrorist use of drones, see the Pool Re SOLUTIONS Threat and Mitigation Report 2019.

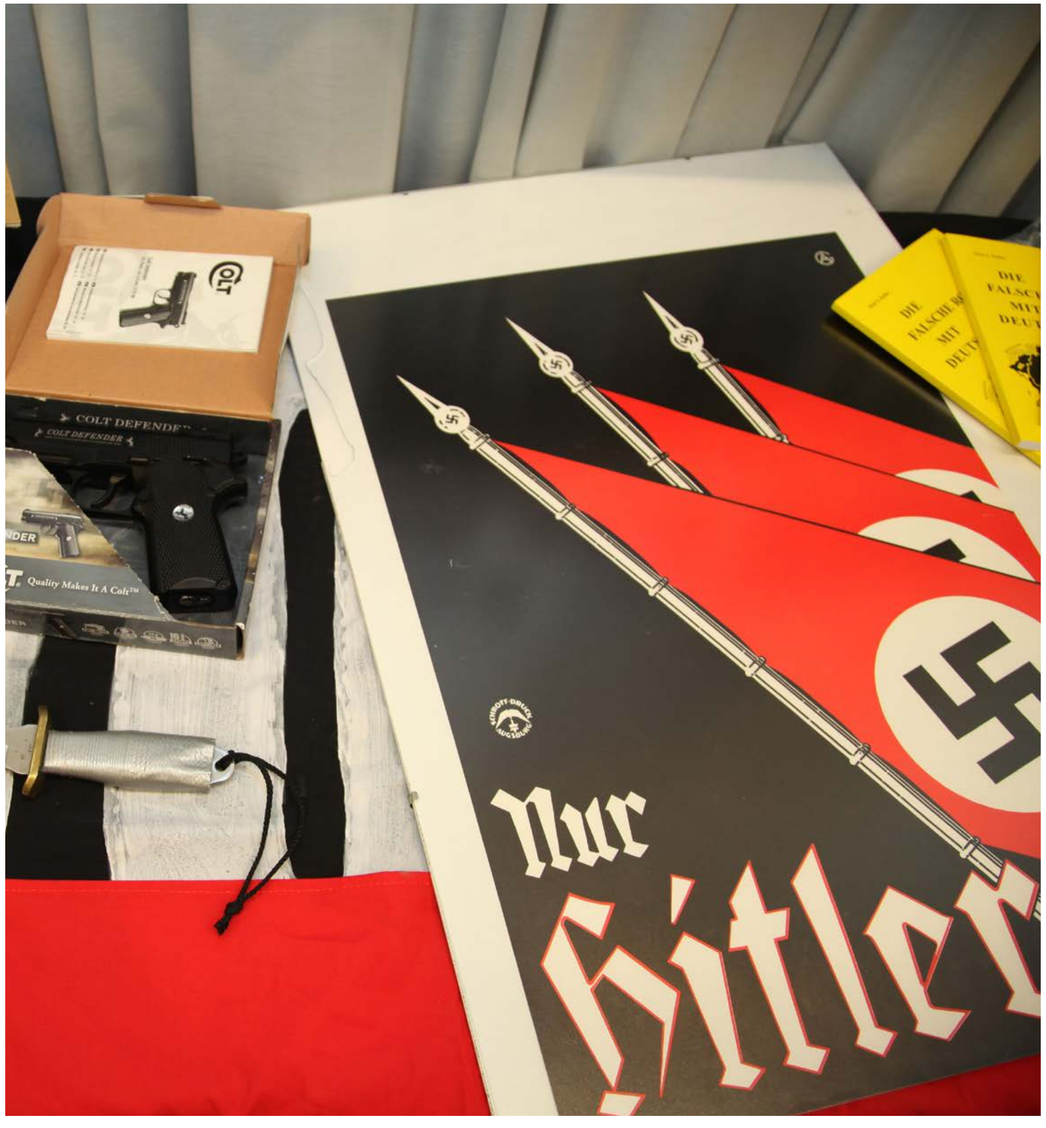
The rising threat of teenage radicalisation

Guest article: Andrew Silke, Professor of Risk and Resilience at Cranfield University

February saw the sentencing of Britain's youngest ever convicted terrorist. The boy was just 13 when he downloaded a terrorist bomb-making manual in 2018 and within a year he was orchestrating the online activities of a cell of the neo-Nazi Feuerkrieg Division. The case potently illustrated the vulnerability of teenagers to extremist self-radicalisation. Such vulnerability has long been recognised by Prevent workers in England and Wales, where teenagers have consistently made up the largest single group referred for attention and interventions.

More worryingly, however, are signs that radicalisation among teenagers has increased in 2020. Recent Home Office statistics show that terrorism arrests for teenagers reached their highest levels in 2020. Up to the end of September, nearly 8% of terrorism arrests involved teenagers, a new high since records began in 2002.

That radicalisation is rising among the young is not a surprise. In a report last year by Pool Re, we noted that the Covid lockdowns were witnessing a surge in engagement with online extremist material.



Within two weeks, far right extremist material for example had already shown a 21% increase in viewings compared to pre-lockdown levels. That this could translate into real world radicalisation was recognised then as a serious risk.

Teenagers in particular are susceptible to online extremist material for a range of reasons. Adolescence has long been recognised as a time when individuals explore their identities. Brain development in adolescence is also associated with heightened sensitivity to rewards, to peers, and to increased risk-taking behaviour. Identification with a radical cause or group can help provide a teenager with a powerful sense of acceptance, belonging and self-esteem.

Further, exposing teenagers and children to increasing violence is a common tactic used by many groups to radicalise child soldiers. Online extremist content can have a similar impact, desensitising teenagers to violence and hardening their sense of identity around an extremist framework.

Fortunately, most will not be so affected, but there are troubling signs that we are now seeing a rise in those who are vulnerable. As lockdowns ease, great care will be needed to try to ensure that online dynamics do not translate into real-world harms.

UK Government launches plans to protect public places from terrorist attacks

On 26 February 2021, the UK Government set out its proposals for a new Protect Duty; a legal requirement for public places to ensure preparedness for and protection from terrorist attacks. The proposals have been championed by victims' groups, including the Martyn's Law campaign, which was established by Figen Murray, who lost her son, Martyn, in the Manchester Arena attack in 2017.

The consultation will run for 18 weeks, closing on 2 July 2021 and will seek the views on:

- Who the Duty should apply to;
- What it will require stakeholders to do;
- How compliance should work; and
- How the Government can support those in scope.

Whilst subject to consultation, the intention is that the Duty would apply to specified owners and operators of public venues, large organisations and those responsible for public spaces. It would require those in scope to consider terrorist threats and observe and implement appropriate and proportionate protective security and organisational preparedness measures.

The full proposal can be found here.

Pool Re intends to issue a briefing note to outline the details and potential impacts to its Members. Working with members and the Association of British Insurers (ABI), Pool Re will also host a series of working groups with representatives from both the UK Insurance market and officials from the Home Office to discuss the Duty.

Further to the forthcoming briefing note, we will also be holding a Webinar for our Members and other stakeholders, involving the Publicly Accessible Locations Team from the Office for Security and Counter-Terrorism and ABI on 14 April. Further details will be announced in due course.

Interesting reads:

The Network of the November 2020 Vienna Attacker and the Jihadi Threat to Austria
https://ctc.usma.edu/the-network-of-the-november-2020-vienna-attacker-and-the-jihadi-threat-to-austria/

The Evolution of the Boogaloo Movement
https://ctc.usma.edu/the-evolution-of-the-boogaloo-movement/

Al-Qa`ida's Soon-To-Be Third Emir? A Profile of Saif al-`Adl
https://ctc.usma.edu/al-qaidas-soon-to-be-third-emir-a-profile-of-saif-al-adl/

Commission for Countering Extremism: Hateful extremism: The need for a legal framework
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/963156/CCE_Operating_with_Impunity_Accessible.pdf

Pool Re
SOLUTIONS
Building resilience against terrorism risk

Risk Awareness **Risk Modelling** **Risk Management**

Understanding risk, enabling resilience

Whilst the human cost of terrorism is devasting, the financial impact an incident can have on communities, businesses and economies is generally greater than most realise.

At Pool Re we understand that terrorism is a significant multi-faceted peril that can expose businesses in a complex way. Like many other catastrophic perils, terrorism is a challenge which requires a collaborative approach.

We have been the UK's leading terrorism reinsurer for over a quarter of a century. During this time our *SOLUTIONS* division have developed a specialist team of experts who can work with you to help you and your Policyholders understand and manage the terrorism threat.

We believe all organisations and businesses can benefit from a better understanding of the terrorism risk solutions available.

To find out more about Pool Re *SOLUTIONS* and how your organisation can take advantage of this service please contact us at: **solutions@poolre.co.uk**

Government advice

Click a logo for more information

ACT ACTION COUNTERS TERRORISM

CPNI Centre for the Protection of National Infrastructure

CSSC Cross-sector Safety and Security Communications

SECURITY SERVICE MI5

COUNTER TERRORISM POLICING UK Protect

SEE IT. SAY IT. SORTED.

RUN HIDE TELL

National Cyber Security Centre a part of GCHQ