G4S
An Allied Universal Company
Academy

UK TERRORISM IN 2022

A G4S BRIEFING PAPER

Contents

1. Key points

- The terrorism threat level in UK is assessed as **severe**, primarily stemming from individuals or small groups associated with Islamic State (IS) and increasingly from far-right groups.
- Terrorist actors, maintain a **high intent** of mounting attacks within the UK, generally aimed at soft targets. Despite the high intent of such actors to mount attacks, their **capabilities are generally low,** with weaponry and tactics constrained to small arms, homemade explosives or use of vehicles as weapons.
- The threat of terrorism has been exacerbated by the **COVID-19 pandemic**, which has increased the time that vulnerable people have spent online viewing harmful, extremist content, increasing radicalisation levels within the UK.
- Terror attacks in the UK are becoming increasingly difficult to prevent due to the lower capabilities of attack methodologies requiring less preparation and thus less time for authorities to identify threats.
- UK security forces are **highly effective** and maintain wide-ranging operations targeting suspected terrorist cells within the UK.
- The implementation of a revised counter-terrorism strategy on June 2018, which was created in response to previous attacks in 2017, further reduces the risk of terrorist groups carrying out attacks using similar tactics.
- In February 2021, the UK government launched the **Protect Duty** consultation to develop plans to make it a legal requirement for public and private venues to improve security measures, following a campaign related to the 2017 Manchester Arena attack.
- On 10 January, the government published its response to the **Protect Duty** public consultation. Findings show that the majority of respondents support tougher security measures to ensure preparedness for and protection from terrorist attacks.

2. Terrorism and UK's Terrorism Threat Levels

Terrorism is a growing threat in the United Kingdom and is defined as the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims. The UK's **terrorism threat level** is broken down into the **National Level** - the threat to the UK (England, Wales, Scotland and Northern Ireland) - and the **Northern Ireland-related Threat Level.**

For both systems, the UK uses a five tier scale Threat Level, ranging from "Low" where an attack is considered highly unlikely, to "Critical" where an attack is assessed as being highly likely in the near future. The current Threat Level in the UK and in Northern Ireland is **"Severe"**, which means that an attack is considered as being a highly likely possibility.

Figure 1: UK's National Terror Threat Levels. Source: M15Source: M15

The threat level for the UK from international terrorism is set by the Joint Terrorism Analysis Centre (JTAC), while MI5 is responsible for setting the threat levels from Irish and other domestic terrorism both in Northern Ireland and in Great Britain. The following factors are taken into account in order to determine the threat level.

- **Intelligence:** Known information about currently active terror groups or individual suspects, past precedent, recent activity and operations in other countries.
- **Capabilities** of threat actors, including common modes of operation, sophistication level, amount of planning required and previous types of attacks that can indicate how easily actors can mount attacks and in what locations their capabilities lend themselves to operating in.
- **Intent** of threat actors. The intent as to whether or not there is an increased motivation for threat actors to stage attacks such as relevant dates, public holidays, political developments or other triggering factors.
- **Timescale:** How quickly terrorist actors can coordinate attacks and what the current trend is regarding increasing or decreasing frequency.

The assessments are intended to guide security practitioners to assess the appropriate level of security mitigation measures given the existing threat.

Date	National Threat Level	Northern Ireland-related Threat Level to Northern Ireland
15 November 2021	SEVERE	SEVERE
4 February 2021	SUBSTANTIAL	SEVERE
3 November 2020	SEVERE	SEVERE
4 November 2019	SUBSTANTIAL	SEVERE
23 July 2019	SEVERE	SEVERE

Figure 2: Recent changes in threat level. Source: M15

Following the killing of MP Sir David Amess on 15 October 2021 and an improvised explosive device (IED) attack outside a hospital in Liverpool on 14 November 2021, the UK government raised the nationwide terrorism threat from **"Substantial"** to **"Severe"**, meaning an attack is assessed as "highly likely". The increase in the threat level was likely driven by the regularity of attacks throughout October and November 2021, rather than any credible increased threat of terrorism.

The threat from radicalised individuals, inspired by both Islamist or far right ideologies, carrying out attacks has increased in the UK and across Western countries since the start of the COVID-19 pandemic, as many vulnerable people have spent more time online viewing extremist content and away from support networks. Following the increase in the UK's terrorism threat level, the Metropolitan Police has urged people in London to be vigilant in crowded spaces, with police patrols also increased across London during the 2021 festive holiday season. According to the Head of MI5, a total of 31 late-stage terror plots have been foiled in the UK in the past four years, most of which are related to Islamic extremist, but there have been a growing number planned by right-wing terrorists.

2.2 Types of terrorism

Terrorism threats - international, domestic and from Northern Ireland - all are assessed as currently posing a severe national security threat to all parts of the UK.

2.2.1 International / Islamist - the highest threat

International terrorism is any activity linked to or motivated by a terrorist organisation based outside the UK. According to the UK government, Islamist terrorism is defined as "individuals from Islamic proscribed groups who advocate, justify or glorify acts of violence (especially against civilians) or other illegal conduct to achieve fundamental changes to society."

Islamist terrorists maintain a high level of **intent** to carry out attacks in the UK and pose a significant terrorist threat to the country. The high intent among these individuals is largely motivated by the UK's role in foreign conflict, particularly in the Middle East, as well as its contribution to counter-terrorism (CT) operations around the world. A part of the Islamist threat can also be traced to individuals who travelled to Iraq and Syria to fight with Islamic State (IS) and subsequently have returned to the UK to carry out attacks from within the country in coordination with small regional cells. Groups like IS and al-Qaeda are considered by the government to be "long-term global threats" with sustained high levels of intent to operate in the UK despite occasional periods of inactivity that usually coincides with heightened security pressure or other global triggering factors.

Global affiliates of major transnational terror groups like IS and al-Qaeda also have a key role in facilitating the capabilities and training of UK-based militants, particularly those involved in diaspora communities. For example, Salman and Hashem Abedi, the brothers responsible for the 2017 Manchester Arena attack, were known to have been in Libya for training ahead of Manchester attack. It is highly likely that they were trained with former al-Qaeda and Libyan Islamic Fighting Group (LIFG) members who facilitated their operations.

Islamist terror networks are also able to exploit the use of **migrant flows** into Europe and into the UK. IS and al-Qaeda regularly seek to use these migrant networks to project threats into Europe, particularly from Libya into Malta and Italy. Other routes include traveling through Sudan, which has relatively porous borders with states that have a high presence of terrorism like Libya, Egypt, Ethiopia, and Somalia. However, it is important to note that this is a minor proportion of migrants who are likely to be exploited by terror networks.

Other Islamist networks like the Al-Muhajiroun (ALM), while relatively low in capability, have a key role to play in inspiring and recruiting young and vulnerable people. Whilst the ALM was officially banned in the UK in 2005, a covert network and its group leaders remain active in radicalising individuals linked with the majority of UK terror attacks over the past ten years. Individuals such as Anjem Choudary, who was released from prison in 2018, have previously been key members of ALM in the UK. While under strict watch by the government, his release and his restored right to speak in public, could potentially see an increase in covert ALM activity and attack plotting.

Despite the known presence of organized groups in the UK, most of the Islamist threat in the UK stems from "lone wolves". While the term has been criticised by some, as to whether an individual can act completely in isolation, the term describes a threat actor who, despite being inspired by terrorist groups or individuals, has no known affiliation with any larger group. Currently, across UK prisons, the majority of prisoners incarcerated on terrorism offences are classed as Islamist terrorist threats, with a total of approximately 157 incarcerated individuals, compared with 44 from far-right extremists as of March 2021, illustrating the sustained threat from Islamist extremism across the UK. Prisons also provide fertile grounds for radicalisation across the UK.

The **COVID-19 pandemic** has also contributed to a heightened threat of radicalisation and growing intent amongst Islamist extremists as extended periods of lockdown have allowed vulnerable citizens to spend more time online viewing potential harmful or extremist content, away from their support networks. Amid an easing of COVID-19 restrictions driven by globally rising vaccination rates, 2021 saw an uptick in lone-wolf attacks, primarily of low-capability, across Europe. As highlighted by the change in threat level, growing radicalisation, as well as global events, such as the Taliban takeover of Afghanistan, will likely continue to encourage radicalised individuals to carry out inspired attacks, posing a growing threat to UK security. Whilst the change in radicalisation may not be instant, it is likely that there will be an increase in attempts at online inspiration and the radicalisation of individuals in the UK as Afghanistan becomes a potentially more permissive environment for al-Qaeda.

Capabilities

Despite the high intent of such actors to mount attacks, their **capabilities are generally low,** with weaponry and tactics constrained to small arms, homemade explosives or use of vehicles as weapons. These attacks, which tend to be carried out by a single individual or a small group, tend to be difficult to prevent and detect and often rely on taking advantage of the delay prior to the arrival of security forces at the scene. There is no indication that Islamist militant capabilities have become more sophisticated in recent years and there have been no examples of complex cyber-attacks or ransomware emanating from Islamist extremism.

Terrorist groups are able to increasingly exploit advances in technology to communicate anonymously, often over encrypted messaging services. The use of sites like Telegram, an online instant messaging service popular among IS, remains vital to the organization's communication system. The platform offers strong functionality, as well as a track record of relatively lax enforcement of Telegram's terms of service, giving IS militants an easy to use way for members to engage with like-minded supporters. Calls for the removal of encrypted messaging options like WhatsApp and Telegram or for the placing of back doors into encrypted applications would likely only push terror communications into locations that are harder to monitor for western authorities.

Funding - The use of cryptocurrencies

Terror networks now also have access to a larger variety of funding options, including ones that are harder to trace as well as more lucrative. The rise of cryptocurrencies has served both as a way of terror groups to profit through Bitcoin mining and as a way to anonymously finance various parts of their network such as criminal groups that provide drugs, weapons, fake travel documents. A large portion of this funding occurs on the dark web, as seen in January 2020 when authorities uncovered a dark web website called "Fund the Islamic struggle without leaving a trace". This exploits the ability of cryptocurrencies to be transferred directly and anonymously, meaning higher amounts of money can be transferred with a lower risk of detection by authorities due to the lack of a centralised financial institution to oversee transactions.

Notes: includes persons on remand as well as those sentenced to prison. Figures for 31 March 2021 are not directly comparable with previous years.
Source: Home Office, Operation of police powers under the Terrorism Act 2000 and subsequent legislation: financial year ending March 2021, table P.01, 10 June 2021

Figure 3: Ideology classification of recent terrorism prisoners. Source: HMG.

Targets/high-risk areas

Attacks target mostly crowded public spaces, such as transport systems, stadiums, markets and shopping centres. Targets such as city squares, bridges, markets and large events, all of which have high levels of foot traffic pose attractive targets due to having high impact potential but are often stopped quickest due to a higher presence of security forces. Finsbury Park and London underground stations such as Parson's Green have also been targeted in recent years for their high concentration of people and ease of access.

Venues that are considered symbolic of western values or that are perceived to oppose Islamic values such as music venues and nightlife locations represent visible and high-profile targets for Islamists terrorists. This is highlighted by the Manchester Arena bombing or the London Bridge attacks, both of which targeted central urban symbols.

Government buildings also remain attractive targets, particularly parliament and other symbols of government; however, extensive security measures in place means that lower-capability militants pose a reduced threat to these targets. There is also a growing threat to public officials and members of parliament. On 15 October, MP Sir David Amess was killed after being stabbed multiple times by an assailant with extreme Islamist views. The attack illustrated the vulnerability of MPs while in their constituencies and has led to calls to better secure and regulate who has access to high profile politicians while they return to their constituencies. The attack on Sir David Amess represents one of the most high-profile incidents in recent years, since the murder of Jo Cox in 2016, highlighting the threat posed to MPs as potential targets.

Targets/high-risk areas

Attacks target mostly crowded public spaces, such as transport systems, stadiums, markets and shopping centres. Targets such as city squares, bridges, markets and large events, all of which have high levels of foot traffic pose attractive targets due to having high impact potential but are often stopped quickest due to a higher presence of security forces. Finsbury Park and London underground stations such as Parson's Green have also been targeted in recent years for their high concentration of people and ease of access.

Venues that are considered **symbolic of western values** or that are perceived to oppose Islamic values such as music venues and nightlife locations represent visible and high-profile targets for Islamists terrorists. This is highlighted by the Manchester Arena bombing or the London Bridge attacks, both of which targeted central urban symbols.

Government buildings also remain attractive targets, particularly parliament and other symbols of government; however, extensive security measures in place means that lower-capability militants pose a reduced threat to these targets. There is also a growing threat to public officials and members of parliament. On 15 October, MP Sir David Amess was killed after being stabbed multiple times by an assailant with extreme Islamist views. The attack illustrated the vulnerability of MPs while in their constituencies and has led to calls to better secure and regulate who has access to high profile politicians while they return to their constituencies. The attack on Sir David Amess represents one of the most high-profile incidents in recent years, since the murder of Jo Cox in 2016, highlighting the threat posed to MPs as potential targets.

Recent terrorist incidents (international / Islamist)

Date	Location	Description
November 2021	Liverpool	A homemade bomb was detonated outside the Liverpool Women's Hospital, inside a taxi. The bomb killed the assailant and injured the driver.
October 2021	Southend-on Sea	MP Sir David Amess was stabbed to death by an Islamist extremist while hosted a surgery at his constituency.
June 2020	Reading	An assailant attacked two groups of people socialising in Forbury Gardens, killing three people and injuring another three.
February 2020	Streatham, London	The assailant, while wearing a fake suicide vest, was shot dead by armed police after stabbing and injuring two people.
November 2019	London Bridge	Two people were killed in a stabbing attack and three were left injured. The attacker was shot dead by police.
August 2018	Westminster	A car drove into three pedestrians outside the palace of Westminster, injuring all three and attempting to hit two police officers.

2.2.2 Domestic / far-right & left-wing - a rising threat

Far-right extremists remain intent on carrying out attacks across the UK, largely motivated by political issues such as rising immigration and the perceived constraint of civil liberties, an issue exacerbated by the COVID-19 pandemic. The far right are not a unified organisation and are spread out across various, often nebulous groups.

Support for these groups has been increasing in recent years, predominantly supported by the use of social media in which these groups can spread their messages and organise themselves. These groups often use sites such as Telegram, which remain outside the reach of security forces, to organise protests and spread their message.

Data published by the Home Office in November 2021, shows that half of the most serious cases of suspected radicalisation reported by schools and colleges in England and Wales in 2020 now involve far-right activity, with extremists using COVID-19 related topics and online gaming as the main ways of recruiting young people. Only one in five of the cases reported were related to Islamist extremism.

It is difficult to estimate both the level of support for the far right in the UK given its lack of centralised, hierarchical organisation. The most radical groups such as National Action, which is now outlawed, seem to have little support outside specialized and often difficult to access forums and servers, often active on the dark web. Outside of these niche and exclusive locations, there is a relatively large amount of support for neo-Nazi, neo-fascist and populist ideas available online, including on more mainstream social media sites, but whether the support translates into an increased number of people willing to stage attacks or who have the capability to do so is unclear.

Some known far Right Groups with a UK presence:

- The Base (banned in July 2021)
- Sonnenkrieg Division (banned in February 2020)
- System Resistance Network - alias of National Action - (banned in February 2020)

The capabilities of the far right have improved since 2019, in part due to the spread of their ideas, which have attracted increased support. Attacks are generally of low capability, utilizing small blades or knives, as opposed to high-capability, coordinated attacks by domestic or international organisations. Radicalisation of vulnerable people has increased, with far-right groups exploiting global or domestic political events, such as the migrant crisis and the COVID-19 pandemic, to create polarisation and increase their support base. MI5 has stated that teenagers are now comprising an increasing component of counter-terrorism case work, particularly related to far right radicalisation, due to the strong online element of the ideology, with children as young as 13 found to have been radicalised through online gaming and streaming sites.

While the COVID-19 pandemic has played a role in radicalising people into far-right ideologies, not all far-right members are opposed to COVID-19 vaccinations or lockdown measures. Although findings indicate that up to 10 percent of the NHS, and large sections of the UK Black, Asian and minority ethnic (BAME) community are against vaccination and lockdown restrictions, this does not imply that they support right-wing ideologies or related violent activity.

While attacks remain of relatively low capability, far-right attacks in other parts of Europe indicate growing capabilities to increase the impact. For example, a small IED attack targeting a vaccination centre in the Netherlands in March 2021 was perpetrated by a local far-right group. In Italy, a Molotov cocktail attack on a vaccination centre in Brescia also illustrates the growing capabilities and intent to carry out violent attacks.

Several UK citizens have been arrested since 2019, all of which were plotting attacks to target immigrants, Muslims, members of the LGBTQ+ community and police stations. In 2020, MI5 confirmed that eight out of the 27 late-stage terror plots foiled by the government came from the far right, meaning they now pose a significant threat across the UK. Further, the majority of cases referred to the UK's "Prevent" de-radicalisation programme are from far-right threats indicating an increase in its prevalence and therefore likely its capabilities among the youth of the country. There were 1,229 referrals owing to concerns related to extreme rightwing radicalisation in the year ending 31 March, and 1,064 because of suspected Islamist radicalisation.

Targets/high-risk areas

Far right extremists remain intent in carrying out attacks across the country, primarily targeting locations close to them as these often provide potent symbols for the ideology, such as government buildings, mosques, media companies and more recently with the pandemic, specific companies such as pharmaceuticals and departments involved in the production and distribution of vaccines.

Further, they are likely to target individuals and groups who they consider not to fit or against their ideals. Far-right and white supremacist actors are also increasingly targeting high-profile individuals in order to generate the most media attention and to generate fear that their capabilities are high enough to target high-profile people traditionally seen as heavily secured, as seen in the 2016 murder of MP Jo Cox in West Yorkshire.

Recent terrorist incidents and arrests (domestic / far right)

Date	Location	Description
November 2020	London	A police officer was arrested for his membership of the far-right group "Feurkrieg Division".
September 2017	Nationwide	Three men arrested for membership of the neo-Nazi organisation called "National Action".
June 2016	Birstall	A white supremacist murdered MP Jo Cox outside a surgery in her constituency.
April 2013	Birmingham	A right-wing extremist fatally stabbed one person and later detonated a homemade bomb outside a mosque.
April 1999	London	A far-right extremist detonated three nail bombs in London targeting the black, Bangladeshi and gay communities, killing three people and injuring 129.

Left-wing Terrorism

MI5 have also been increasingly investigating the activity of far-left terror organisations and other far-left pressure groups such as Insulate Britain which are often responsible for significant disruptive protest activity and who's members promised to escalate their tacticsfollowing recent court appearances. Although the number of left-wing terror cases investigated are in the single digits, according to MI5, and only represent a minor threat, it is possible that, as environmental crises worsenmovements become more notorious and engaged, pressure groups on the far-left could increase their activities and become a more prominent threat.

2.2.3 Northern Ireland

According to MI5, "dissident republican terrorist groups pose the most significant threat to national security in Northern Ireland." The nature of the terrorist threat in Northern Ireland has changed significantly in recent years. The Provisional Irish Republican Army (PIRA) and the main loyalist groups have ceased their terrorist campaigns and engaged with the political process. However, dissident republican groups rejected the political process and the institutions created by the Good Friday Agreement, which was signed in 1998, and continue to carry out terrorist attacks.

There are four main active dissident republican groups in Northern Ireland: the New IRA, the Continuity IRA (CIRA), Óglaigh na hÉireann (ONH – which recently split into two factions ONH and IRB), and Arm na Poblacht (ANP). All of which oppose the peace process and regard violence as a legitimate means of achieving a united Ireland. These groups are also often significantly involved in criminal activities for personal financial gain, including smuggling and extortion, which are often used to fund terror activities.

Common tactics for these groups include targeted attacks against police and other security forces, as well as violent attacks against people within the communities deemed to hold contrary views.

Whilst there is continued intent within the New IRA and other dissident republican groups to launch attacks on mainland UK, it is thought that the capability amongst these groups, to carry out a major attack on mainland UK, may not yet be in place. While there have not been any major terrorist incidents in Northern Ireland in recent years, police make relatively regular arrests of citizens suspected of assisting or of being part of terror organisations. Police arrest suspected bomb-makers and criminals that supply terror networks with financial support. Most recently, in December 2021, a 52-year-old woman was arrested in the Creggan area of Londonderry under the Terrorism Act as part of a police investigation into the New IRA's bomb-making activities including how the group store and maintain their explosive devices and equipment.

2.3 2022: Rising threat of terrorism

The recent elevation of the UK nationwide terror threat from substantial to severe illustrates the growing threat posed by terrorism. The threat from radicalised individuals carrying out attacks has increased across Western countries since the pandemic began in early 2020 as many vulnerable people have spent more time online viewing extremist content and away from support networks. Former MI6 boss Sir John Sawers warned that the UK's terror threat level had also risen following the Taliban's takeover of Afghanistan, as radicalised individuals feel emboldened to carry out attacks.

The increase in frequency and intent can be seen in the 15 October attack in which UK Conservative MP David Amess was killed at his constituency meeting in Essex by an individual inspired by Islamist extremism. The attack was the second reported in Europe in the month of October, after a man killed five civilians with a bow and arrow in the town of Kongsberg, Norway on 13 October in a similarly attack intended to instill fear and generate media attention. These attacks highlight the rising threat of lone-wolf attacks across Europe, which are often of low-capability, involving knives, guns or small blades weapons, and are generally exceptionally hard to detect ahead of time.

A similar trend can be observed from the far right with rising concern from security sources over the number of attack plots generated and being foiled by right-wing terrorists. MI5 has reported that over the past four years they have prevented 31 late-stage terror attacks. The recent EU Terrorism Situation and Trend Report 2021 published by Europol earlier this year stated that Europe experienced nearly 60 completed, failed, and foiled terrorist attacks in 2020.

Despite this, Jihadist terrorism will likely remain the greatest threat to Europe, with the number of completed jihadist-motivated attacks increasing each year since 2019. The threat from Islamist terrorism can also leed to an increase in social tensions, as highlighed by issues such as the caseof Shamima Begum and the debate around her eligibility to maintain her UK citizenship after returning from Syria. The controversy around this has placed a burden on government resources and led to a debate regarding the treatment of returnees from Iraq and Syria.

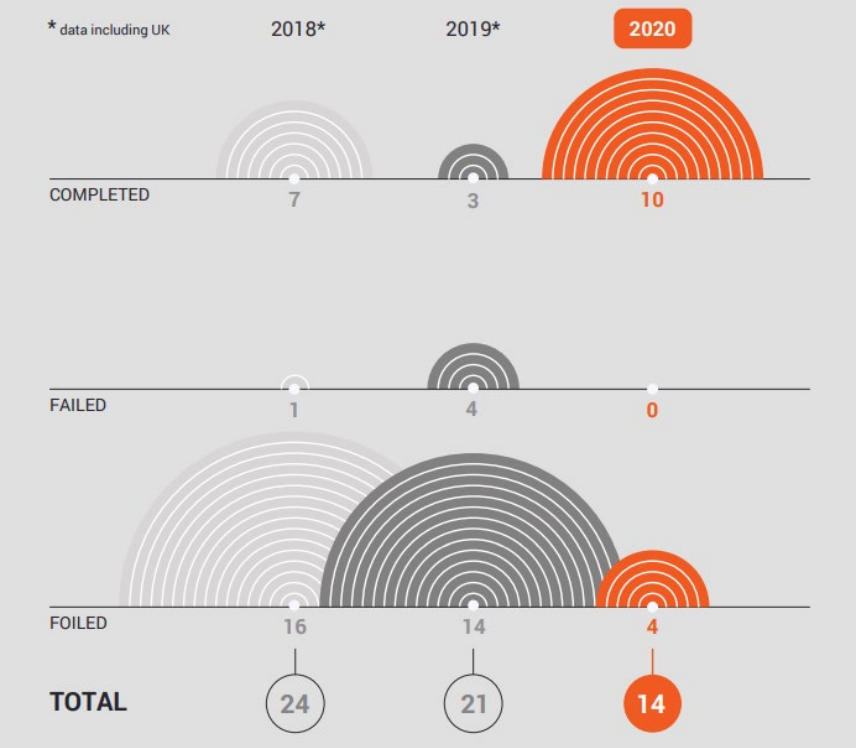

Figure 5: Islamic terrorist attacks in the EU in 2018-2020. Source: European Union Terrorism Situation and Trend Report 2021 by Europol.

Recent foiled terrorist attacks

Date uncovered		Location	Description
October 2019	Safiyya Shaikh	London	Planned to put an explosive device at St Paul's Cathedral and a hotel.
July 2019	Mohiussunnath Chowdhury	UK	Planned a series of attacks targeting a gay pride parade and Madame Tussauds
2018/2019	Lewis Ludlow	Kent	Planned to carry out an attack in London.
July 2017	Jack Renshaw	Warrington, Lancanshire	Planned to murder Rosie Cooper MP and a police officer.
July 2017	Peter Morgan	Edinburgh	Began to assemble an explosive device.
June 2017	Ethan Stables	Barrow-in-Furness, Cumbria	Planned to attack an LGBT event.
May 2017	Liam Seabrook	Thornaby, Middlesbrough	Stockpiled weapons and made threats to kill.
November 2014	Connor Ward	Banff, Aberdeenshire	Acquired bomb making components and kept a list of mosques.
February 2012	Michael Piggin	Loughborough, Lancanshire	Stockpiled weapons.

3 Cyber-terrorism - a growing threat

Various hostile actors, including terrorists, maintain intent to use the cyber space to harm UK interests. Cyber-attacks can be carried out by state actors, as well as by non-state actors with criminal intent, for example to extract ransom payments or to steal sensitive information with the aim of selling this on the black market. However, cyber experts believed that until recently, most of the attacks targeting Critical National Infrastructure (CNI) were often carried out by state actors as opposed to criminals motivated by profit.

It is likely that successful major cyber attacks require the backing of a state, most likely from Russia, China or Iran. This due to the fact that targeting CNI carries a higher risk and requires a higher level of specialised knowledge and tools than targeting standard commercial business. Other forms of online hostile foreign activity by state actors include the manipulation and promotion of misinformation online, with the aim to undermine the government's legitimacy or influence a political outcome.

There is a growing threat of cyber-attacks worldwide and in the UK, due to the growing intent of threat actors and their increasing capabilities. The UK's National Cyber Security Centre (NCSC) dealt with a record 777 cyber incidents between November 2020 and November 2021, up from 723 over the same previous period, with COVID-19 vaccine research centres representing one of the major targets for the majority of attacks.

The continued demand for remote working, as a result of the COVID-19 pandemic, provides additional opportunities for cybercriminals to exploit vulnerabilities in company systems by gaining access through unsecure networks. Furthermore, there has been a surge in cyber-attacks globally linked to the health sector and vaccines, including hospitals and research centres doing work around COVID-19, with ransomware being the most common attack type.

CI Sector	Frequency
Government Facilities	249
Healthcare and Public Health	163
Education Facilities Subsector	140
Information Technology	77
Critical Manufacturing	74
Emergency Services	67
Transportation Systems	58
Commercial Facilities	46
Communication	44
Financial Services	35
Energy	31
Food and Agriculture	25
Chemical	11
Water and wastewater Systems	7
Defense Industrial Base	5
Nuclear Reactors, Materials and Waste	0
Total	**1032**

Figure 6: Frequency of attacks worldwide from 2013-2021 by sector. Source: US data on ransomware attacks on CNI collected by Temple University.

Recent cyber-attacks in the UK

Date	Location - Sector	Description
December 2021	UK	Gumtree classifieds site suffered leak of personal data
November 2021	London - government	A vendor that handles data for the UK Labour Party was subject to a cyberattack.
May 2021	UK - government	The FBI and the Australian Cyber Security Centre warned of an ongoing Avaddon ransomware campaign targeting multiple sectors across various countries including the UK The targeted industries include academia, airlines, construction, energy, equipment, financial, freight, government, health, it, law enforcement, manufacturing, marketing, retail, pharmaceutical.
October 2021	Glasgow - business	Engineering firm hit by ransomware attack. Forced to delay shipments cost GBP 50 million.
October 2021	Sunderland - education	Sunderland University hit by cyber-attack, IT systems taken down.
October 2021	UK Comms Council - Nationwide	Sophisticated attack against Voice over internet Protocol (VoIP) - DDos attack.
August 2021	Isle of Wight- education	Six Isle of Wight schools hit by ransomware attack which encrypted all of its data
July 2021	Nottingham- transport	Nottingham City Transport hit by cyber-attack - prohibited access to emails and caused disruptions.
July 2021	UK - Northern Rail	Northern Rail ticket machines hit by ransomware attack - machines were down for a week.
January 2021	UK - Government	Hackers linked to Hezbollah breached telecom companies and internet providers in the UK for intelligence gathering and data theft.

3.1 Outlook: growing cyber-security threat

Although the UK is one of the leading countries in the world in implementing cybersecurity measures across its CNI sectors, ranking 88 out of 100 in the protection of nuclear facilities (Nuclear Security Index 2021), the threat of a cyber-attack is growing. The majority of business leaders are anticipating a rise in cyber-attacks in the coming year, with 61 percent believing that ransomware will pose the main threat. Ransomware, a type of malware, which threatens to publish a victim's personal data or perpetually block access to it, unless a ransom is paid, is a relatively accessible and affordable tool available to cyber criminals.

In response to the growing threat of cyber-attacks, which has accelerated since the COVID-19 pandemic, the UK has taken proactive measures to deter the threat of cybercrimes and cyberattacks. In December, the UK published the National Cyber Strategy for 2022, setting out a comprehensive framework to enable the UK to protect and promote its cyber interests. Its objective is that by 2030, the UK will continue to be a leading cyber power, able to protect and promote its interests and support national goals. The strategy is based around the following five pillars: investing in people and skills and closer collaboration between the government, academia and industry; building resilience and reducing cyber risk; building the UK's industrial capacity on technologies vital to cyber power; global leadership and influence; and enhancing national cyber security and countering threats.

Hostile state actors pose the most credible threat of being able to carry out major cyber attacks. Hostile state activity has been reported in recent years, most significantly during the 2018 Salisbury Novichok nerve-agent poisonings of Sergei and Yulia Skripal as well as a police officer attributed to the Russian government. The incident highlights the potential for hostile states to carry out attacks on UK territory and raises concerns over the possibility that hostile states could use their influence in other ways, including through manipulating political narratives and promoting misinformation online.

4. Counter-terrorism

UK security forces are highly effective and maintain wide-ranging operations targeting suspected terrorist cells within the UK. The implementation of a revised counter-terrorism strategy on 4 June 2018, which was created in response to previous attacks in 2017, further reduces the risk of terrorist groups carrying out attacks using similar tactics.

The 2018 Counter-terrorism strategy, known as (CONTEST), revolved around ensuring effective responses to the increasing terror threat and increased systemic coordination across the public sector, private sectors, communities, citizens and overseas partners. Each of these comprised a number of key objectives: prevent: to stop people becoming terrorists or supporting terrorism, pursue: to stop terrorist attacks, protect: to strengthen our protection against a terrorist attack, prepare: to mitigate the impact of a terrorist attack. The initiative renewed the focus on disrupting terror threats at the earliest possible stage by increasing resilience and awareness across the public and private sectors.

In February 2021, the UK government launched a consultation to develop plans to make it a legal requirement for public and private venues to improve security measures, following a campaign related to the 2017 Manchester Arena attack. The measures, which include free counter-terror training events for staff, and more thorough security checks for the public when entering these premises, will likely contribute to mitigating the increasing threat.

4.1 Counter-terrorism and Sentencing Act 2021

In April 2021, the government passed the Counter-terrorism and Sentencing Act, which put an end to the prospect of early release for anyone convicted of a serious terror offence. This marks a significant escalation in the sentences given to those convicted for the most serious terrorism offences.

Those found guilty of preparing or carrying out acts of terrorism where fatalities were reported or lives were placed at risk now face a minimum of 14 years in prison and up to 25 years on license, with stricter supervision. The legislation aims at improving the capacity of courts to consider whether a range of offences have a terror component/connection such as the supply or possession of firearms with a proven link to terrorist activity, expanding the courts ability to punish terrorist accomplices or supplier networks. The Act also aims at improving the capabilities of counter-terrorism police and the security services, allowing them to better manage the risk posed by terrorist offenders and individuals of concern who used to be outside of their custody, making it more likely they will prohibit attacks in the early stages of planning by making early, preventative arrests.

Finally, it redefined the scope of offences that can be classed as terror-connected and thus amplifies the legal mandate for police to request offenders with regular updates on changes to their circumstances, such as a new address or when they plan to travel abroad. This improves the capability of security forces to monitor network connections and any unusual activity within known criminal or terrorist circles.

4.2 Martyn's Law / Protect Duty

Martyn's Law, also known as "Protect Duty", is a piece of proposed counter-terrorism legislation that aims to create a coherent and proportionate approach to protective security, with a focus on securing events. The law applies to any place or space that the public has access to, ranging from small cafes to large arenas. The new regulation, which was proposed following the attack on the Manchester Arena in 2017, has five key components:

- A requirement that public spaces have access to and engage with freely available counter-terrorism advice and training. For example, ensuring that at least 25% of site event staff have received counter terrorism awareness training from resources such as the UK Government's National Counter Terrorism Security Office (NaCTSO).
- A requirement for organizations to conduct terrorism vulnerability assessments of their operating places and spaces.
- A requirement to carry out actions to mitigate risks identified in the vulnerability assessment.

- A requirement for organizations to have a counter-terrorism plan in place.
- A requirement for local authorities to plan for the threat of terrorism.

The law is designed to enable businesses to better assess and improve both the security environment and the preparedness of their businesses, their personnel and the public using the space in the event of an attack. It will encourage and educate businesses on how to identify security vulnerabilities as well as how to detect suspicious behaviour, mitigating the risk from lone-wolf attacks. Further, counter-terrorism and radicalisation training will be provided at no cost by the government, increasing the awareness and response capabilities of businesses.

4.2.1 Protect Duty consultation findings

On 10 January, the government published its response to the Protect Duty public consultation, which ran from February to July 2021. The consultation focused around the following four key areas:

- Who or where the legislation should apply to.
- What the requirements of the legislation should be.
- How compliance should work.
- How should the Government best support and work with partners?

Findings show that the majority of respondents support tougher security measures to ensure preparedness for and protection from terrorist attacks. Over 70 percent of respondents agreed that those responsible for publicly accessible locations should take appropriate and proportionate measures to protect the public from attacks. This included ensuring staff were trained to respond appropriately.

There was also agreement that venue capacity should determine when the duty applies, with most people expressing the need for measures to be proportionate to the size of each organisation, placing more responsibility on larger organisations to take proportionate action to ensure people are protected.

In terms of accountability, findings indicate strong views on the need for clear roles and responsibilities, particularly amongst event organisers, and those at senior level within venues and organisations. However, when it came to penalties to ensure compliance, results were divided, with those against citing the potential financial implication to organizations, including those resulting from legal action.

To further support the public and private sector, the Home Office announced it is collaborating with the National Counter Terrorism Security Office (NaCTSO) and Pool Reinsurance to develop a new interactive online platform, which is currently under testing, due to launch publicly this year. The platform will provide a central digital location for advice, guidance, e-learning and other helpful content. It will provide support for all organisations, not just those captured by the Protect Duty.

4.2.2 Challenges

Martyn's law faces several challenges before being fully implemented. One of the main obstacles remains ensuring all locations have access to reliable information on how to properly and consistently assess security risks. Correct understanding of the risks will help event organisers identify where the vulnerabilities lie. Coordination will be essential to ensure access to industry and government experts as well as to provide advice to both venues and local authorities.

The financial costs of implementing additional security measures is likely to pose another obstacle. Some event organisers might not be in a position to fund additional, mandated security measures. Furthermore, passing the cost onto event-goers may not be viable in the coming months, due to the impact of COVID-19 on the average household's purchasing power. Financial support from the government, particularly to small business, will be essential to a successful implementation across the industry.

5. Beyond traditional security

We'll go far beyond simple security delivery.

Our G4S Academy is open to all those that operate in the security industry and provides a unique opportunity for networking, CPD and a constant stream of intelligence - such as our weekly threat intelligence report.

Our G4S Academy providing a monthly security bulletin on potential as well as a repository of white papers, webinars and other continuous professional development material

Our Events and Seminars where guest speakers debate the latest market evolution and trends

Our Innovation Forum where we work closely with our customers to discus new security issues and how best to address emerging trends and technologies

Our Podcasts where we support continuous professional development through engaging debate - available at your leisure

An Allied Universal Company Academy

Listen to Noah's introduction and subscribe with our G4S Academy at

https://www.g4s.com/en-gb/what-we-do/academy

G4S
An Allied Universal Company
Academy

If you would like to find out more please contact us:

UK: 08459 000 447 (option 1)

enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447

g4ssales@ie.g4s.com