

POOL RE

REINSURING TERRORISM RISK

Terrorism Threat & Mitigation Report

August – December 2016

TMR-1-17

epic.org

EPIC-17-03-31-DHS-FOIA-20180416-Production-2

000001

NPPD 000720

Contents

Overview	01
Executive Summary	03
Terrorism: The United Kingdom and Europe	04
UK: Threat Summary	06
Europe: Threat Summary	07
Islamist Extremism Global Presence, 2016	08
Threat Trajectory: The United Kingdom and Europe	10
When, not if?	12
The Resilience of Al Qaeda	14
CBRN	16
How 'clean' is 'clean enough'? The Threat of Chemical, Biological, Radiological & Nuclear Terrorism in the UK	17
Cyber Terrorism	22
Trending: #CyberTerrorism	23
Emerging Risk Report: Drones	26
Unmanned Terror	27
Risk Mitigation and Resilience	30
Building Resilience	31
Notes	35




This document was prepared by Pool Reinsurance Company Limited (Pool Re). While this information has been prepared in good faith, no representation or warranty, express or implied, is or will be made and no responsibility or liability is or will be accepted by Pool Re, or by any of its respective directors, officers, employees or agents in relation to the accuracy or completeness of this document and any such liability is expressly disclaimed.


In particular, but without limitation, no representation or warranty is given as to the reasonableness of future suggestions contained in this document.


Pool Re is a company limited by guarantee and registered in England and Wales under company no. 02798901 having its registered office at Hanover House, 14 Hanover Square, London W1S 1HP.


© Pool Re's Terrorism Research and Analysis Centre 2016.

Attack types

-  **Bladed**
Non-firearm attack
-  **Vehicle**
Vehicular-based attack
-  **Firearms**
Terrorist firearms attack

 **PBIED**
Person-borne improvised explosive device (IED)

 **VBIED**
Vehicle-borne improvised explosive device (IED)

 **CBRN**
Chemical, biological, radiological, nuclear

 **Cyber Terrorism**



Overview

The Pool Re Terrorism Research and Analysis Centre (TRAC) is pleased to present its second regular Threat Report.

The first report, published in August 2016, was well received and is available through the Pool Re website [<https://www.poolre.co.uk/Reports/Quarterly-Threat-Report-Aug-2016.pdf>].

In this second edition, the team has focused on key terrorism events and trends between August and December 2016. Pool Re has invested significant resources into its research and peril analysis capability. Combined with the Pool Re Emerging Risk Reports, which provide focused assessments on specific threats, our intention is that this edition will provide a valuable source of information and guidance to the (re)insurance sector as well as our wider stakeholders.

Purpose

The purpose of this report is to inform Pool Re Members and wider stakeholders of the current and future terrorism threat and its implications for the resilience of the end customer, UK businesses, and by extension the national economy.

Methodology

The report's findings are based on a wide range of open source material, in combination with retained subject matter experts. The information contained in this report has been drawn from and corroborated by extensive research collected from academia, think tanks, social media, security, intelligence and risk conferences, as well as subscription-based content. The sum of this provides Pool Re with an opportunity to furnish a unique perspective to the terrorism (re)insurance market.

All assessments and trends are made in relation to the threat posed to the UK and tailored principally to the (re)insurance sector; it is also intended that these assessments are of use to the wider business community and serve to better inform the private sector of the salient terrorism-based risks to business continuity. In order to fully understand the threat to the UK, Pool Re analyses information on the global terrorism landscape that could impact the UK mainland. Pool Re produces Threat Reports (including an Annual Review in the late summer), post incident reports on particular terrorist events and Emerging Risk Reports. The first of these, on Chemical, Biological, Radiological and Nuclear Weapons (CBRN), was issued in July 2016 and is available through the Pool Re website [<https://www.poolre.co.uk/Reports/Emerging-Risk-Report.pdf>].

As well as providing assessments and analysis, Pool Re is also developing sophisticated loss estimation models in collaboration with our external research partners. The current model development is focused on CBRN and the emerging risk of destructive cyber terrorism. Pool Re will publicise the findings of these ongoing projects to industry risk carriers, security specialists within the private sector and government partners.

We hope that you find this edition informative and would welcome any feedback that you might have.

Further information about Pool Re can be found on our website [www.poolre.co.uk] or by following us on LinkedIn.

Ed Butler CBE DSO
Head of Risk Analysis, Pool Re

Target types

 **CP**
Crowded place

 **Symbolic**
Iconic sites such as tourist attractions

 **Property**
Commercial & residential property

 **CNI**
Critical national infrastructure

Impact and Probability of Terrorist Attack Methodology in the United Kingdom

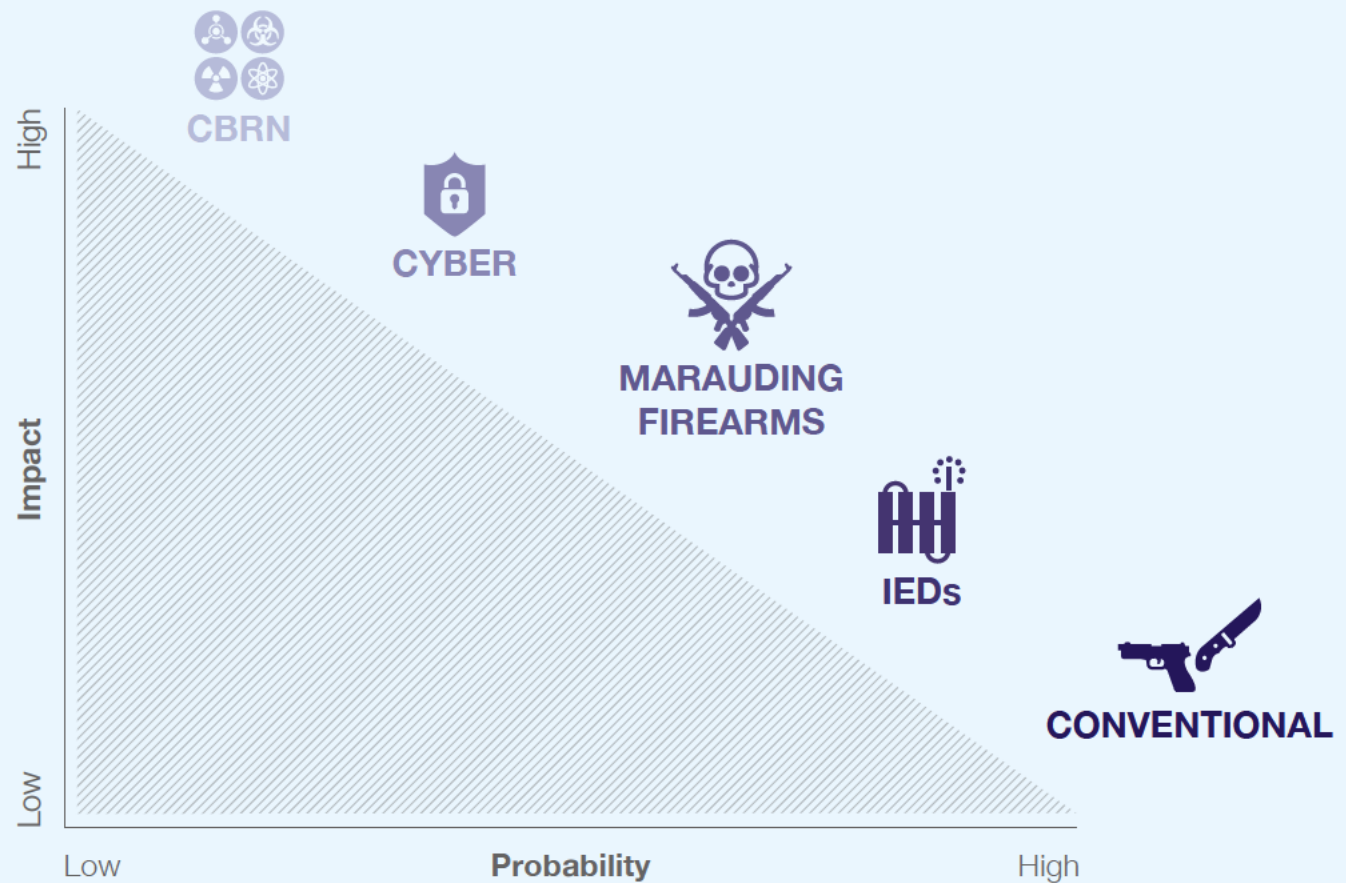


Figure 1. Potential attack methods within the UK

Understanding the impact and probability of a terrorist attack is key to responding to the terrorism risk. Some attack types, while more likely to have a high impact, are less probable due to the methodology, preparation or acquisition of materials required. Other attacks, however, are more probable due to their relatively low complexity.

Figure 1 illustrates the Pool Re assessment of potential attack methods within the UK. This forms the basis of the assessments, scenarios and predictions made within this report.

Executive Summary

The threat level to the United Kingdom remains SEVERE and persistent in its nature. The main driver for this threat continues to be Islamist extremism, in particular Al Qaeda (AQ), Daesh* and their global affiliates.

Alongside the salient risk posed by Islamist extremism, we cannot discount the rise of far-right extremist groups. The reporting period has been dominated by the use of a hijacked lorry to kill and injure visitors to a Christmas Market in Berlin and the killing of 39 people in an Istanbul nightclub on New Year's Eve 2016. These attacks demonstrate the power of ideology to motivate 'lone actors' to commit acts of terrorism. The year 2017 is likely to see similar attacks across Europe. Terrorist suspects continue to be arrested on a regular basis, with many plots disrupted.

Against this backdrop, it is unsurprising that there have been repeated warnings from Western political leaders and security chiefs about the very direct threat posed by Islamist extremist groups preparing to undertake a mass-casualty attack. AQ's continued aspiration to execute some form of 'spectacular' and well-resourced attack continues to pose a threat. The current head of MI6, Alex Younger, warned in his first public statement in December about the significant threat posed by Daesh and AQ to the UK. This underlined similar messages from the UK Secretary of State for Defence and the Director of the FBI.

A number of themes are emerging that are likely to dominate the security landscape in 2017. Despite the probable military defeat of Daesh in Iraq and Syria, the ideology of the group is likely to endure, with the expectation that the group will mutate and evolve into a more dangerous and diffuse entity. Secondly, the so-called Caliphate will become more 'virtual' than physical, with the group increasing its activity online as its physical security is threatened. It is expected that Daesh will move into 'ungoverned spaces' – be they geographical areas, or the Dark Web. It is likely that the focus will be on the most motivated and hard-line followers of Daesh, inspired or directed to cause mass casualties and economic damage. The third, and perhaps biggest, challenge is how security agencies and governments deal with the high number of experienced foreign fighters returning to their home countries.

This 'reverse flow' phenomenon will present a challenge for liberal democracies and how they should manage, de-radicalise and reintegrate those who are sitting outside the criminal justice system. A final theme for 2017 is the possible reassertion of AQ as the dominant global terrorist group, with the capability, experience and technology to match. A worst-case scenario would see the alignment of Daesh and AQ.

Despite the political upheavals in 2016, governments across Europe continue to improve collaboration and information exchange on terrorist activities. The 2015 UK National Security Strategy and Strategic Defence and Security Review (SDSR) both recognised the threats posed by radical extremism and have directed significant resources into counter-terrorism measures. The government's counter-terrorism strategy, CONTEST, is being refreshed. There is an expectation from the business community of improved public/private sector partnerships. A key strand of this is the provision of more appropriate and timely information on the nature of the contemporary threat to businesses, their people and their assets. Closing the terrorism 'information gap' will remain high on the private sector's list of priorities during 2017.

Pool Re and other terrorism reinsurance pools recognise that interaction and collaboration between the state and private sector is fundamental to successful terrorism risk management and the long-term resilience of economies. This was demonstrated at the Australian-hosted Global Terrorism Risk Insurance Conference, in October 2016, where much of the discussion focused on emerging counter-terrorism strategies and how terrorism pools and the global (re)insurance market need to innovate and provide appropriate and affordable terrorism cover to mitigate losses incurred by the changing nature of the terrorist threat.

As terrorist tactics continue to evolve, using a combination of both conventional and unconventional methodologies, so must the insurance sector further adapt to these novel ways and means by providing appropriate products to their insureds. Pool Re continues to work closely with all its strategic partners – government, its Members, academia, its regulators, the reinsurance market and business – focusing on improving intelligence-led risk mitigation and resilience measures.

Terrorism: The United Kingdom and Europe



Key terrorism incidents, United Kingdom and Europe (inc. Turkey)* 2016**

Perpetrators:

- Daesh-directed
- Daesh-inspired
- Kurdish separatists
- Dissident republicans
- Gulen Movement
- Far right

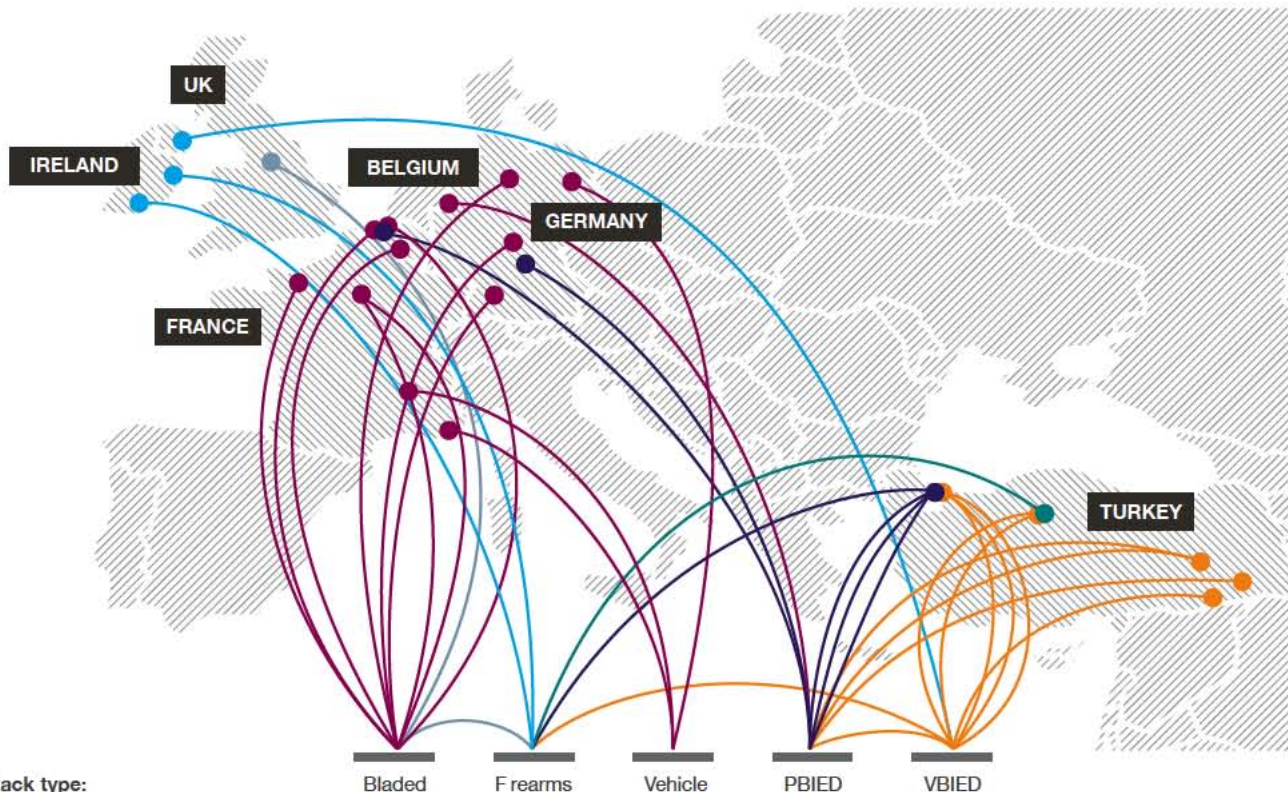


Figure 2. Attack types and perpetrators

Methodology



Bladed

There were ten bladed attacks in Europe in 2016, one in the UK (the murder of Jo Cox MP).



Firearms

There were six incidents involving firearms in the reporting period, one in the UK (the murder of Jo Cox MP). The majority of attacks took place in Ireland and Turkey.



Vehicle

There were three attacks involving vehicles as a weapon in the reporting period, none in the UK. Two of the attacks took place in France, and one in Germany.



PBIED

There were ten attacks involving PBIEDs or suicide bombings in the reporting period, none in the UK. The majority of attacks took place in Turkey.



VBIED

There were seven VBIED attacks in the reporting period, one in the UK. The majority of attacks took place in Turkey.

* It is recognised that Turkey currently sits outside the European Union. It is, however, considered within our analysis because of its geographical position and nexus with the modern terrorism threat landscape.

** Attacks throughout the whole of 2016.

UK Threat Levels:



UK: Threat Summary

Attack type	Bladed	Vehicle	Firearms	PBIED	VBIED	CBRN
Target type	CP	CP	CP	CP	CP	CP
	Symbolic	Symbolic	Symbolic	Symbolic	Symbolic	Symbolic
	Property	Property	Property	Property	Property	Property
	CNI	CNI	CNI	CNI	CNI	CNI

Threat level The Joint Terrorism Analysis Centre (JTAC) assesses the threat from international terrorism to the United Kingdom (UK) remains SEVERE, meaning an attack is highly likely. MI5 assesses the threat from Northern Ireland-related terrorism to the UK mainland remains SUBSTANTIAL, meaning an attack is a strong possibility.¹

Key actors **Islamist Extremists**
 Islamist extremists remain the principal threat to the UK. Daesh and AQ associates and affiliates represent the key threat actors, with both the intent and the capability to inspire and direct attacks at varying levels of complexity against UK targets. Probable targets remain crowded places, national infrastructure, such as aviation and other means of transport, as well as institutional targets, including the military and police. It is now commonplace for both aspiring attackers and perpetrators to have been in direct contact with extremists overseas, via social media or instant messaging services, or inspired by extremist propaganda online.

Dissident Republican Groups
 The Continuity IRA (CIRA), the New IRA and the Óglaigh na hÉireann (ONH) all remain active and have retained significant quantities of weapons and explosives. The groups operate mainly on the criminal fringes of Northern Ireland's society, controlling cross-border smuggling routes and low-level crime. The threat level of Dissident Republican (DR) groups to the UK mainland was raised to SUBSTANTIAL by MI5 in May 2016. This is an indication of increased intent from DRs to mount an attack on the mainland, with targets more likely to be high profile individuals, the military and the police.

The UK specifically has seen a rise in the capabilities of Al Muhajiroun (ALM). 23% of Islamist terrorists convicted in the UK have a "direct and provable" link to ALM and the organisation has recently encouraged British nationals to travel to Syria in support of Daesh.² A Daesh video released in December 2016 depicted Mohammed Reza Haque, a close follower of Anjem Choudary and a British national, executing a prisoner. In 2016, two senior ALM members, Choudary and Mohammed Rahman, were convicted of terrorism offences and imprisoned for five and a half years.* ALM offers an enduring appeal to young Muslims in the UK, and further arrests should be expected as MI5 and the police continue to disrupt their extremist influences.

Far-Right Extremism in the UK
 The UK has seen an increase in far-right extremism in 2016. In June, Thomas Mair, an individual with ties to British nationalist, pro-apartheid and neo-Nazi groups, murdered Jo Cox MP. Mair had purchased manuals from white supremacist groups in America, indicating an international dimension to far-right extremism in the UK. In December, National Action became the first far-right group to be proscribed under the Terrorism Act 2000. Far-right extremism is an ongoing threat to UK community cohesion and national security.

Arrests and enforcement The Home Office assesses around 850 people have travelled from the UK to engage in the Syrian conflict and about half have returned.³ Managing this extremist travel either out of or into the UK is likely to present extensive casework for the police and MI5. As the police and government have been taking steps to restrict attempts to travel, combined with a likely reduction in appeal to travel to the so-called Caliphate as coalition forces maintain military action against it, an increase in UK domestic attack plots should be expected. Senior intelligence officials have been explicit about the terrorist threat to the UK, with at least 13 plots disrupted since June 2013.⁴

Assessment Daesh and AQ will continue to direct and inspire attacks across Europe. An attack in the UK by Islamist extremists remains 'highly likely'.

Most likely scenario

An attack by one or two Daesh or AQ-inspired individuals using knives and a vehicle against a high-profile target such as a crowded place, or police/military personnel.

Most dangerous scenario

Firearms combined with PBIEDs against a crowded place or transport hub, directed by Daesh or AQ. Such an event would likely result in mass casualties akin to the Paris and Brussels attacks.

Emerging scenario – conventional

A UK mass-casualty attack against a crowded place involving automatic firearms acquired as a result of an increased overlap between terrorist and organised crime groups.































Emerging scenario – unconventional attack

As more Daesh fighters return to the UK from Syria and Iraq, they bring with them knowledge and expertise in chemical, and potentially biological and radiological, weapon development for a UK-based attack. In addition to this, there is the threat of such a weapon being smuggled into the country from Iraq/Syria.

Probability Assessment: 

- More Likely
- Possible
- Less Likely

Europe: Threat Summary

Attack type	Bladed 	Vehicle 	Firearms 	PBIED 	VBIED 	CBRN 
Target type	 CP	 CP	 CP	 CP	 CP	 CP
	 Symbolic	 Symbolic	 Symbolic	 Symbolic	 Symbolic	 Symbolic
	 Property	 Property	 Property	 Property	 Property	 Property
	 CNI	 CNI	 CNI	 CNI	 CNI	 CNI

Threat level Europe is facing a persistently high terrorist threat, demonstrated over recent years by several mass casualty attacks. The start of 2016 saw the highest number of terrorism deaths in Western Europe since 2004 (when the Madrid train bombings left 191 people dead)⁵ and the year drew to an end with the attack upon the Christmas market in Berlin. This illustrates how in countries such as Germany, France and Belgium terrorist attacks may happen imminently. For the most part, terrorist attacks across Western Europe are highly likely. Daesh or AQ and their associates and affiliates remain the most likely actors, with the involvement of many Western European countries in airstrikes and other military action in Iraq and Syria remaining the most likely driver for extremists to attack.

Key actors

Islamist Extremists
Daesh and AQ associates and affiliates are the main threat actors in Europe. Daesh has a greater presence among would-be inspired extremists owing to its ability to exploit social media and instant messaging services. Both groups have the capability to direct and support attacks across continental Europe. This support was evidenced by recent attacks in Berlin and Istanbul.

Far-Right Extremism
Far-right extremist groups and individuals continue to contribute to the European terrorist threat. Since 2000, one in three lone actor terrorists in Europe have been motivated by extreme right-wing beliefs,⁶ and the current refugee crisis could lead to an increase in far-right extremism.⁷

Arrests and enforcement France is facing a sustained threat, leading to frequent counter-terrorism activity, disruptions and arrests. Those arrested have often been known to the police and security agencies, with links to other European countries including the UK.⁸ The methodology of attacks, or intended attacks, in mainland Europe has remained likely to involve the use of explosives and automatic weapons. In some plots, such as in Germany in October, similarities in the types of explosives intended for use have been identified.⁹ This clearly illustrates the enduring threat.

As this major disruptive activity continues, Daesh extremist propaganda is now encouraging more low complexity and low cost attacks in countries that have recently experienced 'the spectacular', in a likely attempt to ensure more attack plots are successful¹⁰ and can occur with more regularity. Attacks in Europe are likely to remain focused on key individuals and crowded places, although it is possible more attacks using bladed articles and vehicles could be expected over marauding firearms attacks.

Total arrest figures for 2016 have not yet been released by Europol, however it is likely they will illustrate counter-terrorism activity in the UK, France and Spain remains high.¹¹ The majority of those arrested are likely to be male and aged under 35 years.

Turkey Turkey faces a terrorist threat from international groups such as Daesh and domestically from groups such as the Kurdistan Workers' Party (PKK) and the Revolutionary People's Liberation Party (DHKP-C). Attacks happen with great regularity, with little or no warning, against official targets such as police and military assets along with tourist locations and national infrastructure. When an attack happens, attribution is often problematic without official claims of responsibility. When claims are made, they frequently indicate the motivation of the group responsible, which is often linked to Turkey's domestic or foreign policies, emphasising the country's strategic importance to both countries with shared interests and terrorist organisations. For example, the assassination of Russian Ambassador Karlov in Ankara in December 2016 was perpetrated by a Turkish domestic extremist in response to Russia's military action in Syria. Turkey has been a key gateway for extremist travel to and from the UK for many years and supports the UK counter-terrorism (CT) effort to some extent, benefiting from the presence of UK CT police officers in-country, assisting with capacity building and investigations. Turkey currently supports and participates in airstrikes against terrorist groups, which leads them to reciprocate with attacks such as the New Year's Day 2017 nightclub attack in Istanbul.

Assessment Daesh and AQ will continue to direct and inspire attacks across Europe. Attacks are highly likely and may happen with little or no warning. Methodology is likely to be a combination of complex, well-resourced attacks together with low sophistication ones, targeting crowded places and high-profile individuals. The attackers are likely to have direct links to senior leaders overseas, or have significant association with individuals and extremists' ideology via social media and the Internet.

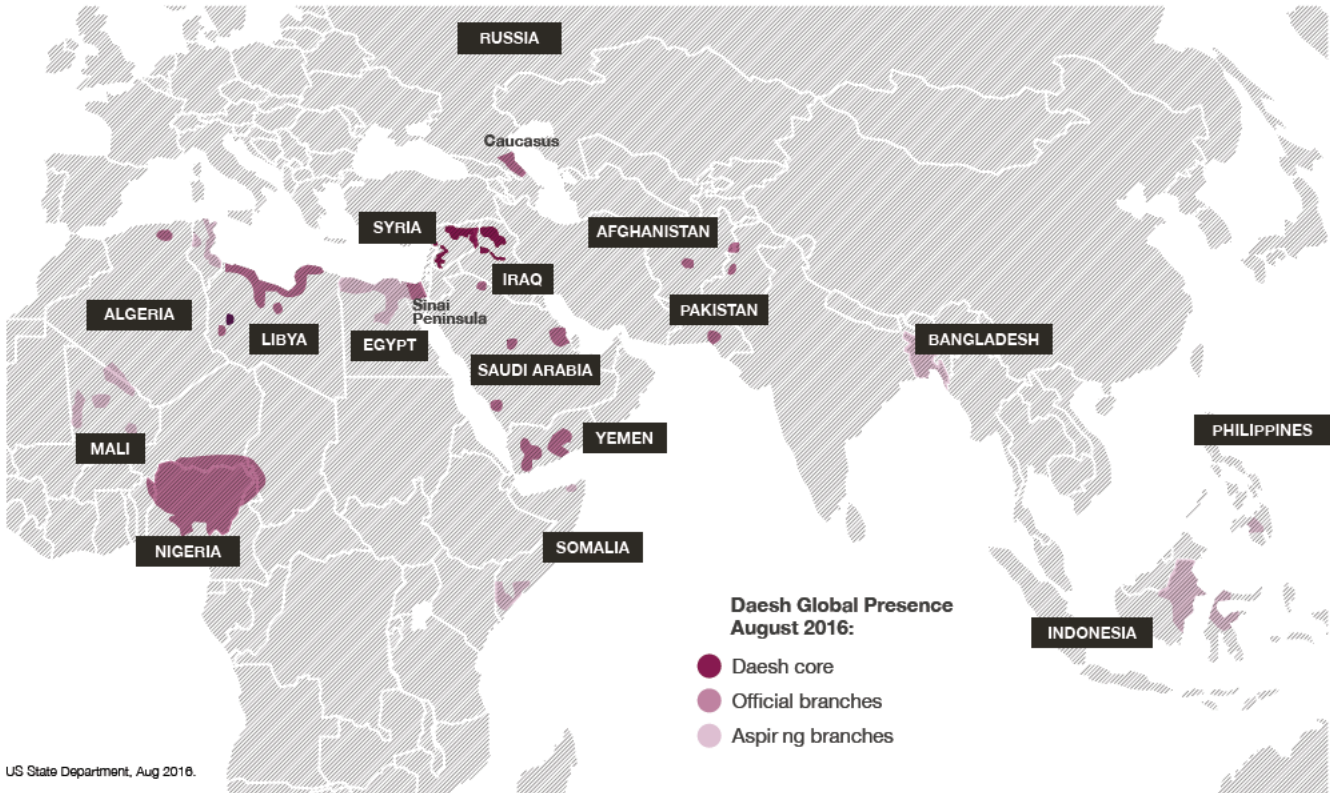
Most likely scenario
Attacks involving firearms and vehicles continue with frequency across Europe, targeting crowded places.

Most dangerous scenario
A combined PBIED and firearms attack resulting in mass casualties occurring simultaneously across multiple target sites.

Emerging scenario – unconventional attack
As stated in the UK threat summary, as more Daesh fighters return to Europe from Syria and Iraq they bring with them knowledge and expertise in chemical/biological weapon development for an attack, or could smuggle a viable weapon into Europe from Syria and Iraq for use in an attack.

Islamist Extremism Global Presence, 2016

Threat posed to the UK homeland by Islamist extremist groups overseas


























US State Department, Aug 2016.

Threat Actor	Area of Operations	Capability	Recent Activity and Attacks Relevant to Western Targets	Contribution to the UK Threat
Daesh core	Iraq, Syria, Libya	Inspire and direct attacks against Western targets. Territorial control in Iraq, Syria and Libya.	Brussels bombings, March 2016; Orlando, June 2016; Nice attacks, July 2016; bladed attack, Normandy, July 2016; Ansbach bombing, Germany, July 2016; bladed & vehicle attack, Ohio USA, November 2016; Berlin, December 2016; Istanbul, December 2016.	More Likely Trend ▲ August 2016 ▲ December 2016
Daesh affiliate ISIL-Sinai Province (formerly Ansar Bayt al-Maqdis)		Focus on Egyptian military targets.	No specific targeting of Westerners in the attacks in the reporting period. Last attack: downing of the Russian passenger jet departing Sharm el-Sheikh, October 2015.	Possible Trend ▶ August 2016 ▶ December 2016


Probability Assessment: 

- More Likely
- Possible
- Less Likely

Threat Actor	Area of Operations	Capability	Recent Activity and Attacks Relevant to Western Targets	Contribution to the UK Threat
Daesh affiliate Boko Haram		Conduct and direct attacks in West Africa.	Ongoing operations against regional forces (Nigeria, Niger, Cameroon & Chad). No specific targeting of Westerners in the attacks in the reporting period, although attacks can be indiscriminate. Ongoing kidnapping of Chibok schoolgirls (April 2014).	 Less Likely Trend  August 2016  December 2016
AQ branch Al Qaeda in the Arabian Peninsula (AQAP)		Territorial control in Yemen. Access to heavy weaponry and sophisticated bomb-making material. Ongoing operations in Yemen's civil conflict.	No specific targeting of Westerners in the attacks in the reporting period although attacks can be indiscriminate. Last Western attack: Charlie Hebdo, January 2015.	 More Likely Trend  August 2016  December 2016
AQ branch Al Qaeda in the Islamic Maghreb (AQIM)		Conduct and direct attacks in West and North Africa with the aim of overthrowing the Algerian government. Focused on Western targets within North and West Africa. Territorial safe haven in Trans Sahel region.	Splendid Hotel, Burkina Faso, January 2016; attack on beach resort in Grand-Bassam, March 2016.	 More Likely Trend  August 2016  December 2016
AQ branch Al Qaeda in the Indian Subcontinent (AQIS)		Regularly conducts targeted assassinations in Bangladesh. Operationally focused on Pakistani and Afghan military.	No specific targeting of Westerners in the attacks in the reporting period. Evidence suggests AQIS's main focus is on the Indian Subcontinent and does not present a threat to UK homeland.	 Less Likely Trend  August 2016  December 2016
AQ affiliate Al-Shabaab		Conduct and direct attacks in the Horn of Africa and Arabian Peninsula.	Ongoing operations in Somalia's civil conflict. Threats continue against Mogadishu International Airport which houses Western interests.	 Less Likely Trend  August 2016  December 2016
Former AQ branch Jabhat Fateh al-Sham (formerly al-Nusra Front)		Conduct and direct attacks on the UK and Europe.	Ongoing operations in Syria against the Assad regime. No specific targeting of Westerners in the attacks in the reporting period.	 Possible Trend N/A August 2016  December 2016

Threat Trajectory: The United Kingdom and Europe



Probability Assessment: 

- More Likely
- Possible
- Less Likely

Changing terrorist threat

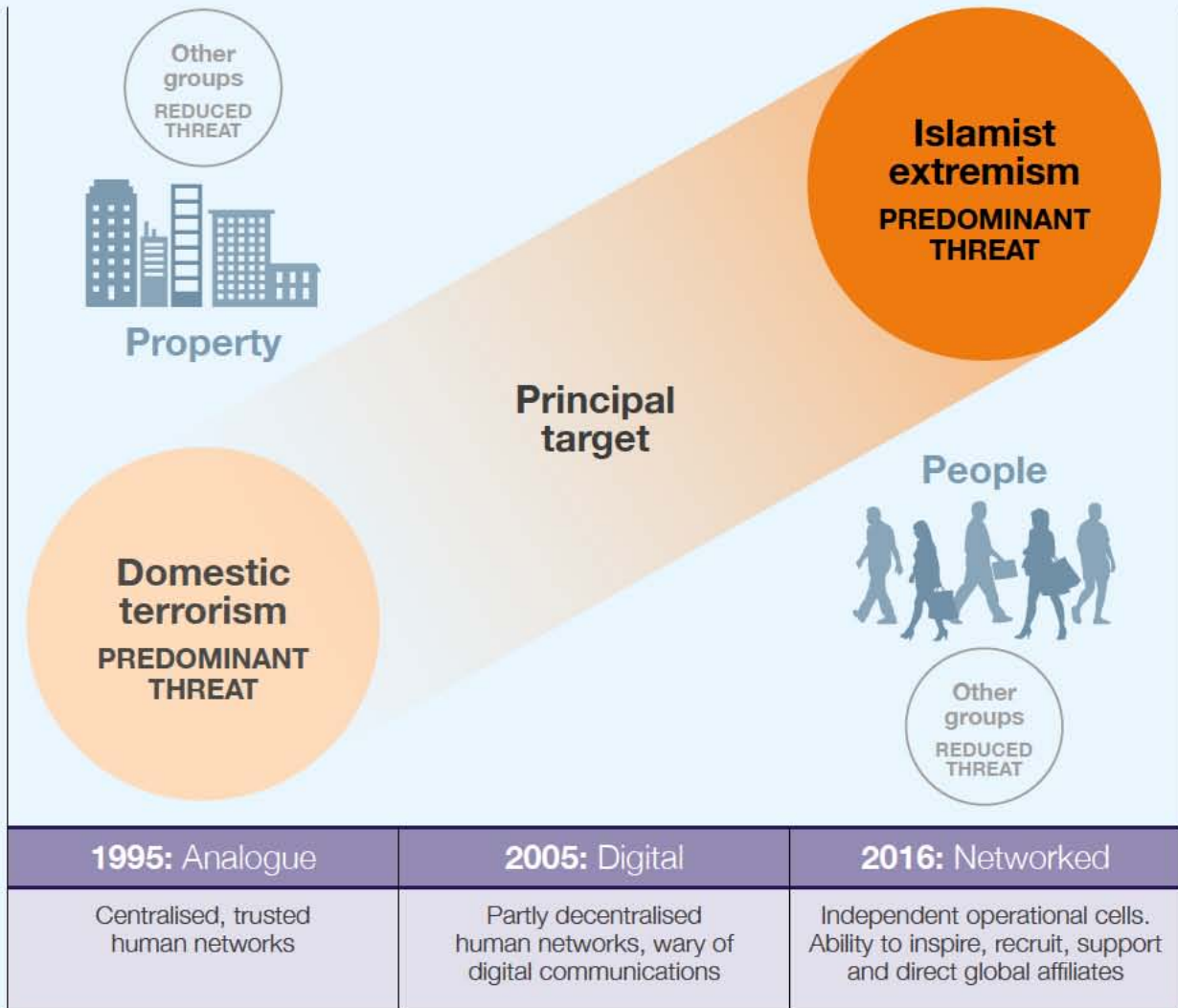


Figure 3. Changing terrorist threat

Domestic terrorism

 	<p>Method of attack:</p> <p>Intent:</p> <p>Economic disruption (discriminate targeting)</p> <p>Risk transfer needs:</p> <p>Property damage and business interruption</p>
--	---

Islamist extremism

      	<p>Method of attack:</p> <p>Intent:</p> <p>Mass casualties, economic disruption (indiscriminate targeting)</p> <p>Risk transfer needs:</p> <p>Property damage, business interruption, non-property damage business interruption, cyber, impacts on people ad damage to brand and reputation</p>
---	--

When, not if?

The international terrorist threat to the UK and its interests is persistent. The UK threat level remains at SEVERE (an attack is highly likely) despite no major attacks within the reporting period.

This level of threat is now becoming accepted as normal. Vigilance throughout the Critical National Infrastructure (CNI), particularly major economic sites, should be encouraged to prevent complacency and threat fatigue. The threat from Dissident Republicanism to Great Britain remains at SUBSTANTIAL, although recent comments in October by Neil Basu, Senior National Coordinator for Counter-Terrorism Policing at the Metropolitan Police Service, suggested this remains persistent.*

The UK's SEVERE threat level is underpinned by the increasing number of thwarted attacks (13 since June 2013),¹² and a 57% increase in terror arrests since 2013. Reports indicate that MI5 is dealing with 550 live cases at any one time,¹³ with a suggested figure of approximately 400 Daesh fighters who have now returned to the UK (of whom 70 are reported to be high risk).¹⁴

Europe has faced a sustained threat from Islamist extremists. The lorry attack on the crowded Christmas market in Berlin in December 2016 is a reminder that attacks in Europe are likely to continue with symbolic events being targeted. The assassination of Ambassador Karlov also illustrates the threat to high-profile official figures who may be targeted because of their countries' foreign policy, particularly intervention in Iraq and Syria.

European security agencies have thwarted several other attacks and have arrested over 800 terrorist suspects (see Figure 4). The arrests made by police and security agencies across Europe now appear to have achieved more than picking the 'low hanging fruit' and have resulted in significant disruptions to terrorist networks. This may be due to greater intelligence sharing, operational collaboration and resilience throughout Europe, enabled by the maturing European Counter Terrorism Centre. However, the Berlin lorry attack highlighted the intelligence shortcomings that still exist among some of our European partners.

“We can put a stake through the heart of Islamic State as an army. We can put a stake through the heart of its leaders. You can take away its territory. But you can't put a stake through the heart of the ideas, of the ideology.”

General David Petraeus¹⁵

The threat to the UK homeland from Daesh endures. As its territories in Iraq and Syria are reduced, and it suffers other military setbacks** in the region, it is likely that these factors will cause extremists to consider returning to their home countries, creating a 'terrorist diaspora'.*** There continues to be an influx of migrants from North Africa and the Middle East into Europe, and evidence suggests that terrorists are using fraudulently obtained travel documents to exploit these migration routes.**** The 'reverse flow' of fighters back to the UK, with potential hostile intent and increased experience and capabilities, will escalate the threat, especially if coupled with home-grown supporters. Monitoring and interdicting the increasing numbers of returnees will continue to be a major challenge for MI5 and the police.

It should also be noted that the probability of unconventional attack methodologies being employed across Europe is increasing, as recently highlighted by the Minister of State for Security Ben Wallace MP.¹⁶ The CBRN capabilities of overseas extremists are growing and relevant knowledge is being shared internationally; reporting also suggests that individuals with technical expertise relating to CBRN systems are returning to their homelands. Daesh has also started using the Internet as a way of sharing CBRN knowledge. The use of drones, either in reconnaissance or in IED attacks, has continued overseas, and their increased sophistication and availability in the UK require careful thought.

It is unknown how the UK's exit from the European Union (EU) and the new Trump Administration will affect security regarding international terrorism. However, it is assessed that the implications of a change in approach to security and defence under a Trump Administration could have greater consequences than Brexit.

* Neil Basu, the Senior National Coordinator for Counter-Terrorism Policing at the MPS, commented: "The continuing threat from Northern-Ireland-related terrorism and al-Qaida also remains present, with supporters of both seeking to act", (*The Guardian*, 28/10/16).

** Their recent expulsion from Sirte in Libya is a prime example.

*** James Comey, Director of the FBI: "They will not all die on the battlefield in Syria and Iraq. Through the fingers of the crush are going to come hundreds of very dangerous people. There will be a terrorist diaspora sometime in the next two to five years like we've never seen before." FBI director: ISIS "loss will create a terrorist diaspora" like we've never seen before. (*Business Insider UK*, 27/09/16).

**** It is understood that the majority of the terrorists involved in the November 2015 Paris attack used migration routes.

The UK has committed to remaining in Europol for at least two more years,¹⁷ but will lose its lead role within the organisation and will not head up any of the other security organisations. Despite not being at the decision-making table, it will be essential that the UK remains active in generating influential policy approaches, building on the long-term relationships and experience that have been built up over many years. This is indicated by the Home Secretary's recent comments on her commitment to Europol after Brexit.¹⁸

Daesh is operating across Europe and the reduction of the so-called Caliphate will free up human capacity,* financial, and technical resources to attack Western targets. It is expected that Daesh will continue to employ low sophistication attack methods, as witnessed during the Nice and Berlin attacks. The attacks also demonstrate the capabilities of Daesh to exploit the Internet, including the Dark Web, and instant messaging services to share their ideology, attack planning and post-incident propaganda. This is likely to cause MI5 and the police to face an increase in UK attack planning investigations.

Attack methodology in the UK remains likely to involve one or two inspired or affiliated individuals mounting a low complexity attack with bladed weapons or vehicles against high profile targets, such as diplomatic and police personnel, or crowded places (including transport networks). The risk of a 'spectacular' attack remains possible, especially considering the desire of AQ senior leadership and their proven abilities. AQ leader Ayman Al-Zawahiri has been explicit in his instruction for attacks in the UK and in October 2016 Sir Michael Fallon, Secretary of State for Defence, stated that the group poses a "very direct threat" [to the UK and Europe]... "Al Qaeda is still alive and kicking in Afghanistan, in Syria, in Yemen and elsewhere".¹⁹ Nigel Inkster, former Director of Operations MI6, commented on the 6th October 2016 that "Al Qaeda have been rebuilding quietly and [...] waiting to see the Islamic State come under pressure it has come under."²⁰

This clearly illustrates why a terrorist attack in the UK remains highly likely.

Terrorist/Criminal Nexus

Throughout Europe and the UK there is a strengthening nexus between criminality and terrorism with the buying and exchange of weapons, travel documents, money laundering, specialist equipment and ideas. Although the links between crime and terror are nothing new, the emergence of Daesh – and the ongoing mobilisation of European extremists – has meant the nexus has become "more pronounced, more visible, and more relevant to the ways in which jihadist groups operate".²¹ Of the 816 individuals reported to Europol for terrorism-related offences, 66% had previously been reported for involvement in serious or organised crime.²² The Internet further facilitates this symbiotic relationship with the existence of chat rooms and forums where knowledge and ideas are exchanged.

In the UK, as increasing numbers of terrorists enter the criminal justice system, they enter the prison estate, which offers an environment for extremism to flourish and networks to be made. A number of released criminals have been radicalised while serving prison sentences, and attacks within the UK have been made by terrorists with substantial criminal connections. This terrorism and crime nexus represents an increasing contribution to the domestic threat. The acquisition of automatic weapons by terrorists is currently difficult on the streets of the UK. However, the networks being established in prisons have the potential to change this, with increased collaboration between terrorists and organised crime groups. Subsequently, this is likely to change attack methodology by Islamist extremists in the UK.

Terrorism/Criminal Nexus in Europe

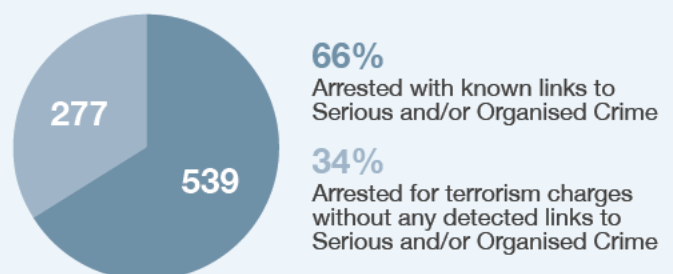


Figure 4. Pie chart representing the links between arrests for terrorism and serious or organised crime

* The Director of Europol, Rob Wainwright, suggested at the National Security Summit (27/10/16) that 5,000 European citizens have gone out to Syria and Iraq, of whom 50% have been killed or returned home.

The Resilience of Al Qaeda

While international attention has been focused on Daesh over the last four years, Al Qaeda has continued to grow in its shadow. Will 2017 see the continued evolution and expansion of Al Qaeda?

Extinct?

Five years ago AQ was viewed, by some commentators, to be on the verge of strategic collapse.²³ Its founder and leader, Osama bin Laden (OBL) and lead radicaliser, Anwar al-Awlaki, were dead, along with the majority of its commanders. Despite a period of UK-based attack plans with AQ connections, including the attack on Glasgow Airport in 2007, plans to attack London over Christmas 2010 (Operation NORBURY) and a Birmingham-based bomb plot in 2011 (Operation PITSFORD), the organisation appeared inactive and irrelevant to the Arab Spring transformation across the Middle East and North Africa. Attempts to establish democracy had replaced the appetite for violence and repression.

Arguably, however, it was also civil unrest that contributed to the growth of part of AQ. The Houthi insurgency in Yemen allowed AQ in the Arabian Peninsula (AQAP) to flourish. The same effect was seen in the Trans-Sahel region with AQ in the Islamist Maghreb (AQIM), particularly during the conflict in northern Mali. AQAP's contribution to the international threat landscape subsequently changed counter-terrorism globally and illustrated the enduring threat of AQ.

Enduring

When the UK threat level was raised to SEVERE in August 2014, it is highly likely a key driver to this was AQAP's capability to attack civil aviation using non-metal content (NMC) bombs. Just prior to the UK threat level change, new travel restrictions were implemented for uncharged computer tablets and electronic devices on United States-bound planes, with the threat from AQAP cited in open source reporting.²⁴ While Western intelligence and security agencies were grappling with the emergence of Daesh (with its origins in AQ in Iraq), the main AQ threat was not extinct. It was this combination of AQ and Daesh capabilities that meant the probability of a terrorist attack by Islamist extremists in the UK went from 'a strong possibility' to being 'highly likely'.²⁵ AQ's threat to the UK can be assessed to be enduring.

"Al Qaeda's obituary has been written countless times over the decade. Each iteration has proved to be ephemeral, as the [movement] has continually shown itself to have a deeper bench than we imagine."

Bruce Hoffman²⁶

Military action subsequently directed against AQAP and other AQ-associated groups after mid-2014, resulting in the deaths of high-value targets such as David Drugeon²⁷ and Nasir al-Wuhayshi,²⁸ is likely evidence of the weight they contributed to the threat against the West. AQ was quick, however, to illustrate its resilience. December 2014 saw AQAP post *Inspire 13* online, with advice on defeating airport security measures and instructions on how to make a NMC bomb.²⁹ This knowledge, previously held by a few individuals within the organisations, was subsequently shared openly across the Internet.

Evolving

Since 2014, despite becoming decentralised, AQ has continued to operate in North Africa and the Trans-Sahel (AQIM), Yemen and the wider Arabian Peninsula (AQAP), Afghanistan and Pakistan. Late 2014 also saw the creation of AQ in the Indian Subcontinent (AQIS). While the military action against the organisation across Pakistan, Afghanistan and Yemen has been significant, it has not impeded its current senior leadership, including global Emir Ayman al-Zawahiri. Al-Zawahiri, in a series of speeches in 2015, redirected the organisation's strategic direction back to the West (notably France, the UK and the USA) after a period of preoccupation with the Indian Subcontinent.³⁰ AQ also staked a claim for the 2015 Charlie Hebdo attacks in France,³¹ serving a stark reminder of its capabilities. Also at this time al-Zawahiri pledged allegiance to the Taliban and Mullar Mansour,³² a likely attempt to regain ground in Afghanistan to help its regeneration and exploit the many Taliban successes against the remaining Western presence and influence. This allegiance is a clear indication of al-Zawahiri's attempt to regain dominance of the global jihadist movement – an effort that was subsequently bolstered by the support of Hamza bin Laden, son of Osama.

Expanding

Hamza bin Laden has played an increasing role in AQ's communications. His media releases are frequently in pace with al-Zawahiri's, and both are losing their traditional religious rhetoric in a move likely to appeal to a younger generation of extremists. AQ continues to disseminate its narrative across the Internet, learning from Daesh's publishing capabilities. While al-Zawahiri maintains an Emir's strategic perspective in his messages, Hamza bin Laden's are geographically and conceptually wide ranging. This is a likely indication of his desire to be globally recognised in preparation for a future leadership role, following on from his late father.

Hamza bin Laden's global perspective is taking place at a time when international AQ affiliates remain active. Jabhat Fateh al-Sham (JFS, previously known as Al Nusra Front) is probably the largest of the AQ groups, and, while focused on attacks in Syria, the group retains a desire to attack the West directly. Al Shabaab and AQIM remain very active in Somalia and North/West Africa. While these groups may not pose a direct threat to the UK homeland, they do threaten British interests in-country, particularly tourists, business travellers and foreign direct investment.

Under OBL, AQ had a preoccupation with the spectacular attack, illustrated across the world with successful attacks against the World Trade Centre in 1993, American embassies in Kenya and Tanzania, the USS Cole, the Madrid train bombings, 7/7 and 9/11. AQ now, however, appears to be adjusting this strategy. At the same time as redirecting attention to the West, within its *Inspire* magazine AQAP publicised instructions on attack methodologies of lower complexity.³³ Potential targets remained crowded places with associated mass casualties. However, another spectacular attack at the design of an AQ group is plausible, with the commercial aviation sector (airports and aircraft) remaining a desirable target. AQ has also illustrated UK-based CBRN aspirations with the Wood Green ricin attack plan in 2002,³⁴ the disrupted plot leading to the murder of Special Branch Detective Stephen Oake.

If 9/11 is considered a peak in AQ activity, the world experienced an escalation of violence thereafter. That threat was met by direct military action from the Western world, resulting in AQ capabilities being reduced for some time. That pattern is currently applicable to Daesh, and, while it remains the focus of military and intelligence agency effort, this overshadowing affords AQ the opportunity to expand. Furthermore, it is possible AQ stands to gain the support of Islamist extremists disillusioned by the brutal tactics of Daesh. In summary, AQ has demonstrated its ability to endure and evolve and is continuing to expand.

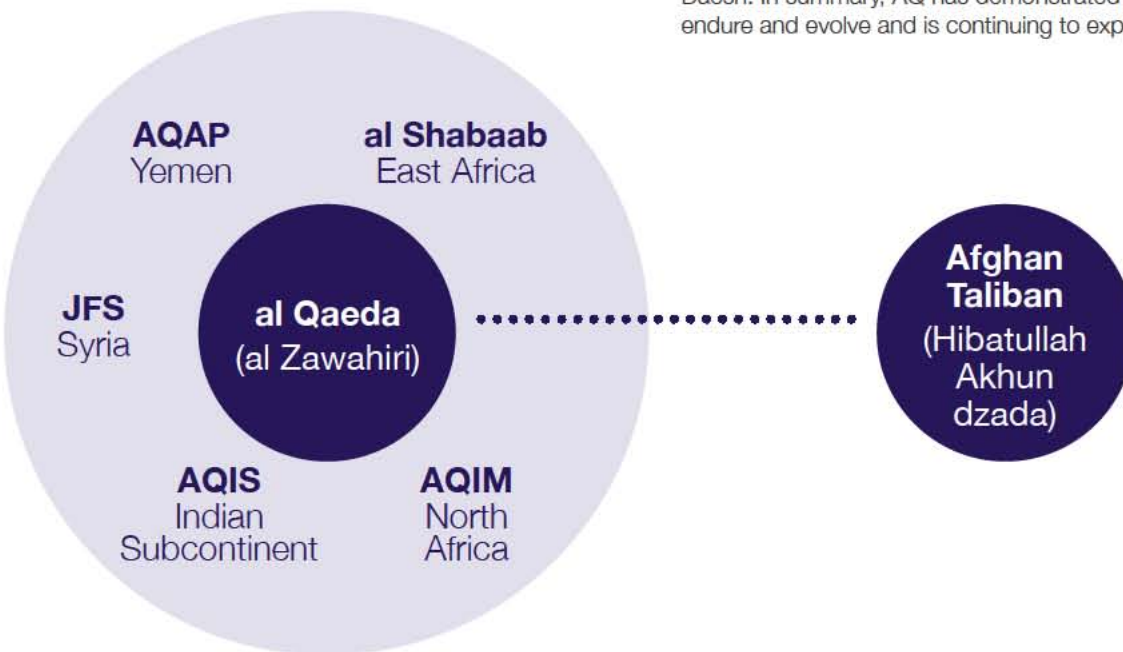


Figure 5. AQ network

CBRN



How ‘clean’ is ‘clean enough’?

The Threat of Chemical, Biological, Radiological & Nuclear Terrorism in the UK

A terrorist attack involving CBRN material is a high-impact, low-probability event. The Cabinet Office National Risk Register of Civil Emergencies recognises the potential for such an attack, from which an operational framework and contingency plans have been developed for such an event.³⁵

The current international landscape could offer potential opportunities for the acquisition, development and proliferation of CBRN material. Reporting suggests basic chemical weapons (CW) (chlorine and sulphur mustard) have been used repeatedly in Iraq.³⁶ Use of CW in Syria is also well documented, with use attributed to both Daesh and government forces, and documented aspirations of Jabhat Fateh al-Sham to obtain them.³⁷ In September and October 2016, the United Nations Joint Investigative Mission identified that military units of the Syrian Air Force had deployed improvised chlorine bombs. There is mounting international pressure to suspend Syria from the Chemical Weapons Convention, as increasing evidence suggests the regime did not fully declare the quantities of their CWs. The muted international response had done little to reduce the threat of their use within an unstable region.

In October, international attention was directed to Russia when it suspended its agreement with the USA to reduce its surplus weapons-grade plutonium. Under the agreement, Russia was obligated to dispose of 34 tonnes of plutonium from warheads dismantled in previous bilateral arms control treaties. Russia’s act presents concerns for the proper security of its plutonium. If terrorists, either through theft or through illegal purchase, acquired such material, it has the potential to be a major threat to the West.

While the lure of CBRN weapons is attractive to many groups, producing a CBRN weapon with mass casualty impact is a technological challenge for non-state actors. There are significant barriers to acquisition, production, weaponisation and delivery. At present, Islamist extremists represent the most likely threat actor to employ a CBRN weapon. However, current assessments conclude AQ’s and particularly Daesh’s aspirations exceed their actual capability.

Impact and probability: CBRN

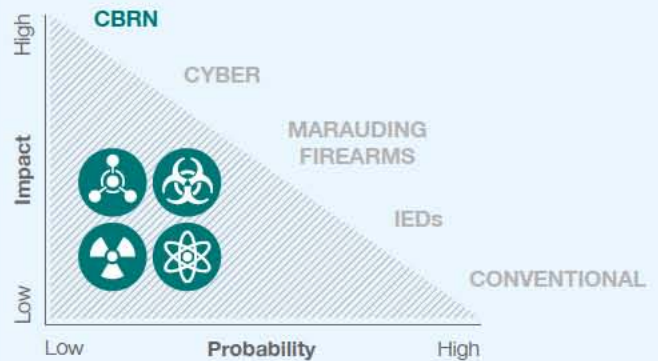


Figure 6.

Nonetheless, Daesh's intent and evolving capacity present a significant cause for concern; over the past two years a growing body of evidence suggests that the group has allocated significant resources to the development of this capability. In January 2016, Sky News reported on a 'weapons lab' based in Raqqa, Syria,³⁸ and, while the initial media reports may have sensationalised the issue, it does illustrate Daesh's dedication to weapons research and development. While it is unlikely some of those initial weapon development claims were credible, subsequent reports amidst the progression of Western military action against the group document their continued research, specifically regarding use of chemical weapons.



“They have no moral objection to using chemical weapons against populations, and if they could, they would in this country.”

Ben Wallace MP,
Minister of State for Security³⁹



Chemical

There is growing evidence of Daesh's CW capability within Iraq and Syria. In February 2016, John Brennan, Director of Central Intelligence, stated Daesh was able to make small quantities of chlorine and mustard agents.⁴⁰ This was corroborated by similar reports, in May 2016, by the Head of the Organisation for the Prohibition of Chemical Weapons.⁴¹ More recent reporting suggests the group has conducted experiments on prisoners to refine their devices,⁴² and key individuals from Saddam Hussein's CW programme have been associated with them. The killing of Abu Malik, a chemical engineer in Saddam Hussein's Muthana chemical weapon programme, and subsequent member of Daesh, in a coalition air strike in 2015 supports this and demonstrates an international recognition of the threat.⁴³

An attraction of CW to terrorists is the insidious nature of the attack and the fear it can spread beyond the immediate effect. The use of the Internet and social media to proliferate knowledge has long been a concern; developing practical expertise within Iraq and Syria is even more concerning. There are a number of limiting factors in the use of CW that make them of limited effect outside the wide-scale use seen by state actors or in war. However even limited and ineffective use could cause significant disruption to an unprepared country.

While a CBRN attack is unlikely in comparison to other attack methods, the growing number of returnees from Iraq and Syria, with their possible knowledge and experience of CW attacks, has the potential to increase the likelihood of such an attack in the UK. This knowledge, combined with the availability of Toxic Industrial Chemicals (TIC) in the country, represents a significant risk. The physical and psychological impact of such a device is likely to mirror that of a CW ordnance.

A potentially dangerous scenario would be the smuggling of new or legacy CW from the so-called Caliphate into Europe. There are sizeable challenges to this, including increasing the risk of discovery and whether the risk is acceptable compared to less challenging attacks. An associated risk might be returnees using their knowledge to try to produce systems in the UK. This is concerning, but also carries an increased risk of detection for the terrorist in a country that is experienced and prepared.



Biological

The use of biological weapons (BW) by terrorists presents a significant challenge. The cultivation of some BWs, such as anthrax, can require high levels of expertise and remains extremely hazardous even to well-equipped specialists working in a secure laboratory. A terrorist cell trying to produce a hazardous agent could well suffer injuries or death. Stealing a pathogen or toxin from a secure laboratory would yield small quantities and still require processing to produce sufficient amounts to cause significant casualties.⁴⁴ Without appropriate equipment and expertise it is more difficult for the terrorist to succeed.

Even if BW are successfully acquired or manufactured, their delivery is difficult. The infection of a person by a BW would not be easy and may lead to an agent being used that fails to infect or poison significant numbers. The onset of symptoms from a BW may be delayed by days and it may take weeks or months before the attack becomes apparent. This could be undesirable for terrorists seeking quick propaganda wins.

Terrorists have maintained aspirations for a BW attack. In January 2014 a Daesh laptop was recovered in Idlib province, Syria, with files that included instructions on how to make BW from animals infected with bubonic plague, in addition to large amounts of data on bomb making.⁴⁵ However, the data show some fundamental lack of knowledge on the varieties of *Yersinia Pestis* (plague) and animal to human transmissions and are not indicative of capability.

In February 2016, Moroccan authorities disrupted a Daesh cell planning to deploy biological weapons. It is reported that “some of the seized substances... are classified by international organisations... as falling within the category of biological weapons dangerous for their capacity to paralyse and destroy the nervous system and cause death”.⁴⁶

In line with CWs, the most likely threat of a biological attack against the UK comes from the knowledge and experience of returning fighters from Iraq, Syria and elsewhere. While online AQ extremist material appears to be focusing on conventional attack methods, Daesh is utilising the Internet, particularly the Dark Web, to share knowledge in the production of bio weapons, particularly ricin.*

There are concerns about the ease with which someone with a basic knowledge of science could manufacture a biological weapon in their kitchen. This threat, specifically where ricin and anthrax are concerned, has been recognised by the government and been the focus of recent contingency plans and emergency service-sector training exercises. The media reporting of these exercises clearly illustrates the psychological hold the use of BWs has over the public, irrespective of how probable or destructive a successful attack would be. Even credible hoaxes have the potential to cause wide-spread alarm and distress, together with significant disruption to businesses. Events such as the 2001 United States anthrax attacks demonstrate the heavy costs to the (re)insurance industry of a successful BW attack in terms of business interruption and decontamination.⁴⁷



Insider Threat

People are an organisation’s biggest asset. However, in some cases they can also pose an insider risk. As organisations implement increasingly sophisticated physical and cyber security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

An insider could be a full-time or part-time employee, a contractor or even a business partner. An insider could deliberately seek to join your organisation to conduct an insider act, or may be triggered to act at some point during his or her employment.

Ongoing vetting of personnel should be an integral part of an organisation’s security strategy.

For further information see CPNI advice [<https://www.cpni.gov.uk/reducing-insider-risk>]



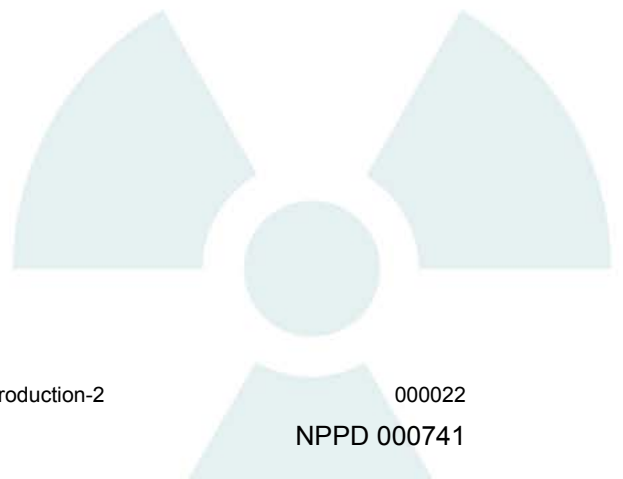
Radiological

A radiological dispersal device (RDD) could be as simple as a small amount of radiological material either strapped to a conventional explosive device, or simply deposited in a public space. The purpose is not to engineer a chain reaction involving nuclear fission like an improvised nuclear device; rather it is to contaminate an area, causing disruption and economic damage. It is highly likely such disruption and damage would last extensively longer than the initial explosion, potentially years. The initial explosion is likely to generate blast damage as well as dispersing the material.

Radiological sources are relatively commonplace, and this availability can make them attractive to terrorists for use in weapons – although this availability has not translated into use. Legitimate use of such material is restricted and highly regulated in fields such as medicine, extractive industries and academic research. Such strict controls may account for them not being used.

Daesh has confirmed aspirations to acquire radiological material for use in attacks. In 2014, the group stole nearly 40kg of low enriched uranium from Mosul University in Iraq.⁴⁸ Owing to its age and limited toxicity, the material could be used to spread panic rather than to inflict serious physical harm. Daesh possession of such material is still a concern.⁴⁹ In late 2015, a number of plots were uncovered in Moldova; organised criminals were planning to smuggle radiological material to people they believed were members of Daesh.⁵⁰ This is indicative of the illegal trade of radiological material within Eastern Europe.

The UK has robust defence protocols to detect radiological material, although the threat of a RDD attack remains. Such an attack would cause significant costs to (re)insurers in the form of property damage and business interruption as well as damaging the public confidence in the ability of the state to protect its citizens.





Nuclear

The probability of any terrorist group acquiring a fully operational nuclear device is extremely low. In the unlikely event of it occurring, it would most likely be in the form of a manufactured Improvised Nuclear Device (IND). This is due to the fact that only nuclear-equipped nation states possess modern nuclear weapons, and the sale or sponsorship of such a capability would not be in the foreseeable interests of any such state. Theft of the correct fissile material, or otherwise illegal means of acquisition, and construction, appear to be the most likely pathway for non-state actors, although this is highly improbable owing to the significant protective measures applied to establishments, including armed police within the Civil Nuclear Constabulary.*

The design of an IND would be extremely complex. Even if one were successfully detonated, it is more likely to result in the dispersal of radioactive material similar to an RDD, rather than be a viable nuclear device. It is unlikely that this could be achieved without significant input and assistance from a nation state. In any such instance, where a nuclear-equipped nation state enables a terrorist group to commit such an attack against the UK, not only would the damage be of a scale as to eclipse any recovery efforts by the (re)insurance industry, but it would likely constitute an act of war, which would have implications for insurance coverage.

A nuclear attack within the UK is highly unlikely. Military and civil establishments are extremely well protected, making any potential penetration by terrorists, or others with hostile intent, improbable. Insider threat and hostile reconnaissance risks are well mitigated against. Nuclear material in transit is also well guarded, making possible interdiction extremely difficult. Even in the unlikely event nuclear material is acquired, the resulting potential device is more likely to be in line with a RDD.

Conclusion

In response to this persistent threat, the UK government's 'CBRN(e) Operational Response Framework'⁵¹ offers a structured approach to managing the stages of a CBRN incident and considers post-incident recovery. Key to the success of this framework will be specialist advice and knowledge at the CBRN Centre, hosted by the West Midlands Counter-Terrorism Unit, and testing emergency service responses through national counter-terrorism exercises.

Counter-terrorism response exercises are likely to convey the reality of the CBRN threat and trigger fear in the public, particularly if there is heavy media coverage. As with any attack method, the wider response and recovery from a CBRN attack in the UK would be greatly assisted by the public and businesses complying with the many official mitigation products available, such as projects ARGUS, GRIFFIN, Run, Hide, Tell and other advice on the CPNI website.** This also emphasises how businesses should have reliable contingency and business continuity plans in place for all attack types, including CBRN.

A CBRN event would have significant effects, lasting well beyond the immediate post-incident time period. Those effects are likely to include public fear of the CBRN materials and a lack of confidence in the effectiveness of decontamination procedures both across both public areas and business premises. It is important that post-incident responses by both the public and private sectors are effective at providing assurances to the public to overcome their fear.

Owing to the complexity and extent of decontamination and clean-up, business interruption (BI) would be significant; the initial decontamination and clean-up of the 2001 anthrax attacks cost an estimated \$330 million.⁵² Such an attack would likely result in significant loss of attraction requiring suitable market coverage for damage and non-damage BI.

A CBRN attack is highly unlikely in the UK; acquisition of any of the necessary components to make an attack successful is very problematic and requires a level of knowledge beyond most capabilities. The UK has strong defences and an ability to detect CBRN material both at the border and within the country.

In order to better understand the effects of a CBRN attack in the UK, Pool Re continues to develop a CBRN loss estimation model with Cranfield University to be used for underwriting and risk quantification.

* The CNC is the non-Home Office police force with responsibility for the armed protection of nuclear sites and materials in the UK. It is subject to consideration for amalgamation with the MOD and British Transport Police forces to safeguard critical national infrastructure.

** See section on Risk Mitigation and Resilience for further information.

Cyber Terrorism



Trending: #CyberTerrorism

The number of cyber incidents continues to increase. An organisation can face a number of cyber threats. Some may be internal, such as from employees with malicious or hostile intent, while others may be external, from threat actors with a range of motives.

State-backed cyber operations, as demonstrated by the alleged Russian attacks against the US Democratic Convention and French TV5 Monde, are now seen by some world leaders as legitimate acts of political aggression. While terrorists are becoming increasingly active on the Internet, their capabilities remain lower than state actors and organised criminals, who are more sophisticated and better resourced. Cyber represents a fast-growing area of crime, owing to expanding IT platforms, the Internet of Things and more criminals being attracted to the opportunity, along with bespoke software, such as ransomware, making crimes easier to commit. Terrorists currently remain largely preoccupied with using the digital sphere for communicative rather than disruptive or destructive means, although they are likely to have aspirations to develop their capabilities. A cyber-attack is considered to be a malicious and deliberate unauthorised act against a computer system's confidentiality, integrity and accessibility in order to disrupt service or cause physical harm.

The UK faces cyber threats from many sources, including organised criminals, espionage, political activists and terrorists. The 2015 Strategic Defence and Security Review (SDSR) and the 2016 National Cyber Security Strategy (NCSS) recognise cyber-attacks as a significant threat. The greatest cyber-terror threat to the UK is from Islamist extremists, although at the moment their ideology calls for direct physical attacks on Westerners rather than harm and disruption through cyber means. As such, traditional terrorist attacks remain more of a threat. There is, however, the potential for cyber threats to increase in line with the evolution of AQ and Daesh's expansion into cyber-space as the groups' physical territory is reduced.

Impact and probability: Cyber



Figure 7.

Daesh-affiliated groups, such as the United Cyber Caliphate Army and the '#britainunderhack' campaign, have carried out small-scale social media and website defacements. This activity is more 'disruptive' than 'destructive' and in line with the traditional concept of 'hackers', rather than a strong terrorist capability to mount a significant cyber-attack.

"In cyber-space those who want to harm us appear to think they can act both scalably and deniably. It is our duty to demonstrate that they cannot act with impunity."

The Rt Hon. Philip Hammond MP⁶³

As with any form of terrorist attack, success depends on shortcomings in mitigation and protection. A successful cyber-attack is often made against websites with weaker security measures or social media accounts with easy to compromise password resets, allowing unauthorised access and use. This has been recognised by the UK government's investment in the National Cyber Security Centre (NCSC) to assist in the protection of UK critical national infrastructure. Furthermore, the NCSS established the pillars of 'Defend', 'Deter' and 'Develop' to offer advice and resilience against attacks.

NCSC

The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. As the public-facing arm of GCHQ, the NCSC aims to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. The centre collaborates with other government agencies and departments as well as with organisations, businesses and individuals.

Terrorists also use the Internet for reconnaissance and intelligence gathering to enable further physical terrorist acts. This was clearly illustrated by the threat posed by Junaid Hussain in Syria, prior to his death in 2015, and the numerous Daesh 'kill lists' published in recent years, either as stand-alone releases or within publications such as AQAP's *Inspire* magazine. While Hussain posed a significant threat to the UK, illustrated by his role in external attack planning, his death did not greatly reduce the capabilities of Daesh and the 'cyber caliphate'.

Terrorist use of the Internet to research and publish personally identifiable information about individuals online to make them vulnerable for attack, or 'doxing', is also increasing. While it is more likely UK-based extremists will focus their physical attacks upon crowded places or specific high-profile individuals such as the police or military, the risk to individuals from 'doxing', or being named in extremist publications, is significant.

While terrorists undoubtedly have aspirations for a major 'destructive' cyber-attack, their behaviour for now is likely to remain focused around enabling attacks, website and social media defacements, and other 'hacking' and fundraising activities. It is likely the UK will experience an increase in extremists with more sophisticated computer skills from which could emanate a cyber threat. This could be a UK-based lone actor who comes into contact with core leadership through participation in online forums. Over the next 12 months, however, an increase in UK attack planning plots should be expected in line with the fighters returning from the so-called Caliphate above any successful major cyber-attack.

It is plausible terrorists may utilise organised criminal groups to mount cyber-attacks on their behalf, potentially with the criminals not being fully aware of on whose behalf they are acting. This would also be in line with the terrorist/criminal nexus being experienced in the physical world, particularly from the prison estate.

State-sponsored terrorism is not a new concept, and, while it remains possible that such activity could progress into the cyber realm, it is unlikely at this time. While attribution of cyber-attacks remains very difficult, which could offer some reassurance to a prospective state sponsor of cyber terrorism, the potential consequences for such an actor would be significant. That risk is most likely to limit the likelihood of this scenario maturing.

Insurance solutions to cyber risks have been emerging over the past decade, but it is fair to say that further development is required to offer clients the cover they need. The cyber market has focused primarily on risks relating to data or other intangible property, in addition to liability consequence and the loss of such property. Cover for damage to tangible property, such as buildings or contents, triggered by remote electronic means is usually excluded by property policies if it involves malicious actors such as hackers or criminals.

Pool Re terrorism cover currently excludes damage caused by cyber terrorists. However, significant resources have been allocated to assess where and if such cover could be provided.

Dark Web

Internet content that exists on the public Internet but that requires specific software or authorisation to access. The Dark Web forms a small part of the Deep Web, the part of the Internet not indexed by search engines.

Incident key:
■ Most incidents
■ Several incidents
■ Fewer incidents

Evidence of cyber capability

	A. Enabling Activity				B. Disruptive Activity				C. Destructive Activity			
	A1. Terror group website	A2. Video & social media	A3. Funding operations manuals	A4. Encrypted communications	B1. Defacement of websites	B2. DDoS website take-down	B3. Data exfiltration hack	B4. Cyber financial heist	C1. Sensor spoofing	C2. Control engineering compromise	C3. Damaging/disabling infrastructure	C4. Scaled destruction on multi targets
Threat Group 1 e.g. al-Qaeda												
Threat Group 2 e.g. Islamic State United Cyber Caliphate												
Threat Group 3 e.g. Cyber group loosely affiliated to a nation state												
Threat Group 4 e.g. Hacktivists Militant Destructive												
Threat Group 5 e.g. Organised criminal group with terror links												
	Enabling Online activities that support the operations of terrorist groups such as publicity and propaganda, fundraising, recruitment, reconnaissance, clandestine communications between members and disseminating manuals and know-how to incite and facilitate attacks by others.				Disruptive Online activities that disrupt the information technology of opponents including proactive cyber breaches of networks, dissemination of malware, exfiltration of digital information, financial theft and fraud, denial of service attacks, phishing and other information technology hacking activities.				Destructive Cyber-attacks that trigger physical damage or injury through spoofing operation technology and digital control systems.			

Figure 8. Cyber Threat Capability Chart, showing evidence for which threat actors have attained capabilities on a 12-point scale, left to right, towards 'Destructive' capabilities, research undertaken by Cambridge Judge Business School and Pool Re



Emerging Risk Report: Drones



Unmanned Terror

There have been significant developments in the commercial and consumer drone markets over the last three years,⁵⁴ and the progression continues at an increasingly rapid pace (Figure 9). Drones, also known as Unmanned Aerial Vehicles (UAVs), were once expensive toys for hobbyists but now appeal to all age groups, price ranges and industries.

Recent analysis by Goldman Sachs forecasts that between 2016 and 2020 there will be a \$100 billion market opportunity within all sectors of the drone market, with a specific \$17 billion market for consumer drones, with more room to grow.⁵⁵ There is a broadening list of commercial clients with the desire to expand into this technological space – Amazon and Domino's Pizza are among many companies making this more commonplace – and the market has seen a significant shift from the military use of drones to industries as diverse as agriculture, filming, construction and energy.

Unsurprisingly, with the growing potential in this space, there are increasing safety and security fears about the use of drones by extremists. The implications of an easily accessible market with a slow, reactive regulatory framework have alerted security professionals and analysts in the UK. Commercial and consumer drones are relatively easy to acquire online, or on the high street, and can now be legally bought with little cost to the consumer. It is possible that terrorists may be inspired to use drones in an attack against the UK as the drone market increases in sophistication and availability. This fear has been heightened by reports of Daesh using drones for surveillance operations, battlefield damage assessment and dropping explosive devices in the Middle East over the last couple of years. The return of foreign fighters from the so-called Caliphate to the UK could result in a knowledge transfer for the potential use of weaponised drones.

Likely Targets

Although Hezbollah and Daesh have been using surveillance drones in the Middle East for several years and weaponised drones since August 2016,⁵⁶ conducting an attack using a drone in the UK would present a novel attack vector.

An airborne IED (ABIED) would greatly expand the target selection for a terrorist group beyond traditional on-the-ground locations. It would be able to access areas outside standard physical security recommendations, not currently considered vulnerable to attack. Risk mitigation measures recommend raising bollards outside buildings to protect against VBIEDs or PBIEDs. However there is currently no equivalent for the roof of a building, or a crowded place, both of which are vulnerable areas. When considering a potential airborne UAV attack involving the use of a chemical or biological weapon, mitigation measures in place are currently even more limited.

A potential target for an ABIED in the UK would be a crowded place, such as sports stadia, airports, shopping malls and open-air festivals, owing to their accessibility and the potential to inflict mass casualties. The list of prohibited airspace areas in the UK (Houses of Parliament, Downing Street, Buckingham Palace, nuclear power stations and military establishments) does not include any such crowded places. Stadia have been targeted recently by ground attacks (for example, the Stade de France in Paris, November 2015) but there have also been earlier incidents.

Global sales set to increase Retail/consumer drone market

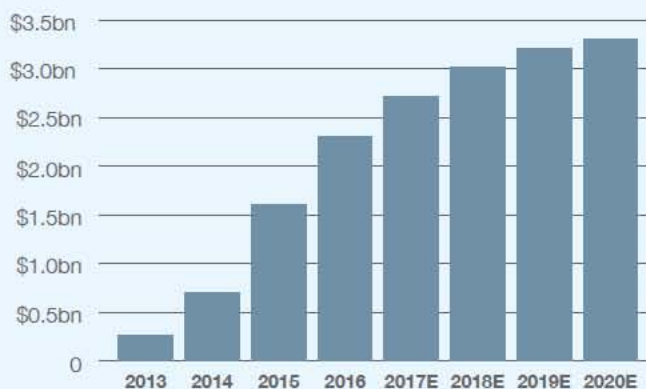


Figure 9. The projected growth of the consumer drone market 2013–2020, Goldman Sachs⁵⁷

“Daesh is like water at the top of a building, it spreads across and tries to find little gaps it can run through. This will be one of the little gaps it is looking at. I think it would be foolhardy for us not to look at our defences for this.”

Admiral Lord West⁵⁸

In October 2014, a football match between Albania and Serbia was halted because of a flag-flying drone hovering just above the pitch. In the UK, a security guard was arrested for flying a drone over, and filming, Premier League, Champions League and Championship football matches on several occasions.⁵⁹ The vulnerability of stadia was further emphasised by the encouragement of Daesh of its fighters to target the 2016 Olympic Games in Rio de Janeiro with “toy drones with small explosives”.⁶⁰

Equally, nuclear power stations are considered to be vulnerable to ABIED for similar reasons of accessibility and risk of damage. In 2012, a Greenpeace activist paraglided over Le Bugey nuclear power station in France in protest over the (lack of) security around power plants. In 2014, there were sightings of around fifteen drones above a nuclear power station in Belleville-sur-Loire, France. Although these were not malicious attacks, both examples highlight the vulnerabilities of the airspace and no-fly zones surrounding sensitive sites.

Intent and Capability

There have been no drones involved in a terrorist attack in the UK, and, according to UK intelligence analysts, there is no evidence to suggest the intention of one being used at this present time. This may be due to the more prolific low-sophistication attack methods seen in the UK, which in turn are led by the difficulty in acquiring firearms and the strength of MI5 and the police to disrupt attack plans. Following the arrests of terrorist suspects in the UK, or in subsequent searches of their premises, there has not been any reference to, or presence of, a drone. This suggests that this attack method may not be considered to be a high priority by terrorist organisations at this time.

The increasingly sophisticated drones on the market with high technological capabilities may appear to increase the threat to the UK; new models have greater payload, range, duration and navigation systems. Agricultural drones, for example, are capable of flying (pre-programmed) over specific areas with sizeable payloads of weed killer or

fertilizer, identifying areas in need of spraying, utilising waypoints and then returning to the ‘pilot’. Daesh have shown capability in the Middle East: two Kurdish soldiers were killed and two French soldiers were injured when an IED on a drone exploded as the soldiers took it back to base. This was reportedly the first drone attack by Daesh to cause casualties, although the full circumstances of the explosion and their deaths are not known. This attack method is not new, and, as the technology advances, it is not difficult to plan a scenario where drones are manipulated to deploy an IED or a chemical weapon in a main city in the UK. However, this threat must be considered in context.

Making an IED is complex and risky. In the UK environment, where it is particularly difficult to acquire commercial explosives such as Semtex or TNT, any IED would most likely be a home-made device. Triacetone Triperoxide (TATP) is an increasingly common explosive, used in the recent device at Zaventem Airport in Brussels and on the Tube in London on 7/7. It is a particularly unstable and flammable⁶¹ explosive, and, despite Al Qaeda’s *Inspire* magazine offering an ‘easy’ how to make a bomb guide – it takes considerable skill and knowledge to use the material. Although not directly linked to terrorism, the recent failed device at North Greenwich tube station proved the difficulty in making a viable explosive that detonates successfully (many devices detonate only partially).

As well as the considerable expense incurred by the perpetrator, there are added complications of weaponising a drone effectively – difficulties in reaching the correct location, challenges of detonation, problems of flying outside the line of sight – all of which would make it a much less viable attack method than leaving the same type of IED on a tube, on a bus or in the street. The more complicated the attack method, the more likelihood of it being detected by MI5 or the police.

AQ’s *Inspire 16* magazine includes a tutorial on a successful pressure cooker bomb, the device used in Boston and New York. If there is an increase in plots seeking to use IEDs, these IEDs are more likely to be pressure cooker devices, because of their relative simplicity of construction. Given the payload and design of drones currently on the market, it is unlikely that a workable device would be attached to a drone.

Alternatively, drones pose a threat as a weapon in itself, mostly to aircraft. Chris Grayling, the UK Secretary of State for Transport, warned that the expansion of the delivery drone market posed a safety risk and should be “handled with great care”.⁶² Near misses with drones have been a nuisance to aircraft and to police; between January and October 2016, 56 drones were involved in near misses with aircraft over the UK – almost double the amount in 2015.⁶³

An aircraft flying over the Shard in London in November 2016 reported a near miss with a drone at over 1,000ft in height, and in December a drone was reported at 11,000ft. However, the likelihood of a drone causing damage to an aircraft does not increase with the sophistication of the drone or the height at which it can fly. At over 1,000ft, it would be challenging to manoeuvre and direct a drone into the wing of an aircraft, and even if the attack were successful, the size of the drone would probably not cause the aircraft to crash nor cause large-scale physical damage. On smaller aircraft, a drone, like a bird, may cause the engine to cut out and lead to an emergency landing. US Airways Flight 1549 emergency landed in the Hudson River after reportedly being hit by multiple bird strikes, which caused both engines to fail. Bringing down a plane would require a swarm of drones, which brings the likelihood of such an event back to the ability of the user(s) to direct them with precision.

Mitigation

Mitigating against an ABIED is a difficult and developing issue. There are no-fly zones in place, but these are only valid only if adhered to. There are other, expensive, anti-drone mitigation measures on the market – geo-fencing, birds of prey, nets, DroneShield are some examples. However above a crowded place, a weaponised drone would present as much of a threat in the air as it would if it were to be brought down. There are added concerns about third party liability and the collateral damage caused by an out of control drone, especially if it has been brought down deliberately by the police.

The average drone on the consumer market costs around £78 and can fly 167.26 metres for 12.83 minutes. The maximum payload of the sample selection is 2.3kg.* Although they can be bought with relative ease, if this was the attack method of choice for a terrorist, the regulation in the UK around drones would be a limitation in itself. While there is no regulation to enforce the registration of drones or drone users, the current regulation requires flight within line of sight of the user (estimated to be 500m), no higher than 400ft in altitude, at least 50 metres away from any person or vehicle and at least 150 metres from a congested area. As such, if a drone were operated within a sensitive environment such as the Government Security Zone (GSZ), it is highly likely the operator would be reported to the police or disrupted by protective security patrols.

It has been recognised that UK Corporate Security Officers do not yet consider drones to be a priority attack method and there have only been a handful of incidents involving hobbyist pilots. The main implications for businesses present themselves through the use of drones for surveillance and data theft. However, the increase in intent and capability, improving drone technology, challenges of mitigating against an expanding market, issues of legislating against individuals who will not adhere to the law and the problems of identification and attribution, heighten the risk of such an attack happening in the UK. It would be necessary at that stage to reassess the technological advances and the probability of this type of attack methodology.

Demonstrated possession and/or attempted UAVs use by terror actors worldwide

Key

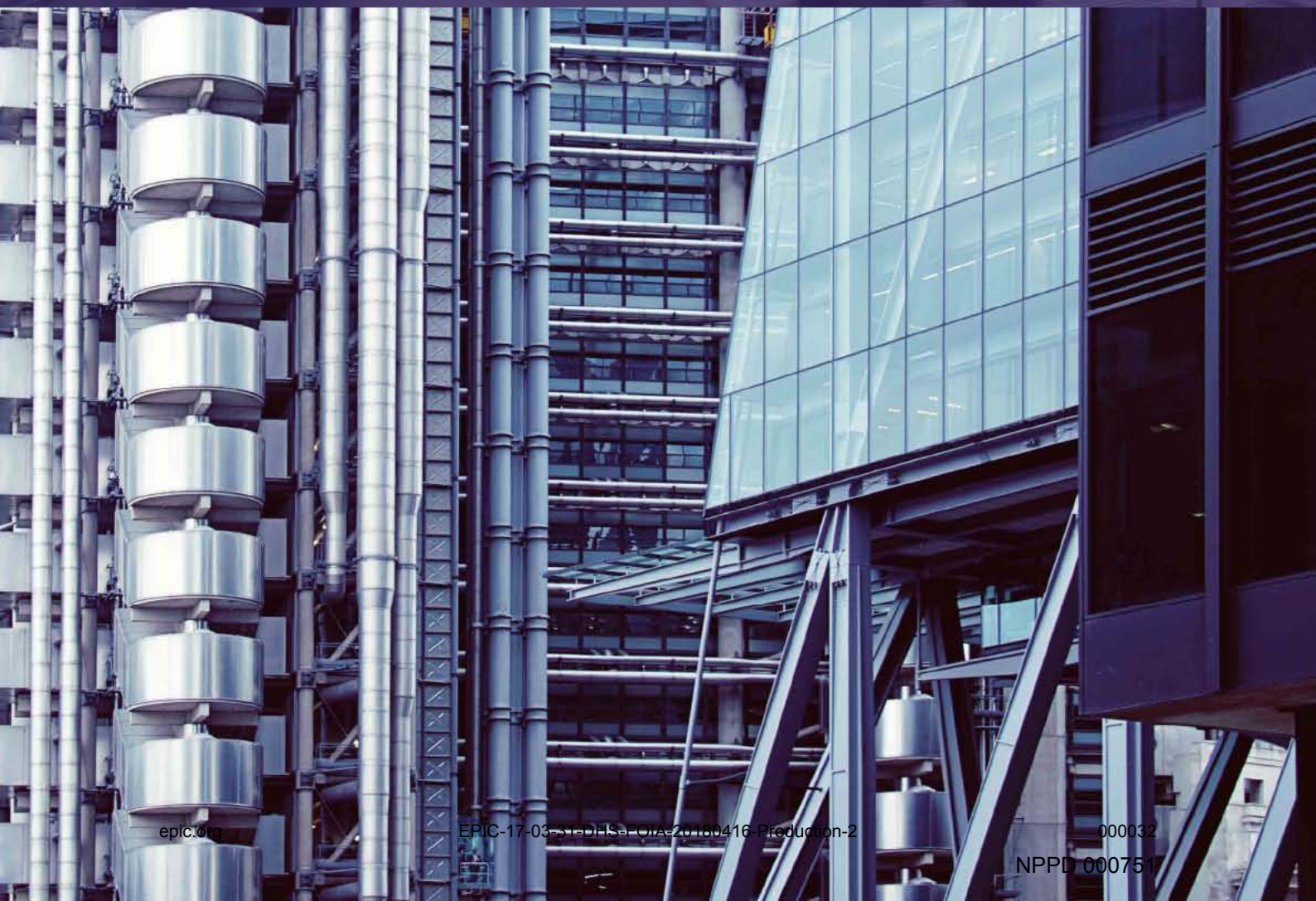
- Terror entity possession and/or attempted use of UAVs

Figure 10. Demonstrated possession and/or attempted UAV use by terror actors worldwide, *Combating Terrorism Centre at West Point*⁸⁴



* Data collected from <http://drones.specout.com> and average taken from the 166 results filtered by the following criteria: price under \$200, maximum flight time more than 10 minutes. The JYU Spider X has the most payload capacity at 2.3kg. Data accurate as at 20 December 2016.

Risk Mitigation and Resilience



Building Resilience

The first duty of any government is to provide security for its citizens. The 2015 National Security Strategy and Strategic Defence and Security Review (SDSR) provided a timely reappraisal of national security threats, reflecting the emergence of Daesh and increased activity by state actors against the UK. The SDSR directed valuable funding to many national security initiatives, including counter-terrorism. The UK CT strategy, CONTEST, is being revised, and the 'refresh' is due to be released early in 2017.

While the pillars of the strategy – PURSUE, PREPARE, PREVENT and PROTECT – are fit for purpose, there is an expectation within the business community of improved public/private sector partnerships.

Pool Re continues to balance the public policy objectives of our UK government partners and regulators, on the one hand, and the commercial requirements of our member insurers and (re)insurers, on the other. Part of this task involves influencing and remaining current with developments in the terrorism insurance market. In October 2016, following on from the conference hosted in London twelve months earlier by Pool Re, the Australian Reinsurance Pool Corporation hosted a Global Terrorism Risk Insurance Conference in Canberra, where discussions focused around many of the issues on which Pool Re has been working. Pool Re attended and presented on the insurance aspects of terrorism in the UK.

The three primary areas of discussion at the Canberra conference were CBRN, cyber terrorism and the emerging coverage gap. The underlying message was that insurance pools are equipped to help shape the provision and type of insurance solution available to businesses, and also to influence resilience. The ability to influence resilience is contingent on a productive working relationship with the relevant government departments; Pool Re is well positioned to fulfil this role in the UK.

Not all insurance companies or brokers are equipped with dedicated terrorism expertise, so one of Pool Re's roles remains the communication of appropriate information to both the insured and the insurer, via the reinsurance transaction. Any organisation in the UK considering its approach to resilience and risk mitigation should start this process by forming a sound understanding of the threat and its associated vulnerabilities.

The MI5 website⁶⁶ remains the official and authoritative source of threat and risk information and is a helpful resource for those who are unfamiliar with the terminology or concepts. Once the threats and risks are understood, there is a range of options for risk mitigation, and the Centre for the Protection of National Infrastructure (CPNI)⁶⁶ offers advice for businesses on physical and personnel protective security, with the National Counter Terrorism Security Office (NaCTSO)⁶⁷ giving excellent advice to the private sector on responses to a terrorist attack, supporting projects such as GRIFFIN and ARGUS. For business exposures overseas, the Foreign and Commonwealth Office travel website⁶⁸ provides advice and guidance.

Businesses are equipped with sophisticated situational awareness assets and are also able to adjust their posture depending on the information with which they are equipped. While there are obvious challenges to sharing sensitive intelligence, mechanisms for sharing information in a more selective way are currently being considered, and the US model of the Overseas Security Advisory Council (OSAC) has been identified as having merit. In the interim, there are useful social media feeds that can provide an organisation with contemporary information about events. These include the FCO for an event overseas and the Metropolitan Police for a terrorism event in the UK:

 <https://twitter.com/FCOtravel>

 <https://twitter.com/metpoliceuk>

Beyond a potential gap in information sharing, terrorism events in Europe during 2015 and 2016 have highlighted the gap that exists in cover provided by traditional property terrorism insurance products, when the major impacts have been loss of life and business interruption and where no, or limited, damage occurred.⁶⁹ There is a mismatch between property-based terrorism cover and the impacts of events focused on killing or injuring people, that do not result in wide-scale physical damage.⁷⁰ Pool Re is currently undertaking work to quantify the gap between the economic losses seen after recent terrorist events and the insured losses. This includes consideration of recent events, including Berlin and Istanbul.

Early research suggests the coverage gap is meaningful in scale and spans multiple insurance classes of business. There also appears to be more of an impact for small and medium-sized enterprises than for larger corporates, which tend to be less reliant on single sites. Not all components of the economic loss after a major terrorist attack will be insurable, but an opportunity does seem to exist for more of the risk to be taken up by the commercial market. Non-damage business interruption (BI) and loss of attraction cover is already available, but it is not currently taken up widely enough to provide a systemic level of resilience.

With regards to coverage for individuals, there is also a potential gap where work, personal or government schemes may not provide adequate protection. Solutions are available in the stand-alone market for issues such as hostage barricade and active shooter scenarios, but these tend to be accessed only by well-informed insurance buyers. A wider solution that provides portfolio-level cover may be appropriate, and Pool Re is currently considering options with its Members and insurance market stakeholders.

“If we are to defeat this threat, if we are to confront [...] terrorism and extremism of all kinds, then we must work together.”

Rt Hon. Theresa May MP⁷¹

Resolving the challenges posed by the coverage gap will not be simple. There are significant interdependencies at play with regard to the insurance and reinsurance of terrorism in the UK. While the government has an obligation to clearly articulate accurate information pertaining to the terrorist threat, Member and non-member companies of Pool Re have their own duty to develop commercially viable solutions. Both have a shared objective of managing the risk and mitigating the potential impacts, and these objectives can be achieved through enhanced partnership working.

Interaction and collaboration between the public and private sectors is crucial to successful terrorism risk management. Pool Re recognises it is well positioned to help this engagement. Pool Re has been working on a number of projects with UK government partners to establish durable and pragmatic ways of public/private sector risk management. To date, the insurance market has been effective at mutualising risk, but it is more challenging to mutualise expertise, particularly when some of the critical information is sensitive and sits in the public sector. There is also a requirement for the public sector to recognise the expertise and resource available in the private sector. Building a workable solution for public and private sector liaison on terrorism risk management is key and should be done in a way that develops trust. Success will ensure that a large number of UK businesses are resilient to potential threats, and they are able to access relevant cover at an appropriate price.

Countering such threats and embracing this period of international change relies on overcoming uncertainty. The UK is facing an exit from the European Union, out of which there will doubtless emerge both threats and opportunities for the UK economy, including the insurance sector.⁷² The threat to Western Europe as a whole has been explicit and proven by numerous attacks in the past two years, and this is likely to continue regardless of the UK’s decision to leave the EU. However, Brexit is unlikely to damage national security severely, as counter-terrorism cooperation has been built up between member states for many years.⁷³ It remains to be seen what impact the American presidential election and the new Trump Administration’s foreign policy focus on defeating Daesh will have in terms of potential further motivation for recruitment and attacks by Islamist extremists.* Nonetheless, throughout this period of change there is an expectation of intelligence and counter-terrorism consistency that, together with enhanced partnership working, may afford greater mitigation to the international terrorist threat.

ARGUS



Project ARGUS is a NaCTSO counter-terrorism testing and exercising initiative, designed to provide an understanding of the threat from terrorism and of simple security measures that can be taken to protect a business or an organisation.

Its aim is to identify measures to help an organisation to prevent, manage and recover from a terrorist incident.

<https://www.gov.uk/government/publications/project-argus/project-argus>

Griffin



Project Griffin is the national counter-terrorism awareness initiative for business produced by NaCTSO, which seeks to enlist the help and support of individuals or groups interested in maintaining the safety and security of buildings, businesses, areas or neighbourhoods.

It provides an official and direct channel through which the police can share and update vital information relating to security and crime prevention.

<https://www.gov.uk/government/publications/project-griffin/project-griffin>

Run – Hide – Tell



Run, Hide, Tell is an information film, released to the public by the police service, that provides advice on the steps to take to keep safe in the event of a firearms or weapons attack.

<http://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx>

Centre for the Protection of National Infrastructure (CPNI)



CPNI is the government authority for protective security advice to the UK national infrastructure. Their role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

www.cpni.gov.uk

Investigatory Powers Act 2016



The Investigatory Powers Act 2016 received Royal Assent on 29 November 2016 and ensures law enforcement and the security and intelligence agencies have the powers required in a digital age to disrupt terrorist attacks, subject to strict safeguards and oversight.

The legislation brings together and updates existing powers while overhauling how they are authorised and overseen. It also creates one new power: the introduction of Internet Connection Records, which will be accessible by law enforcement and the intelligence agencies to disrupt terrorist attacks and prosecute suspects.

The act protects both the privacy and security of the public by introducing:

- a “double-lock” for the most intrusive powers, so that warrants issued by a Secretary of State will also require the approval of a senior judge;
- a powerful new Investigatory Powers Commissioner, to oversee how the powers are used;
- new protections for journalistic and legally privileged material, and a requirement for judicial authorisation for acquisition of communications data that identify journalists’ sources;
- tough sanctions – including the creation of new criminal offences – for those misusing the powers.

<http://services.parliament.uk/bills/2015-16/investigatorypowers.html>

International Protect and Prepare

The National Coordinator for PROTECT and PREPARE has commenced recruitment for a number of Overseas Coordinators to help mitigate the threat from terrorism overseas, either against British interests abroad or to reduce the threat to the homeland. Six priority countries have been identified and will have an International team consisting of four staff permanently deployed overseas with a UK-based team of ten, some of whom will travel out to assist in delivering the products developed by the International P&P team.

<http://www.npcc.police.uk/NPCCBusinessAreas/TAM/Protect.aspx>

CT Specialist Firearms Officers (CTSFOs)

The Metropolitan Police has appointed Project Managers to assist with resource uplifts, specifically the widely reported increase in capacity of the CT Specialist Firearms Officers (CTSFOs). While less likely compared to other attack methods, the threat of extremists undertaking a marauding firearms attack is persistent and requires specialist firearms training and resources within the police to resolve.

The CTSFO uplift has been replicated across the country, which demonstrates a recognition that a potential attack location is not limited to London.

<http://content.met.police.uk/Article/SCO19-Operational-Capability/1400024226698/1400024226698>

Notes

- ¹ <https://www.mi5.gov.uk/threat-levels>.
- ² 'How has al-Muhajiroun hidden in plain sight?', *The Times*, 21/08/16.
- ³ 'British Nationals Abroad: Islamic State', *Written Question HL1579*, 23/09/16.
- ⁴ 'Terrorism most immediate threat to UK, says MI6', *BBC News*, 08/12/16. Figure updated to include arrests in Derby, Burton upon Trent and London in December 2016.
- ⁵ 'Terror deaths in Western Europe at highest level since 2004', *BBC News*, 19/08/16.
- ⁶ 'New Study: European governments neglecting the threat of extreme right lone actor terrorists', *RUSI*, 29/02/16.
- ⁷ 'Lone Actor Terrorism: Motivations, Political Engagement and Online Activity', *RUSI*, 2016.
- ⁸ 'Five arrested in UK after inquiry linked to attacks on Brussels and Paris', *The Guardian*, 15/04/16.
- ⁹ 'Germany's manhunt for Syrian bomb plot suspect extends beyond borders', *Middle Eastern Eye*, 09/10/16.
- ¹⁰ 'Islamic State tells lone terrorists to target people on quiet walks, beaches, and night shifts', *News.com.au*, 15/10/16.
- ¹¹ 'European Union Terrorism Situation and Trend Report 2016', *Europol*, accessed via <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report>.
- ¹² 'Terrorism most immediate threat to UK, says MI6', *BBC News*, 08/12/16. Figure updated to include arrests in Derby, Burton upon Trent and London in December 2016.
- ¹³ 'Children put into care after Met's extremist hunt', *The Times*, 30/10/16.
- ¹⁴ Scott Wilson, National Counter Terrorism Co-ordinator, Protect and Prepare, 2016 Security & Counter Terror Expo, London.
- ¹⁵ 'Lessons of war: David Petraeus warns that a bigger challenge awaits after Islamic State is driven from Mosul', *Los Angeles Times*, 03/01/17.
- ¹⁶ 'ISIS plotting chemical attack on UK', *The Times*, 01/01/17.
- ¹⁷ 'UK to extend Europol membership', *BBC News*, 14/11/16.
- ¹⁸ 'Exclusive: Britain will demand a leading role in Europol after Brexit', *The Telegraph*, 29/12/16.
- ¹⁹ 'Resurgent al-Qaeda plots deadly attacks against UK and Europe', *The Times*, 06/10/16.
- ²⁰ *Ibid.*
- ²¹ 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus', *International Centre for the Study of Radicalisation and Political Violence* October 2016.
- ²² 'Changes in Modus Operandi of Islamic State Revisited', *Europol*, November 2016.
- ²³ 'Quietly and Patiently Rebuilding', *The Cipher Brief*, 07/10/16.
- ²⁴ 'US bans uncharged mobiles and other devices on planes', *Channel 4 News*, 06/07/14.
- ²⁵ MI5 Threat Levels <https://www.mi5.gov.uk/threat-levels>.
- ²⁶ 'U.S. "Within Reach" of Breaking Al-Qaeda, Panetta says', *NTI*, 11/07/11.
- ²⁷ 'Pentagon confirms death of al Qaeda-tied bombmaker', *CNN*, 23/09/15.
- ²⁸ 'Yemen al-Qaeda chief al-Wuhayshi killed in US strike', *BBC News*, 16/06/15.
- ²⁹ 'Al Qaeda threatens to use 'undetectable' bombs against the U.S.', *The Counter Jihad Report*, 06/01/15.
- ³⁰ 'Al Qaeda leader to ISIS: You're wrong, but we can work together', *CNN*, 15/09/15.
- ³¹ 'Al Qaeda branch claims Charlie Hebdo attack was years in the making', *CNN*, 21/01/15.
- ³² Al-Qaida leader pledges allegiance to new Afghan Taliban chief, *The Guardian*, 13/08/15.
- ³³ 'AQAP's Inspire magazine contains 'military analysis' of Charlie Hebdo massacre', *Long War Journal*, 11/09/15.
- ³⁴ Plotter's flat contained ricin ingredients "for an attack on Jewish centre", *The Independent*, 13/04/05.
- ³⁵ 'National Risk Register of Civil Emergencies 2015', *Cabinet Office*, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf.
- ³⁶ 'ISIS used chemical arms at least 52 times in Syria and Iraq, report says', *New York Times*, 21/11/16.
- ³⁷ 'Syrian rebel groups sought sarin gas material, Turkish prosecutors say', *Los Angeles Times*, 13/11/13.
- ³⁸ 'Exclusive: Inside IS Terror Weapons Lab', *Sky News*, 05/01/16 <http://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883>.
- ³⁹ 'ISIS is planning a chemical attack on Britain', *Business Insider UK*, 01/01/17.
- ⁴⁰ 'CIA Director: ISIS has used and can continue to make chemical weapons', *Newsweek*, 12/02/16.
- ⁴¹ 'ISIL manufacturing its own chemical weapons, warns watchdog', *The Telegraph*, 04/05/16.
- ⁴² 'ISIL carrying out chemical experiments on its prisoners as it moves labs into residential neighbourhoods', *The Telegraph*, 22/05/16.
- ⁴³ 'ISIS' chemical weapons: a mix of Saddam, Assad and the West', *Rudaw*, 15/03/16.
- ⁴⁴ For further statistics on secure biolabs, see 'Emerging Risk Report: The threat of asymmetric attack methods, CBRN', *Pool Re*, June 2016.

- ⁴⁵ 'Found: The Islamist State's laptop of doom', *Foreign Policy*, 28/08/14.
- ⁴⁶ 'Arrested ISIS Militants In Morocco Planned "Biological" Attacks: Report', *International Business Times*, 03/03/16.
- ⁴⁷ For further reading, see 'Emerging Risk Report: The threat of asymmetric attack methods, CBRN', *Pool Re*, June 2016.
- ⁴⁸ 'Could ISIL go nuclear?', *NATO*, 2015.
- ⁴⁹ 'Could ISIL go nuclear?', *NATO*, 2015.
- ⁵⁰ 'FBI foils plot to sell nuclear material in Moldova', *The Guardian*, 07/10/15.
- ⁵¹ www.jesip.org.uk/cbrn.
- ⁵² 'Total Decontamination Cost of the Anthrax Letter Attacks', Ketra Schmitt and Nicholas A. Zacchia, *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, vol.10, no.1 (2012).
- ⁵³ Chancellor's speech: launching the National Cyber Security Strategy, 1 October 2016, <https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy>.
- ⁵⁴ The Drones Report: Market forecasts, regulatory barriers, top vendors, and leading commercial applications, *BI Intelligence*, 10/06/16. <http://uk.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2>.
- ⁵⁵ Drones: Reporting for Work, *Goldman Sachs 2016*. Accessed online: <http://www.goldmansachs.com/our-thinking/technology-driving-innovation/drones/?scRef=slipcase>.
- ⁵⁶ 'Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology', *Combating Terrorism Centre at West Point*, October 2016.
- ⁵⁷ 'Drones, Reporting for Work', *Goldman Sachs*, 2016.
- ⁵⁸ 'Ex-Navy chief warns ISIS 'could drop bombs on UK targets using drones'', *The Mirror*, 01/08/16.
- ⁵⁹ 'Man fined for flying drone at football matches and Buckingham Palace', *The Guardian*, 15/09/15.
- ⁶⁰ 'Jihadis call for MAYHEM at Rio Olympics as fears grow over chemical attack on soft targets', *The Express*, 02/08/16.
- ⁶¹ 'Explosives linked to London bombings identified', *New Scientist*, 15/07/05.
- ⁶² 'Delivery drones have their wings clipped by minister', *The Times*, 22/11/16.
- ⁶³ Ibid.
- ⁶⁴ 'Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology', *Combating Terrorism Centre at West Point*, October 2016.
- ⁶⁵ <https://www.mi5.gov.uk/terrorism>.
- ⁶⁶ <https://www.cpmi.gov.uk/>.
- ⁶⁷ <https://www.gov.uk/government/organisations/national-counter-terrorism-security-office>.
- ⁶⁸ <https://www.gov.uk/foreign-travel-advice>.
- ⁶⁹ '2016 Terrorism Risk Insurance Report', *Marsh*, July 2016.
- ⁷⁰ 'Industry must expand terrorism-related cover', *Guy Carpenter*, 13/09/16.
- ⁷¹ 'We must work together to defeat terrorism', *Home Secretary Rt Hon. Theresa May MP*, 18/06/15.
- ⁷² *Commercial Risk Europe*, Volume 7, #10, December 2016/January 2017.
- ⁷³ Baroness Neville-Jones, *Pool Re Insight* magazine, December 2016.



Pool Re was established in 1993 as a response to the market failure triggered by the bombing of the Baltic Exchange. The costs of the Provisional IRA's mainland bombing campaign in the 1990s led to reinsurers withdrawing cover for terrorism-related damage, with insurers compelled to follow suit. Pool Re was founded by the insurance industry in cooperation with, and backed by funding from, Her Majesty's Treasury to form a private sector solution to a public policy objective.

Since its foundation, Pool Re has provided effective protection for the UK economy and currently underwrites over £2 trillion of exposure to terrorism risk in commercial property across the UK mainland. To date, Pool Re has paid out claims of more than £600 million at no cost to the UK taxpayer. The largest claim, £262 million, resulted from the 1993 Bishopsgate bombing in the City of London. The exposures in the same area today would be significantly in excess of that figure.

Pool Reinsurance Company Limited

5 Lloyd's Avenue
London EC3N 3AE

Contact

E enquiries@poolre.co.uk

T +44 (0)20 7337 7170

F +44 (0)20 7337 7171

W poolre.co.uk

 [@poolreinsurance](https://twitter.com/poolreinsurance)

 [linkedin.com/company/pool-re](https://www.linkedin.com/company/pool-re)

POOL RE

REINSURING TERRORISM RISK