Quarterly Threat Report

Pool Re Terrorism Research & Analysis Centre

POOL RE

REINSURING TERRORISM RISK

Quarterly Threat Report
August 2016

Contents

https://www.poolre.co.uk/Reports/Quarterly-Threat-Report-Aug-2016.pdf (retrieved 23 October 2016)

POOL RE
REINSURING TERRORISM RISK

The Security Service threat rating

Critical	An attack is expected imminently
Severe	An attack is highly likely
Substantial	An attack is a strong possibility
Moderate	An attack is possible but not likely
Low	An attack is unlikely

Target types

CP	Crowded place
Symbolic	Place of worship
Property	Commercial & residential property
CNI	Critical national infrastructure

Attack types

Bladed	Non-firearm attack
Dual-use	Vehicular-based attack
MTFA	Marauding terrorist firearms attack
PBIED	Person-borne improvised explosive device (IED)
VBIED	Vehicle-borne improvised explosive device (IED)
LVBIED	Large vehicle-borne IED
CBRN	Chemical, biological, radiological, nuclear

Overview

Introduction

The Pool Re Terrorism Research and Analysis Centre (TRAC) is pleased to present its first Quarterly Threat Report. For the first edition in this series, the team has focused on key terrorism events and trends from January-August 2016. Pool Re has invested significant resources into its research and peril analysis capability and it is assessed that, combined with the Pool Re Emerging Risk Reports[1], this quarterly edition will provide a valuable source of information and guidance to the (re)insurance sector and wider stakeholders. As well as providing reporting and analysis, Pool Re is also developing sophisticated loss estimation models, in collaboration with our external research partners, for CBRN and the emerging risk of destructive cyber terrorism. The Pool Re TRAC will aim to publicise the findings of these ongoing projects to industry risk carriers, security specialists within the private sector and Government partners.

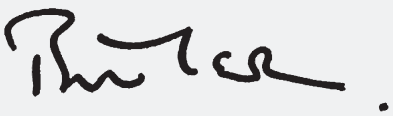
Methodology

TRAC's methodology is based on the effective fusion of open-source intelligence (OSINT) with propriety human source networks (HUMINT). The information contained in this report has been verified and triangulated through extensive research drawn from academia, think-tanks, social media intelligence (SOCMINT), security and intelligence risk conferences as well as extensive subscription-based content. Importantly, this OSINT has been combined with consultations with former Government officials and counter-terrorism experts, trusted individuals working in countries of interest and retained subject matter experts, giving Pool Re a truly unique perspective within the terrorism reinsurance environment.

Purpose

The purpose of this report is to inform Pool Re, its Members and wider stakeholders of the current and future terrorism threat. All assessments and trends are made in relation to the threat posed to the UK and tailored to the information requirements of the (re) insurance sector. ●

Ed Butler CBE DSO,
Head of Risk Analysis,
Pool Re.



1. The first of these, on the subject of CBRN, was issued to Members in July.

Executive summary

In the first nine months of 2016, which constitutes our first reporting period, Europe has seen a dramatic increase in 'inspired' terrorist attacks. Such incidents have successfully employed simple attack methods, targeting people over property, resulting in mass casualties. In addition to this, 'directed' well-resourced attacks, carried out by seasoned networks of terrorist actors, have also targeted key transportation hubs, causing significant damage to commercial property.

Over the course of 2016, Europe has been transformed from a recruiting ground for foreign fighters, destined for the conflicts in the Middle East and North Africa, to a battleground for lone actors, inspired by terrorist propaganda.

Daesh remains the principal threat actor to both mainland Europe and the UK. The intelligence and security services are interdicting terrorist suspects at an unprecedented frequency. The severity of the threat to the UK cannot be underestimated and senior officials and counter-terrorism experts have openly stated that the question of an attack has become a matter of when, not if.

The targeting of people over property is causing risk carriers to re-evaluate their policy triggers as traditional terrorism loss drivers have been damage to commercial property. Although the Brussels bombings at Zaventem airport and Maelbeek metro station did result in damage to property, events such as Nice are tragic examples of high-impact incidents where the principal loss drivers are non-damage and contingent business interruption, as well as a wider loss of attraction. At the same time, the terrorism threat spectrum has broadened and now includes prima facie systemic risks posed by cyber terrorism and unconventional uses of weapons of mass effect (CBRN).

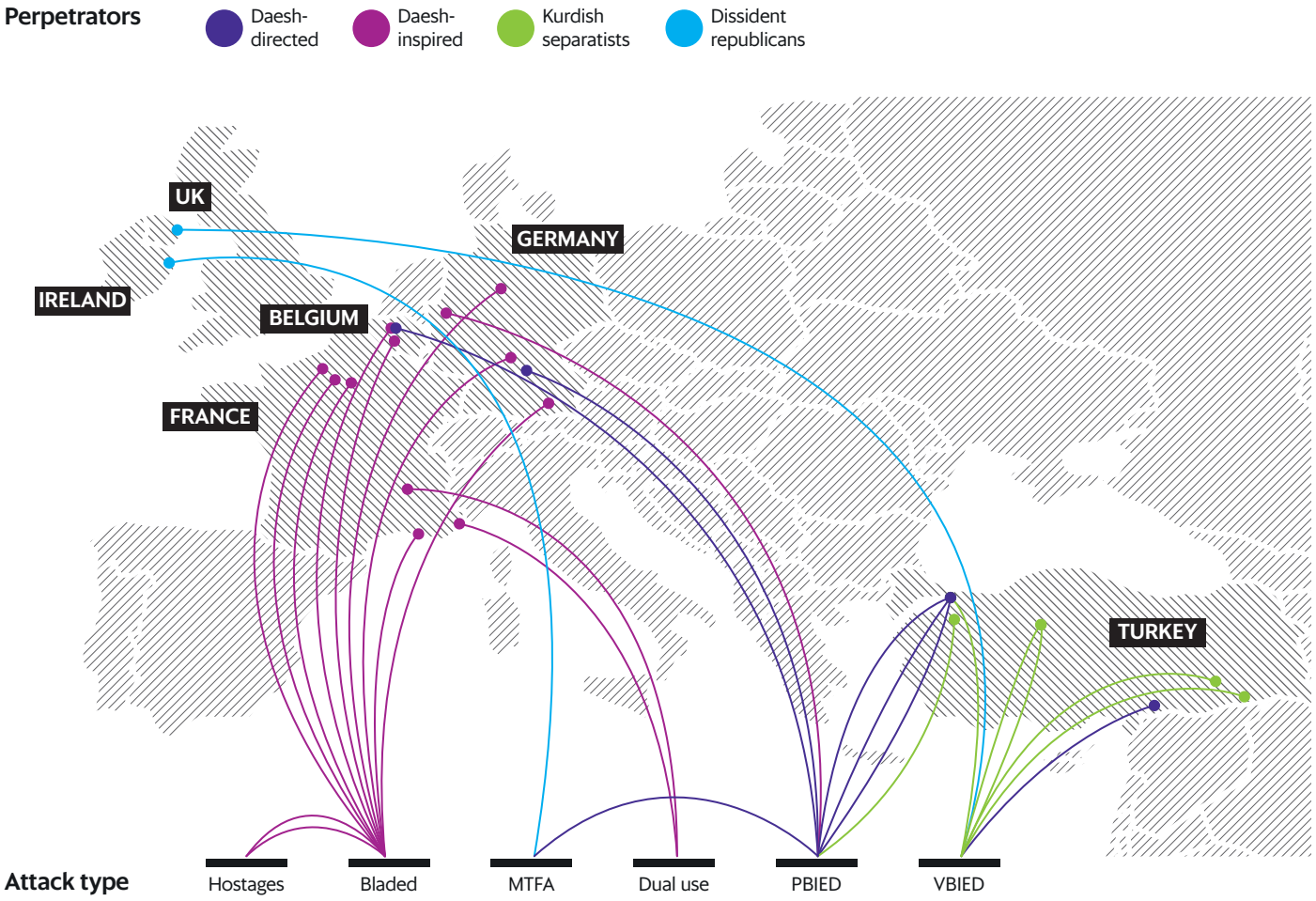
It is at this crucial juncture that state-backed pools can play a vital role: protecting the market from unmanageable risk and enabling commercial risk carriers to innovate and develop new risk products. Alongside this, reinsurance pools should continue to consider how they might evolve with the aim of further removing the taxpayer as the primary insurer of last resort, to the greatest extent possible, and also creating greater resilience in the UK economy.

Collaborating internationally allows us to see how that is happening in other countries. For example, in France, as a result of mass casualties that have put French funds designed to compensate innocent victims of crime under pressure, the pool is being asked to design a reinsurance solution to take the peril away from government. ●

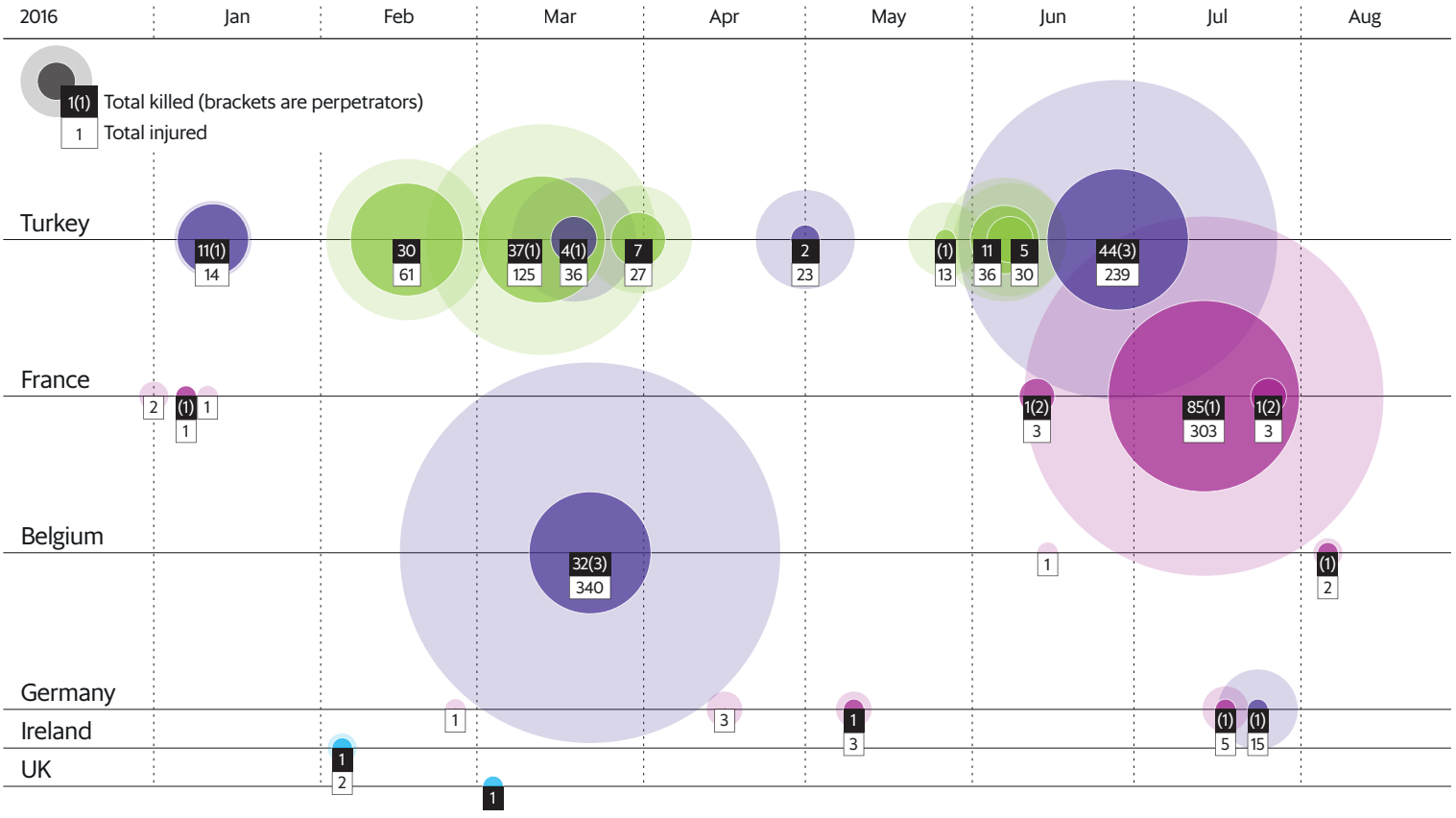
Quarterly Threat Report

Terrorism: Europe and United Kingdom

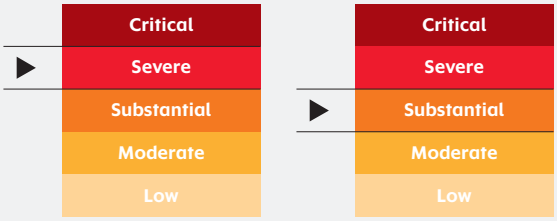
Key terrorism incidents, Europe 2016



Frequency and Impact



UK threat summary



Threat level from international terrorism to the UK

Threat level from Northern Ireland-related terrorism to the UK

Attack type	Bladed	Dual-use	MTFA	PBIED	VBIED	LVBIED	CBRN
Target type	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI

Threat level

The MI5 threat level from international terrorism to the UK is SEVERE (raised from SUBSTANTIAL, August 2014). The threat from Northern Ireland-related terrorism to the UK mainland is SUBSTANTIAL (from MODERATE, May 2016).

Key actors

Jihadi terrorist groups remain the principal threat to the UK mainland. **Daesh** and **al-Qaeda** (AQ) affiliates represent the key threat actors, both with the capability to inspire and direct attacks at varying levels of complexity against UK targets. Recent attacks across Europe demonstrate that both groups have effectively exploited the virtual domain to inspire individuals to acts of violence, in the case of Nice, and employ open-source encrypted messaging services (primarily Telegram Messenger) to actively direct more complex attacks (Charlie Hebdo, Paris and Brussels). This recent development has significantly impaired the intelligence services' ability to track and interdict suspects and increases the threat of attack to the UK.

Dissident republican groups – the **Continuity IRA** (CIRA), the **New IRA** and the **Óglaigh na hÉireann** (ONH) – remain active both north and south of the border and still hold significant quantities of weapons and explosives. These groups operate mainly on the criminal fringes of Northern Ireland's society, controlling cross-border smuggling routes and low-level crime. However, in the past 18 months, the Police Service of Northern Ireland (PSNI) and the security services have warned of a growing range of capabilities. These include improvised explosive devices (IEDs), improvised rocket launchers, increased volumes of small arms (AK variants and munitions) and under-vehicle bombs. The recent change to the threat level from MODERATE to SUBSTANTIAL is related to the groups' intent to target high-profile individuals (military, police, government and business leaders) over traditional property-based targets.

Arrests and enforcement

The intelligence services estimate that in the region of 850 UK nationals are fighting in Iraq and Syria alongside jihadi groups, principally Daesh. It is thought that half of these foreign fighters have returned to the UK. The security services have stopped in the region of 900 suspects leaving the UK to join jihadi groups in the Middle East and North Africa. Reports, and subsequent verification with our sources, show there to be at least five active extremist plots on the UK mainland, with a current average arrest rate of one radical per day. Official Europol figures show that **103 attacks were foiled**, with **134 arrests**, across the UK in 2015.

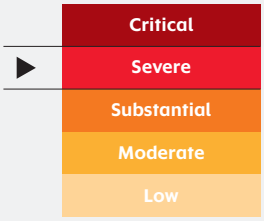
Assessment

Daesh and AQ will continue to direct and inspire attacks across Europe. The UK remains at severe risk of an attack.

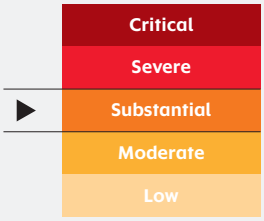
Most likely scenario	Most dangerous scenario	Emerging scenario
Prosecute an attack using simple, low-tech methods – bladed attack against a crowded place or employing a dual-use weapon (Nice).	MTFA, combined with PBIEDs, against crowded places or transport hubs, resulting in mass casualties (Paris/Brussels).	Daesh has developed a significant chemical weapons capability in Syria and Iraq. Reports also indicate that the group has been conducting research into the use of radiological dispersion devices (RDDs, or 'dirty bombs') in Mosul, Iraq[2]. As more fighters return home, there is a growing risk of a technology transfer from current attack methods in the Middle East to future attack methods in the UK.

2. See Pool Re's 'Emerging Risk Report: CBRN', June 2016

UK threat summary



Threat level from international terrorism to the UK



Threat level from Northern Ireland-related terrorism to the UK

Assessment Dissident republican groups pose a secondary threat to the UK mainland

Most likely scenario	Most dangerous scenario	Emerging scenario
Targeted assassinations of high-profile individuals over property.	Employing legacy explosives to conduct a VBIED/LVBIED against government/institutional targets.	No change.

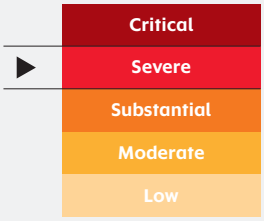
Implications for business

The trend, currently being witnessed in Europe, is an increase of attacks on people, with minimal damage to property. At the target site there is a greater risk of non-damage business interruption. Across a wider geographical space, loss of attraction, particularly in the leisure and tourism sector, and a risk of a reduction in inward foreign investment, all present a threat to the private sector.

Businesses and corporations are also facing increased pressure on resources to enhance the security of their employees, particularly when working abroad, as well as responding to traditional property-based threats. An important mitigation measure for the indiscriminate nature of today's terrorism threat is timely and detailed threat assessments to better inform the private sector of the changing landscape. Given the variety of information and intelligence requirements of the private sector, tailored reporting for specific sectors would enhance the impact of this information. Information, relevant to a large multinational corporation whose premises are likely to be well-protected and present a 'hard target' for threat actors, will be significantly different to the information requirements and mitigation measures of the SME sector, which presents a highly vulnerable target for terrorist groups. It is assessed that a threat-based information service would significantly enhance security within the private sector and enable corporate security officers to allocate resources effectively and justify the required preventative measures.

Europe threat summary

We note that there is no corresponding Europe-wide threat level. European and global threat levels are an adaptation from the UK security services threat ratings and based on current intelligence assessments. Their purpose is to serve as a guide to the threat in the relevant geographical regions.



Threat level from international terrorism to Europe

Attack type	Bladed	Dual-use	MTFA	PBIED	VBIED	LVBIED	CBRN
Target type	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI	CP Symbolic Property CNI

Threat level

Europe is facing an unprecedented rise in the frequency of terrorism incidents and attacks in 2016. France, Germany and Belgium in particular are facing SEVERE threat levels from international terrorism; Italy and Denmark have also been named in Daesh propaganda as targets. Twelve major European countries[3] are active members of the US-led coalition in Iraq and Syria and are therefore subject to targeting by Daesh and AQ operatives and affiliates.

Key actors

Daesh and **AQ** 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 platforms and encrypted messaging services. Both groups have the capability to direct and support attacks across continental Europe.

Arrests and enforcement

Reports indicate that French authorities are operating from a reactive capability, having detained the majority of known suspects; a state of emergency is set to remain in effect. Germany is considering deploying military assets across the country. Belgium's security and intelligence services remain on high alert but are severely overstretched and lack the experience of dealing with a sustained counter-terrorism campaign. To date, there have been **127 deaths** and **670 injuries from terrorist attacks** across Europe in 2016. Current EU arrest figures for Europe are not in the public domain, however the US Homeland Security Committee reports there to have been 46 Daesh-linked plots in Europe this year. In **2015**, Europol figures show that the **EU suffered 211 failed, foiled or completed attacks**, almost half of them (103) in the UK. There were 151 fatalities: 148 in France, two in Denmark and one in Greece. These figures are markedly higher than those of 2014, when four people were killed and six wounded. Nearly two-thirds of the arrestees (63 per cent) were EU citizens. The majority were born in the EU (58 per cent), demonstrating the effectiveness of Daesh's propaganda campaign to inspire domestic extremism.

Assessment

Attacks in 2016 have followed the previous year's trend of a combination of complex, well-resourced attacks, with direct operational support from Daesh's senior Iraq and Syria-based leadership (eg, Brussels), as well as low-skilled, inspired attacks employing dual-use weapons such as vehicles (Nice). Daesh's stated aims for their European campaign is to co-ordinate simultaneous attacks across the continent.

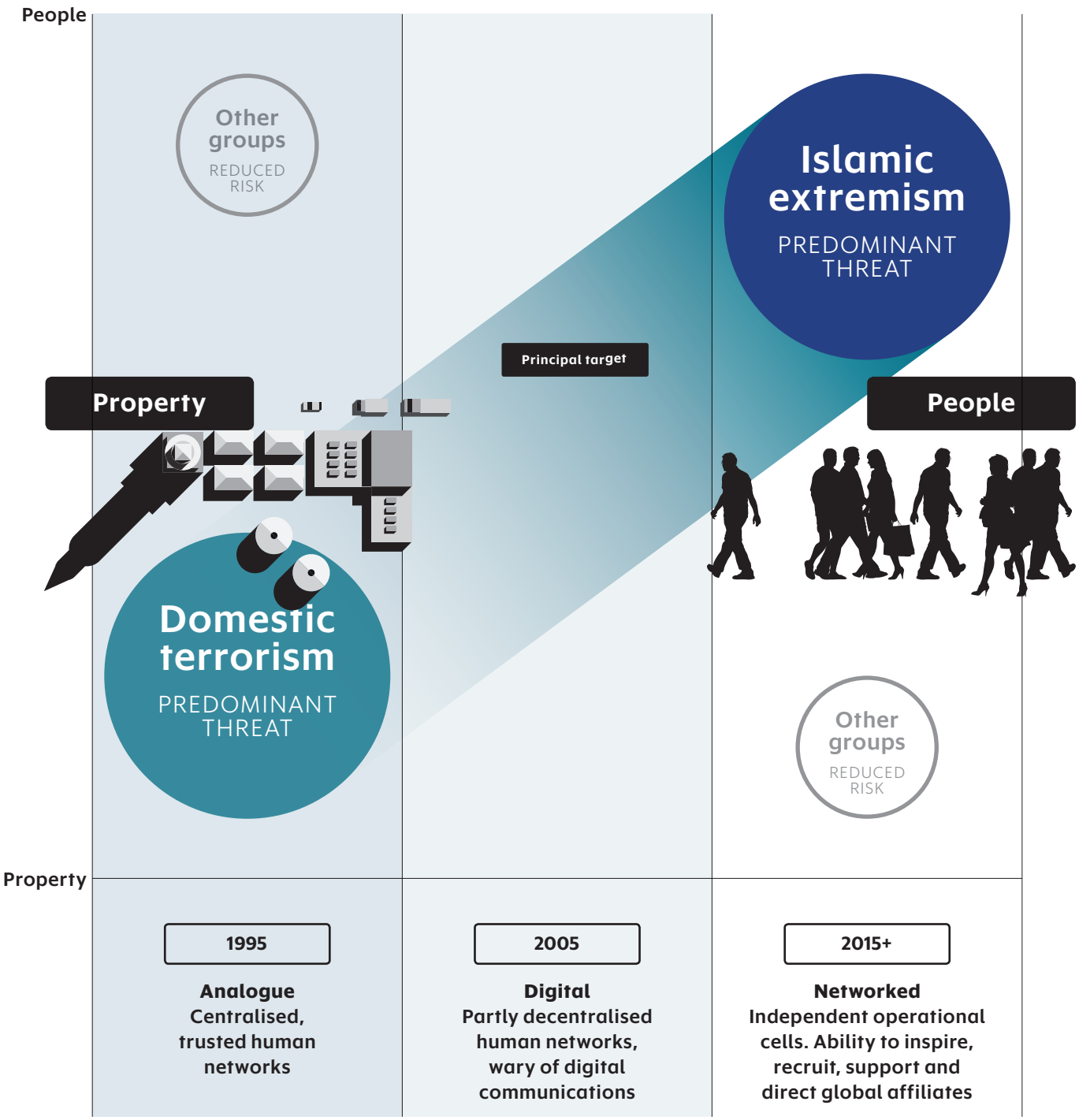
Most likely scenario	Most dangerous scenario	Emerging scenario
Bladed and dual-use attack methods are likely to continue at high frequency across Europe, targeting crowded places.	A combined PBIED and MTFA attack resulting in mass casualties occurring simultaneously across multiple target sites.	As stated in the UK threat summary, unconventional uses chemical agents and radiological isotopes represent an emerging threat to Europe.

Implications for business

Attacks against people over property has increased the risk of non-damage business interruption. Loss of attraction is already affecting tourism in Europe, particularly the French Riviera. The data collection agency YouGov estimated that 10 per cent of US travellers cancelled a trip to Europe after the Paris and Brussels attacks. This represents a loss of $8.2 billion in potential travel spending. Additionally, the University of Cambridge's Centre for Risk Studies estimated that the economic costs of the Paris attacks to be in the region of $9 billion to $12 billion. The French Ministry for the Economy and Finance has also reported a 5.8 per cent fall in air passenger traffic compared with the same period a year earlier. Hotel reservations in the Riviera region have also dropped as much as 30 per cent. Tourism is a key part of the French economy, accounting for 7 per cent of output and employing more than 2 million people.

3. Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Portugal, Spain, Sweden and the UK all contribute military assets to the coalition

Changing terrorist threat



Domestic terrorism	
Method of attack	**LVBIED**
Intent	**Economic disruption (discriminate targeting)**
Risk transfer needs	**Property damage and business interruption**

Islamic extremism	
Method of attack	**PBIED/ VBIED/ CBRN/ Cyber**
Intent	**Mass casualties (indiscriminate targeting)**
Risk transfer needs	**Property damage, business interruption, non-property damage business interruption, cyber, impacts on people and damage to brand and reputation**

European threat trajectory

Europe has suffered from a combination of 'directed' and 'inspired' attacks in 2016. The two most significant attacks this year (Brussels and Nice) demonstrate the cost to human life that both a directed and inspired attack can have.

Although investigations are still ongoing, it appears that Mohamed Lahouaiej-Bouhlel, the perpetrator of the Nice attacks, did not receive any significant help from Daesh central command in Iraq and Syria, or any other extremist group. Undoubtedly, he confided aspects of his intentions to others; someone about to engage in mass murder can act alone but is unlikely to do so in total isolation. It also appears that he was radicalised in a relatively short space of time through Daesh's highly effective propaganda campaign. By contrast, the principal actors in the Brussels attacks operated from a series of well-established terrorist networks, with connections to militant groups in Syria stretching back to the beginnings of the conflict.

The forensic details of these two major attacks in 2016 are significant, and do provide valuable lessons to the intelligence and security services for the future. However, beyond the who and the how, these two attacks demonstrate the worrying trends of contemporary terrorism: the effective co-ordination of inspired, simple, high-frequency terrorism with directed attacks, of greater complexity, both of which have the indiscriminate destruction of life over property as their aim.

Daesh and other militant groups have deep-rooted connections to the West, particularly Europe's francophone countries, who have large North African populations with both linguistic and cultural ties to the current conflicts in the Middle East and North Africa (MENA)[4]. It is through these established networks that complex attacks, such as Paris and Brussels, can be affected. Juxtaposed to this 'conventional' aspect of terrorism – ie, the cultivation of clandestine human-source networks to conduct relatively complex attacks – is the contemporary phenomenon of a terrorist communications campaign.

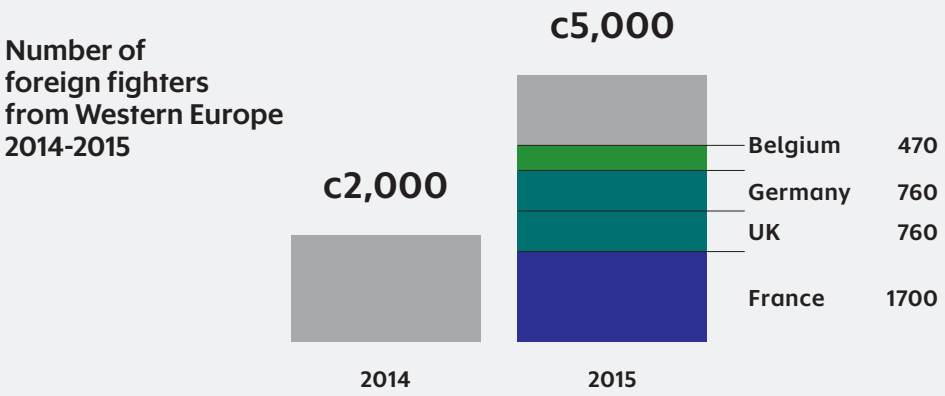
Daesh is the first terrorist group to effectively harness modern digital communications to their ends[5]. This is one of the most significant developments in terrorism during the past five years, enabling the group to propagate its message and inspire individuals to acts of violence with little or no operational support. 'Terrorism in our name' but not by our deed has become a key feature of 2016 for Daesh.

This combination of the conventional (directed attacks) and unconventional (inspired attacks) has caused a spike in the number of terrorist incidents against the West. The fusion of complex, directed attacks with unsophisticated, high-frequency, inspired attacks has caused a highly damaging aggregation of the effects of terrorism. This has had the following consequences in 2016: ►

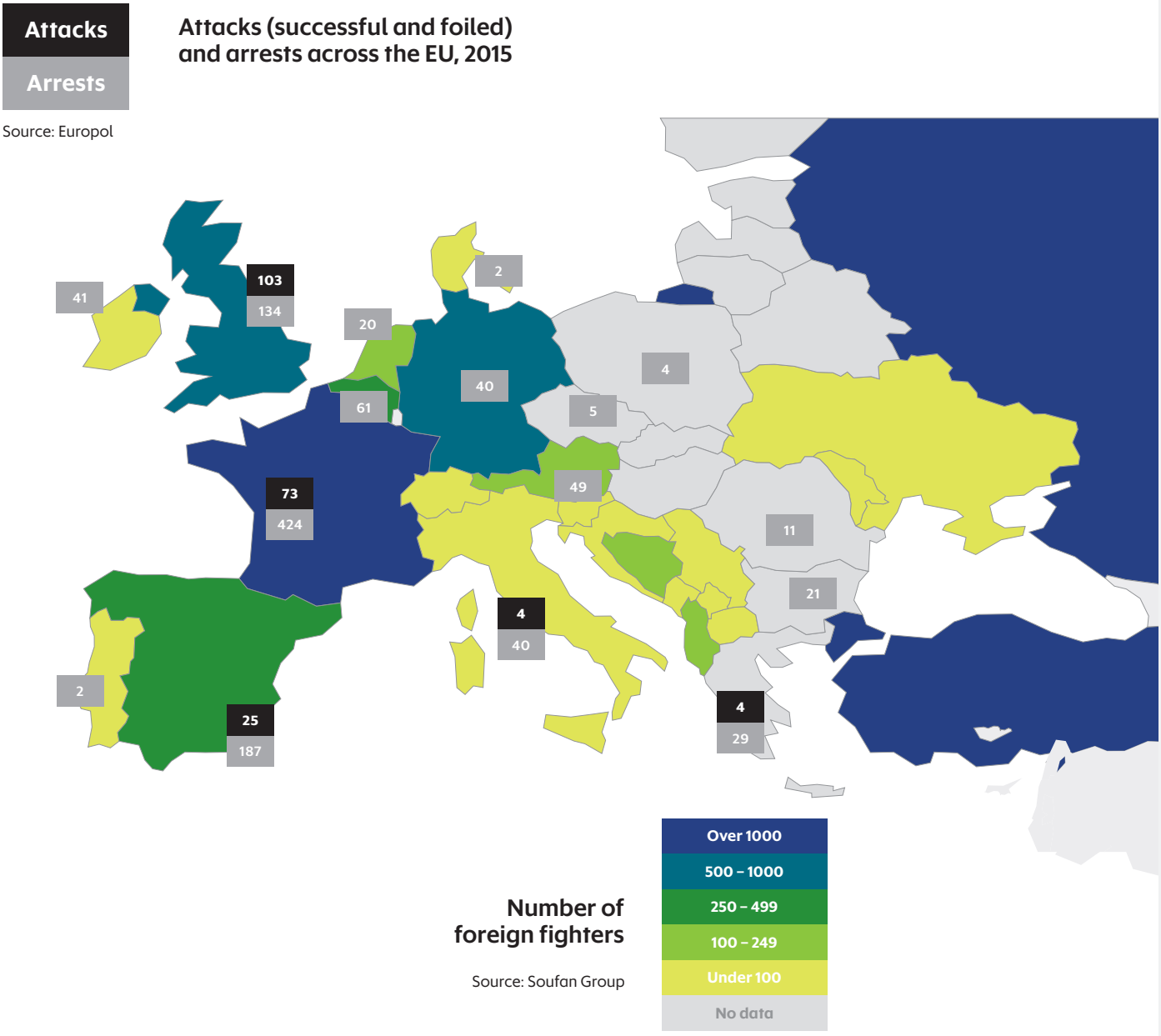
4. The situation has parallels with the 1990s and early 2000s in Britain. The flow of a number of nationals to the Afghan conflict and Federally Administered Tribal Areas of Pakistan was largely due to a number of key radical preachers embedded within the British Asian community, as well as the clear linguistic and cultural ties to the region. Such connections to the Middle East and North Africa are less prevalent among the UK's Muslim community but clearly a powerful recruitment tool that Daesh and other groups have exploited in France and Belgium.

5. The exception to this was the forefather of Daesh, al-Qaeda in Iraq, led by Abu Musab al-Zarqawi, killed by a US airstrike in 2006. General Stanley McChrystal, commander of the Joint Special Operations Command in Iraq during the early 2000s, commented on the challenges of degrading such an organisation that exploited modern digital communications to direct operations: each cell was a self-sustaining operational entity, operating a reach independently from any form of central command.

European threat data



Source: Soufan Group



European threat trajectory

Key consequences

Security and intelligence services appear unable to control and predict actors or targets.

A perceived lack of security causes rifts within Western societies, seen by a marked increase in targeted hate crimes across Europe and the West.

The consequential effects of routinely successful terrorist incidents has a severe effect on business. At the target site, this takes the form of non-damage business interruption, given the low damage to property of recent attacks in the West. Across a wider geographical space, loss of attraction, particularly in the leisure and tourism sector, and a risk of a reduction to inward foreign investment are all impacting Western economies.

The outlook for the near future in Europe is bleak from a security perspective. Daesh's territory in Iraq and Syria is the priority at present for the group's leadership, many of whom are disgruntled Iraqi Sunni military and intelligence officials from Saddam's regime. The group's senior leadership is far more interested in establishing a Sunni powerbase to challenge the Shia-dominated government in Baghdad than the creation of a 'global caliphate', in spite of its propaganda. The reality is that the group is unlikely to maintain this territorial control during the next 18-24 months. From the West they face the Syrian army, no doubt weary from an almost five-and-a-half-year civil conflict but backed by Russian airpower and significant assistance from Iran. In addition, the regime has Hezbollah, a highly effective military force in its own right. From the north-east the Kurds, backed by US-led airpower and special forces, are advancing on Mosul, while the less effective Iraqi army approaches from the south-east, aligned with a dubious affiliation of Shia militias from mainly southern Iraq. The ensuing ground conflict is likely to be extremely costly, particularly in Mosul, roughly equivalent in size to Birmingham. However, the future loss of its operational heartland is likely to increase Daesh's efforts in international terrorism and release significant resources currently employed in fighting the ground conflict in Iraq and Syria.

One of Daesh's key recruitment tools is its so-called caliphate. For elements of the MENA diaspora in Europe the idea of redrawing the colonial borders, created at the end of the First World War by France and Britain, has great appeal. When this is coupled with the promise of legal equality before transcendental laws, in a region that has suffered misrule from mainly secular military regimes, backed by the West or Russia during the twentieth century, one can begin to understand why an estimated 32,000 foreign fighters flocked to the group by mid-2014[6]. Clearly the reality doesn't match the promise; the message, nonetheless, is powerful.

The current existential threat to the caliphate has caused the group to use international terrorism to bolster its global image. The high rate of attacks in Europe helps Daesh claim that, whatever the situation on the ground in Syria and Iraq, its ability to project force globally is unhindered. The next six months in Europe are likely to proceed in a similar manner to the past: higher levels of inspired attacks, using simple dual-use weapons, combined with planned and resourced attacks of greater complexity. Daesh's most recent stated aim in relation to international terrorism is to conduct simultaneous attacks across the continent. Its current geographic spread makes this anything but an idle threat. ●

6. US Homeland Security Committee & Combating Terrorism Centre, West Point (CTC)

Quarterly Threat Report

Global Terrorism

Global threat trajectory

Terrorist groups have suffered from an increase in military operations against their territorial strongholds in 2016.

While the rate of attacks by terrorist groups has increased significantly in Europe, their ability to hold and administer ground has suffered. The potential reduction in ungoverned spaces, which terrorist groups seek to exploit, is likely to further impact on Europe. The primary consequence is that global threat actors will focus their attentions on international terrorism. More sophisticated, higher-impact attacks will become a significant threat once the major terrorist organisations lose their safe havens, or are forced to relocate to less-permissive environments.

Daesh has also developed a significant chemical weapons capability in Iraq and Syria, having seen the damaging psychological impact that such weapons have on local opponents. Once its physical caliphate has gone, it is likely that their long-term strategy will be to use these new capabilities to prosecute attacks of mass effect.[7]

The short to medium-term trends are likely to be an intensification of the ground campaign in Iraq and Syria, as multiple sets of actors seek to drive Daesh from its territory. Western-backed operations in Libya have severely damaged Daesh's presence there. However, the country has plenty of other actors who could prove equally dangerous to Western interests. Additionally, the geographical nature of the country means that even if Daesh loses its principal seat in Sirte along the coast, the vast expanse of desert stretching down to Niger, Chad and Algeria, which often acts as a gateway to other terrorist groups' areas of operations in the Trans Sahel, means that Daesh will be likely to maintain some kind of presence in the country.

Daesh remains the group with the greatest ability to strike at Western targets and currently poses the greatest risk to UK domestic and foreign interests. Al-Qaeda in the Arabian Peninsula (AQAP) and al-Qaeda in the Islamic Maghreb (AQIM) also pose a severe threat to UK interests and generally focus on less frequent attacks with a higher destructive impact. ●

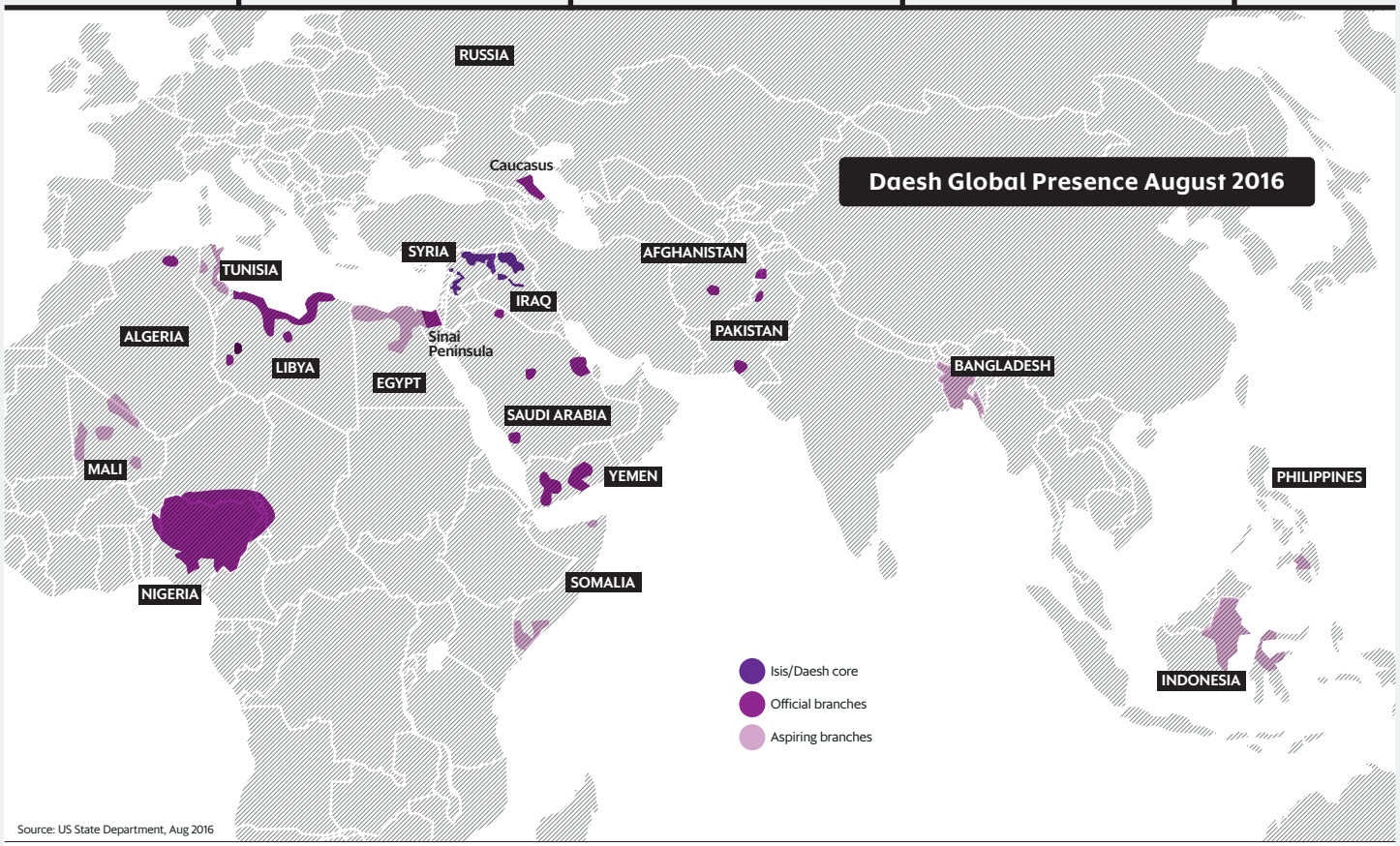
7. See Pool Re's 'Emerging Risk Report: CBRN', June 2016

Daesh global presence, August 2016

Threat in relation to the UK

Critical
Severe
Substantial
Moderate
Low

Threat actor	Area of operations	Capability	Recent activity	Threat level



Source: US State Department, Aug 2016

Daesh affiliates	Syria, Iraq, Sinai Peninsula, Saudi Arabia, Yemen, Somalia, Tunisia, Libya, Algeria, Nigeria, Mali, Chad, Cameroon, Bangladesh, Afghanistan, Pakistan, Philippines, Indonesia, Caucasus	Inspire and direct attacks against Western targets Territorial control in Iraq, Syria and Libya	Ongoing operations in Iraq, Syria and Libya Brussels bombings, March 2016. Nice attacks, July 2016. Bladed attack, Normandy, July 2016. Ansbach bombing, Germany, July 2016	Threat level Trend ▲
al-Qaeda in the Arabian Peninsula (AQAP)		Inspire and direct attacks in the West (key aspect of the group's current strategy) Territorial control, Yemen Access to heavy weaponry and sophisticated bomb-making material	Charlie Hebdo attacks Ongoing operations in Yemen's civil conflict	Threat level Trend ▲

al-Qaeda in the Islamic Maghreb (AQIM)

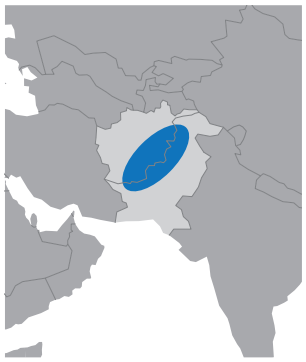
- Conduct and direct attacks in West and North Africa
- Inspire and direct attacks in Europe
- Territorial safe haven in Trans Sahel region
- Focused on Western targets within North and West Africa

- Radisson Blu hotel, Bamako, Mali, November 2015
- The Cappuccino restaurant and the Splendid Hotel, Ouagadougou, Burkina Faso, January 2016
- Attack on the beach resort in Grand-Bassam, Ivory Coast, March 2016

Threat level

Trend

Al-Qaeda in the Indian subcontinent



- Operationally focused on Pakistani and Afghan military
- Regularly conducts targeted assassinations in Bangladesh
- Access to heavy weaponry and explosives
- Strong connections to Europe through the Pakistani diaspora

- Multiple attacks against Pakistani and Afghan military
- The murder of a Pakistani scholar and three journalists, accused of blasphemy
- Ongoing operations with the Taliban in Afghanistan

Threat level

Trend

Ansar Bayt al-Maqdis

(Daesh affiliate)

- Coming under increasing pressure from the Egyptian military
- Able to conduct operations outside Sinai Peninsula (Cairo)

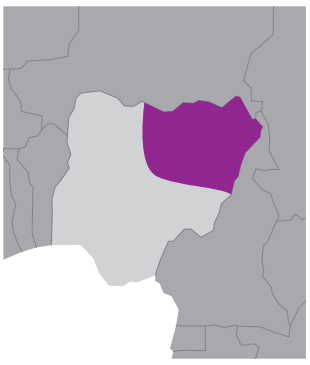
- Downing the Russian passenger jet departing Sharm el-Skeikh, October 2015

Threat level

Trend

Boko Haram

(Daesh affiliate)



- Conduct and direct attacks in West Africa

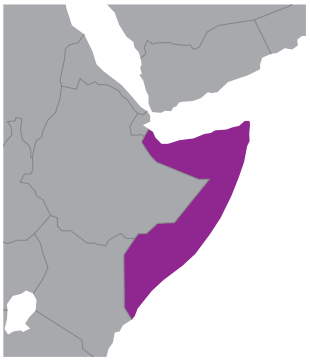
- Ongoing operations against regional forces (Nigeria, Niger, Cameroon & Chad)
- April 2014, Chibok schoolgirls kidnapping

Threat level

Trend

Al-Shabaab

fractured Daesh-al-Qaeda affiliation



- Conduct and direct attacks in the Horn of Africa and Arabian Peninsula
- Inspire and direct attacks in Europe
- Strong links to Europe (particularly UK) through Somali diaspora

- Garissa University, Kenya, April 2015
- Ongoing operations internal to the Somalian civil conflict

Threat level

Trend

Daesh

Smoke billows from the Daesh bastion, Fallujah, on 14 June 2016, during the Iraqi forces' ongoing battle to retake the city (Getty)

Size

In 2014 the CIA estimated Daesh's forces in Iraq and Syria to be in the region of 30,000. The Pentagon's figures for 2016 put the group's strength at 15,000. We note that these figures are difficult to verify owing to the nature of the conflict – even official figures need to be treated as a guide. US military data shows that airstrikes have killed in the region of 20,000 Daesh fighters by the end of 2015. After the Paris attacks, military operations were increased and, in December 2015 alone, it is estimated that coalition airstrikes killed some 2,500 fighters.

Loss of territory

Analysts estimate that, in 2015, Daesh's territory in Iraq and Syria contracted by 12,800 km² to 78,000 km², representing a loss of 14 per cent.[8] In the first six months of 2016, this territory shrunk again by 12 per cent. As of 4 July 2016, Daesh controls roughly 68,300 km² in Iraq and Syria, broadly equivalent in size to the Republic of Ireland.[9] However, much of this territory represents uninhabited areas. The group is now beginning to lose urban centres in eastern Syria and western Iraq. Palmyra in Syria and Fallujah and Ramadi in Iraq represent key losses in 2016. The group has also lost important border crossings on the Syria-Turkey border, the most recent of which was Manbij, where US-backed elements of the Syria Democratic Forces (SDF) recaptured the town in August 2016. A good metric to asses Daesh's control of territory is through the civilian population within the area. Current figures estimate there to be between 6 and 7 million people still residing within the group's territory, demonstrating its persistent hold on significant urban population centres. ▶

8. IHS Jane's Terrorism & Insurgency Centre

9. Ibid

Daesh

Foreign fighters

The number of foreign fighters travelling to join Daesh peaked in mid-2014 and was estimated to be between 27,000 and 31,000.[10] After the six-month siege of Kobani (September 2014-March 2015), the group suffered heavy casualties and was reported to have been tactically and strategically bankrupt in its use of manpower, particularly in relation to foreign fighters. More than 6,000 Daesh fighters were killed during the engagement and many more were severely injured. Since this event, numbers are reported to have dropped significantly. However, between June 2014 and the fourth quarter of 2015 the number of foreign fighters travelling from Western Europe more than doubled.[11] Additionally, 20-30 per cent of this group are thought to have returned to their home countries, representing a significant threat to security and intelligence services.[12]

Finances

In mid-2015, Daesh's total monthly revenue was in the region of $80 million. By March 2016, it had dropped to $56 million.[13] Estimates indicate that revenues have decreased by a further 35 per cent.[14] By early 2016 increased military action against Daesh reportedly forced the group to cut fighters' salaries by 50 per cent.[15] Military action has also forced oil production to drop by 30 per cent from 2014 to 2015. In 2015 Daesh generated approximately half of its revenue from oil and controls more than 80 per cent of Syria's extractive infrastructure.[16]

Although Daesh generates a significant portion of its revenue from oil, counting the Assad regime as one of its clients, other sources of funding include the smuggling of antiquities, kidnapping for ransom and taxation on the local population.

It should be noted that the loss in revenue will not necessarily impede the group's military capability in the short to medium term. Not only does it have significant cash reserves, but it has also captured large quantities of weapons and equipment from the Iraqi army, after its retreat from Mosul and western Iraq in 2014.

Recent developments

Inspired Daesh attacks in 2016 by country: Denmark, Bosnia & Herzegovina, United States, Canada, Algeria, Australia, Germany.

Directed Daesh attacks 2016 by country: France, Turkey, Libya, Lebanon, Egypt, Tunisia, Yemen, Afghanistan, Kuwait, Bangladesh, Indonesia, Belgium, Saudi Arabia.

Enhanced IED capability

The reported emergence of unconventional explosive munitions has risen to prominence across the international intelligence community after a Daesh IED attack in Karrada, Iraq on 3 July 2016 that killed 324 civilians. Industry experts have identified the employment of a fuel air explosion (FAE) IED (a napalm-based deflagrating munition) in the form of a more traditional vehicle-borne IED (VBIED) attack. Napalm remains a cheap, available and lethal material for Daesh to employ. This attack represents a potential direction change in the IED capabilities of Daesh. Industry experts claim these FAE IEDs are up to 16 times more destructive in terms of property and personnel than detonating-based IEDs. Additionally, they could be manufactured on a mass scale by Daesh as a natural progression beyond its 2015 efforts to employ improvised chemical weapons. ●

10. Foreign Fighters in Syria and Iraq, the Soufan Group, December 2015

11. Ibid

12. Ibid

13. Ibid

14. Ibid

15. 'Air strikes help force ISIS to halve fighters' pay: Glaser', Reuters, 8 February 2016

16. US Homeland Security Committee

Daesh and al-Qaeda (AQ) • Key differences

AQ relies on trusted networks of operatives to plan complex, low-frequency, high-impact attacks on high-value targets.

The 2013 In Amenas hostage crisis in Algeria, carried out by al-Qaeda in the Islamic Maghreb (AQIM), provides a good example of what AQ operatives aspire to.

AQ does not have the same digital presence as Daesh and therefore has a lower profile among Western-based radicals. Its recruitment process is also assessed to be more rigorous than Daesh's. AQ is reported to select and screen applicants thoroughly and rely on known human-source networks for recruitment. Daesh, by contrast, has made general calls for fighters and civilians to become 'citizens' of its so-called caliphate.

Daesh has developed new forms of terrorism. It is the first group to administer territory and effectively advertise this fact through digital propaganda. AQ has a territorial presence in Syria, Yemen, the Horn of Africa, the Trans Sahel and the Federally Administered Tribal Areas, located on the Afghanistan-Pakistan border. However, it operates in these locations at the behest of local power-brokers; Daesh, by contrast, is the local power-broker in its principal territories.

Outside the conflict in Iraq and Syria, Daesh encourages the use of a small number of attackers with low-tech attack methods, the exception being when it actively directs more complex attacks (Paris and Brussels). It has increased the focus on human casualties over property damage and pioneered the deployment of dual-use weapons (trucks, cars, knives, locally sourced improvised explosives). It also operates from a highly autonomous operational structure, employing encrypted messaging services to support and direct operations. ●

Quarterly Threat Report

Emerging Risks CBRN and Cyber

CBRN

Context

Pool Re's Terrorism Research and Analysis Centre recently conducted a detailed assessment of Daesh's, and other threat actors', chemical, biological, radiological and nuclear capabilities (CBRN)[17]. The findings indicate that asymmetric uses of chemical and radiological devices present the greatest threat to the UK within the CBRN threat spectrum. Given the increased use of chemical weapons in Iraq and Syria, the barriers to acquisition, production, weaponisation and delivery are lower than other CBRN attack methods. In line with this, the conditions surrounding these barriers are significantly different within Europe for chemical and to a large extent radiological devices due to the dual uses these materials have – chemicals, suitable for weaponisation, can be found in a commercial setting, as can radiological isotopes. This is not the case for biological[18] or nuclear weapons.

Potential consequences

It should be stressed that conventional CBRN weapon systems represent highly advanced capability. Current intelligence assessments conclude that Daesh's aspirations exceed their ability to unleash a chemical or radiological device against a Western target, but they are investing significant resources into enhancing this capability. In spite of the many technological barriers, it is usually the psychological impact of these weapon systems that has the potential to cause widespread panic and significant economic losses, irrespective of the success of an attack. Recent examples of CBRN incidents demonstrate the potential interruption to business and losses that (re)insurers could face. ▶

17. See Pool Re's 'Emerging Risk Report: The Threat of Asymmetric Attack Methods', June 2016

18. Although deadly biological pathogens and toxins are used in medical research, the quantities available, complex storage requirements and number of institutions holding them are severely limited. By contrast, certain chemical and radioactive isotopes have almost everyday applications. See Pool Re's Emerging Risk Report: 'The Threat of Asymmetric Attack Methods', June 2016, for a more detailed breakdown of this aspect of the threat posed by CBRN devices.

US anthrax attacks

Following 9/11, anonymous letters containing dried anthrax spores were sent to US senators and several media offices.

In spite of minimal casualty numbers – **5 deaths** and **17 non-fatal injuries** – and damage to property, the clean-up operation, and other associated costs, was estimated by the FBI to exceed **$1 billion**.

In terms of business interruption, the Brentwood postal facility was closed for **26 months** and cost **$130 million** to decontaminate.

The New Jersey postal facility was closed until March 2005 and cost **$65 million**.

The US Environmental Protection Agency spent **$41.7 million** on the decontamination of a number of government buildings in Washington D.C.

GETTY

CBRN

Mitigation

The UK has robust detection procedures for illegally trafficked radiological isotopes in place at many points of entry; protection is further enhanced by the UK's fleet of mobile detection units. This is run under a joint UK Border Force and Home Office initiative entitled Programme Cyclamen. These preventative measures provide a robust defence to the UK against a radiological device. However, as the targeted assassination of Alexander Litvinenko with a small amount of polonium-210 at a Mayfair hotel in 2006 suggests, small-scale radiological attacks are possible (although it should be noted that Programme Cyclamen did not become fully operational until 2009, and the government continues to improve and invest in these capabilities). In spite of only one fatality, 10 buildings, two cars and four planes were contaminated. The Millennium Hotel suffered 12 days of business interruption, with some areas said to have been off-limits for up to five years. Additionally, the total clean-up cost exceeded £4.4 million.

In addition to the trafficking of material, sourcing of radiological isotopes, chemicals and even biological pathogens or toxins has also prompted research into replacement technologies. This has particular application to the radiological sources that can be found in hospitals and certain extractive industries. The table below identifies potential sources of radiological isotopes – all of which would be applicable for an RDD. ▶

Examples of radiological isotopes and their common use

Radionuclide and emission	Half-life	Chemical form (typical)	Typical use and activity	Common radiation uses	Typical setting
Cobalt-60	5.3 yrs	Hard metal	Teletherapy (1,000s Ci)	Used to treat cancer tumours	Hospitals/medical research facilities
Caesium-137	30.1 yrs	Salt powder	Irradiators (1,000s Ci)	Used to irradiate blood before transfusion	Hospitals/medical research facilities
Iridium-192	74 days	Hard metal	Radiography (~100 Ci)	Used to determine the quality of a particular material and detect areas of varying density and composition	Extractive industries/ academic research facilities
Americium-124/ Beryllium	432 yrs	Mixture of oxide/metal	Well logging (~10Ci)	Radiation is used to measure properties of the geologic strata through which a well has been or is being drilled to examine earth formations	Extractive industries

Source: Nuclear Threat Initiative

CBRN

Daesh's use of chemical devices

October 2015
Mustard gas attack on Marea, near Aleppo, using 122mm artillery shells, reported to have been part of the Syrian regime's missing stockpiles

11 February 2016
Chlorine gas used against Peshmerga forces in Sinjar, Iraq

8 March 2016
The town of Taza in northern Iraq, was attacked with a **blister agent**, killing three children and wounding more than 3,000

5 April 2016
Syrian forces reported that the contested government-controlled airbase in Deir al-Zour was attacked with rockets armed with **mustard** agent

April and May 2016
Mustard and **chlorine** gas attacks against Peshmerga forces near Makhmour and Gwer, located close to the Daesh-controlled city of Mosul

2 May 2016
Mustard agent used against the Iraqi village of Bashir, near Kirkuk

Appropriate sources of biological pathogens or toxins do exist in medical research facilities. However, biological attack methods tend to require higher levels of technical expertise and the incubation period for most biological weapons represents a disadvantage for threat actors seeking propaganda from the deed, as such agents are not generally fast acting and lack the immediate effects of an explosive-based device. The risk of theft has increased with the rise in medical research facilities with the authority to carry lethal biological agents.[19] Additionally, as the US anthrax attacks demonstrate, large costs can be incurred from even a partially successful CBRN incident, owing to the lengthy decontamination processes required and the psychological effects on the wider population. Business interruption and loss of attraction therefore represent the most likely consequences for (re)insurers.

This, of course, does not apply to situations in which the attack method is full-scaled, given the mass effect these weapon systems have in their conventional forms. However, the complexity of weaponisation needed to achieve the full effect of these weapons generally means that unconventional uses by terrorist groups are likely to result in a partial effect. A damage to public order and decontamination issues are therefore the most likely areas of concern for (re)insurers. The recent attack on the Iraqi village of Taza illustrates the point: in spite of minimal casualties (three fatalities) compared with losses suffered in conventional operations, Hussein Abbas, the local mayor, reported that 25,000 people left the surrounding area in fear of another attack. ●

19. See Pool Re's 'Emerging Risk Report: The Threat of Asymmetric Attack Methods', June 2016, for further details

Cyber

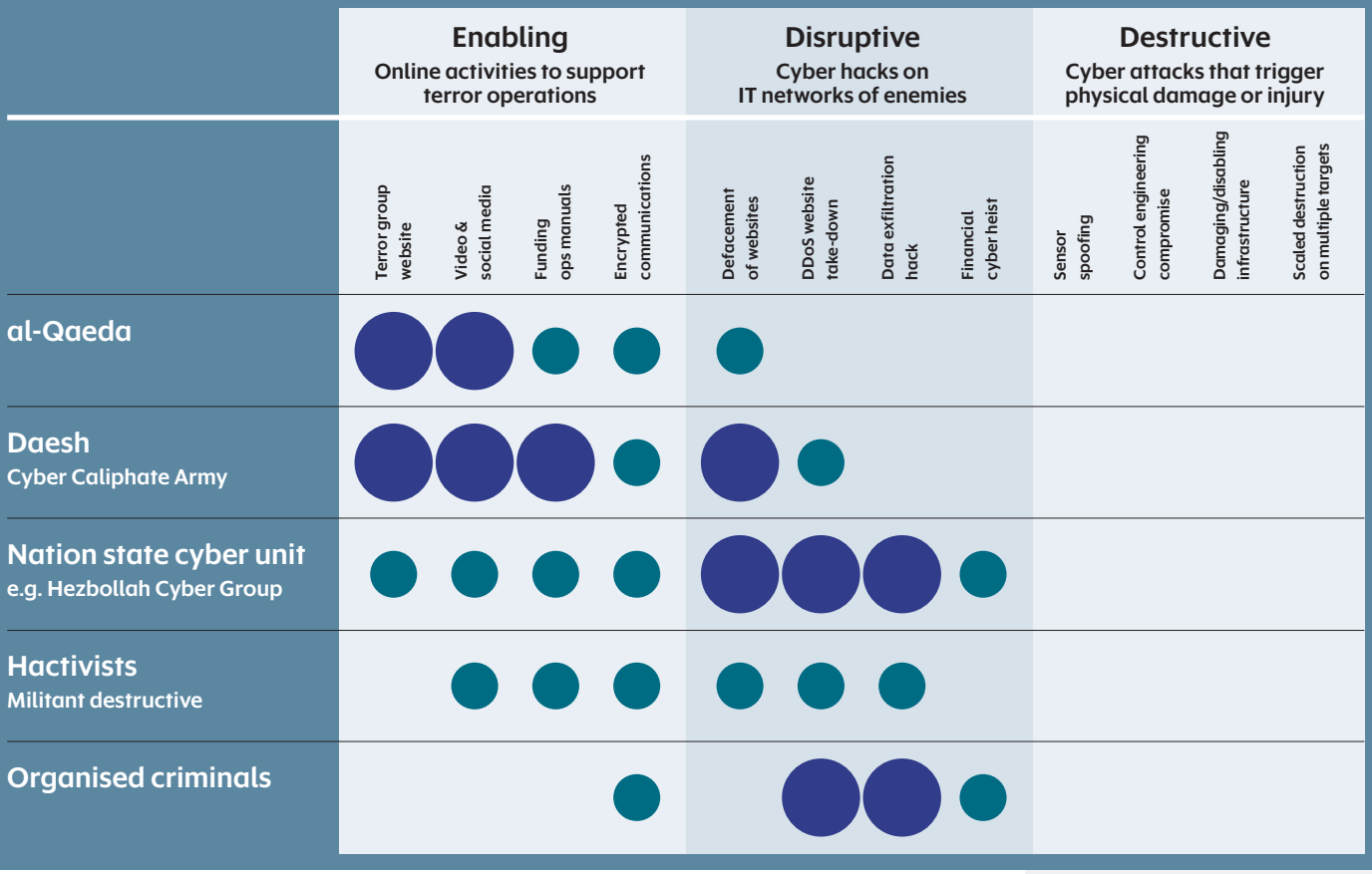
Pool Re has recently commissioned research by the Centre for Risk Studies at the University of Cambridge on the likelihood and potential impact of destructive cyber attacks, committed by terrorist groups. The cyber capability of terrorist groups is broken down into three categories:

Enabling Online activities that support the operations of terrorist groups, such as publicity and propaganda, fund-raising, 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 hacking activities.

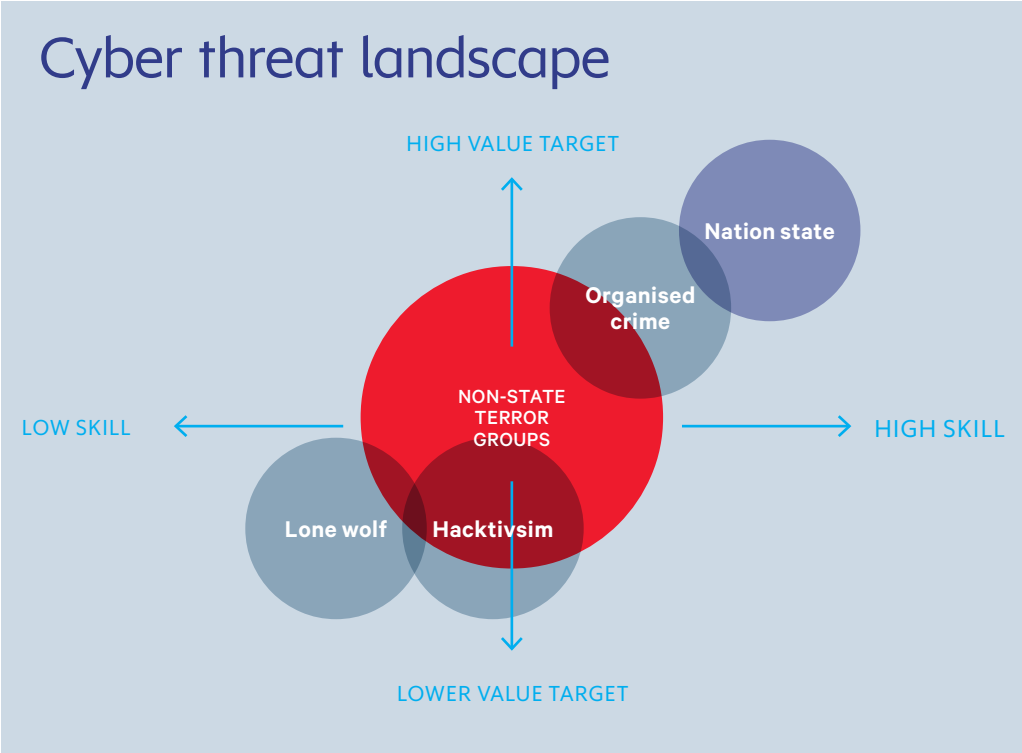
Destructive Cyber attacks that trigger physical damage or injury through spoofing operation technology (OT) and digital control systems, attacks on Supervisory Control and Data Acquisition (SCADA) systems, disabling control and safety systems. ▶

Evidence of cyber capability



Source: Centre for Risk Studies, Univ of Cambridge

Cyber



It is thought that only nation-state cyber teams currently possess the capability to commit destructive cyber attacks. The most recent assessment from the ongoing research suggests that terrorist groups would be unlikely to develop a destructive capability within the next five years. However, as stated earlier in this report, as terrorist groups begin to lose ground in their principal areas of operations it is likely that they will focus on developing more advanced attack methods. Destruction to property and lives through remote interference with digital operating systems clearly represents an attractive attack method to terrorist groups. Regardless of the technical barriers, it is a pathway that they have already begun to effectively exploit through their current cyber-enabling capability, the effects of which we are already witnessing across Europe in the form of inspired attacks.

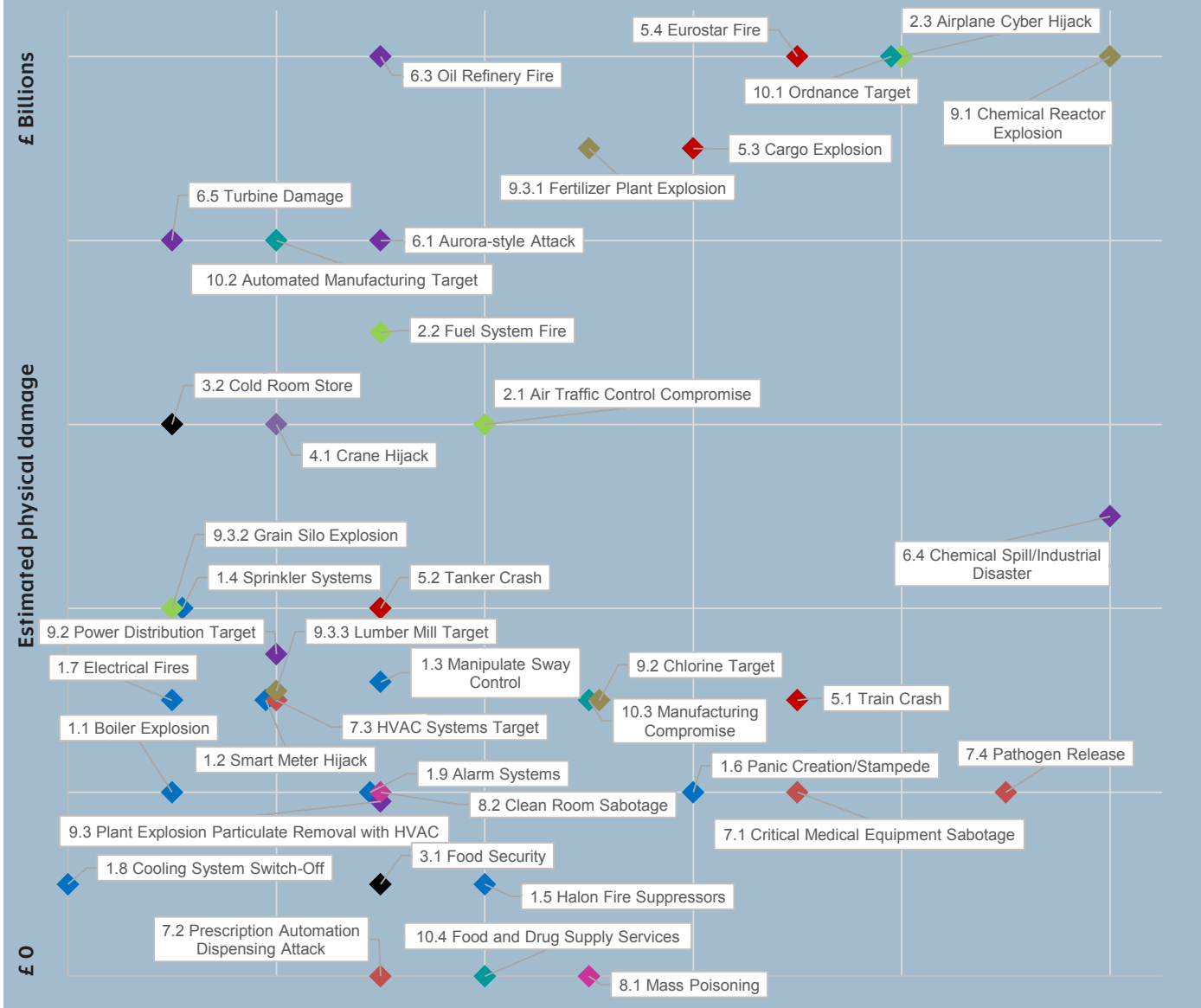
Potential impact of destructive cyber attacks

The research conducted by the Centre for Risk Studies has identified a number of scenarios and their potential impact on the UK. The graph on the next page illustrates the estimated physical damage and loss of life for each scenario. ▶

Cyber

https://www.poolre.co.uk/Reports/Quarterly-Threat-Report-Aug-2016.pdf (retrieved 23 October 2016)

Potential cyber terrorism scenarios

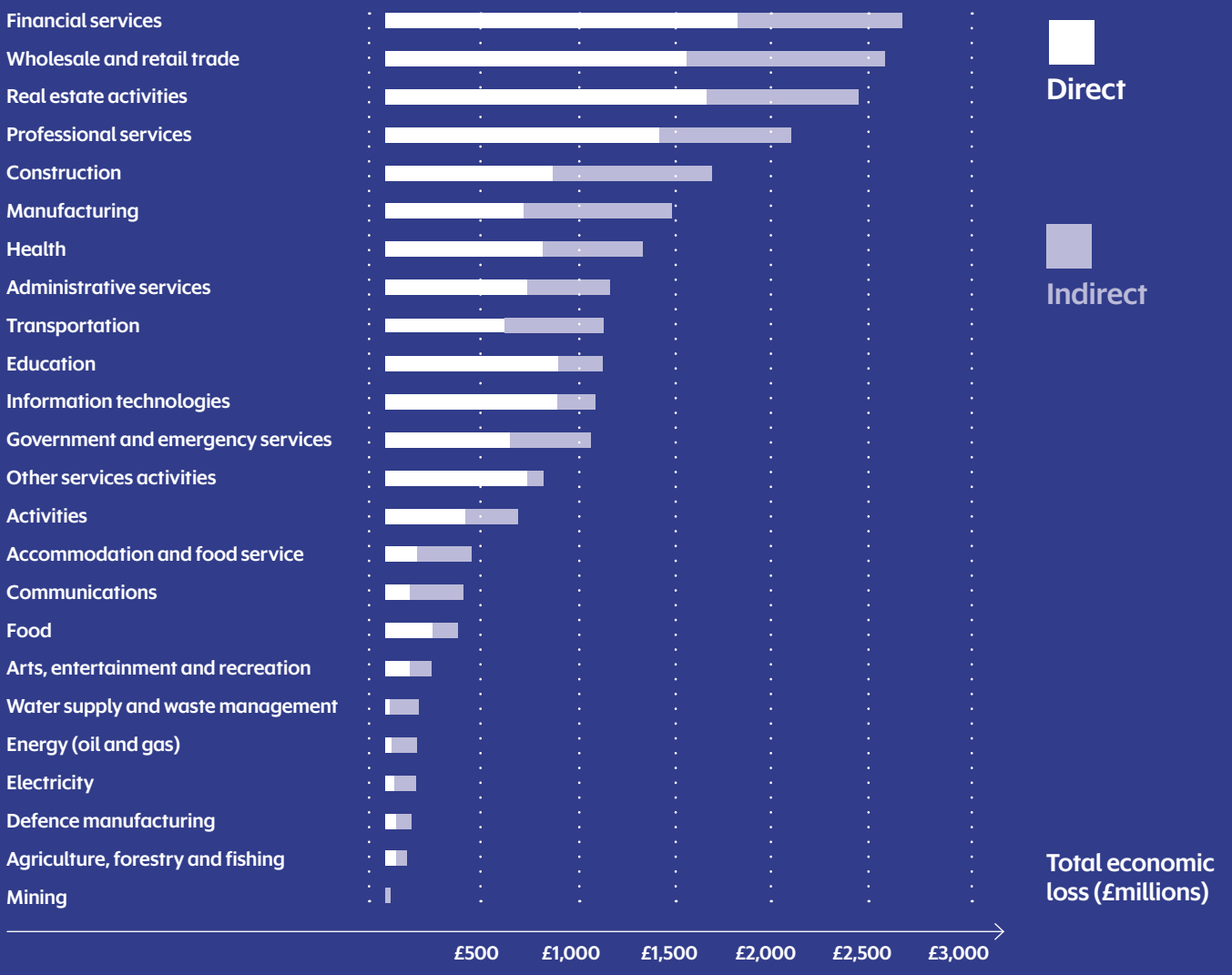


Source: Centre for Risk Studies, Univ of Cambridge

A UK cyber blackout scenario also describes a well-resourced and carefully developed attack on the electricity distribution network in the south and east of the UK and its impacts on UK CNI. The direct economic losses to the sectors modelled are estimated to range from £7.2 billion to £53.6 billion; the overall impact on UK GDP ranges from £49 billion to £442 billion across the entire UK economy in the five years after the attack. The table below details the direct and indirect economic losses across 23 sectors. ▶

Cyber

UK cyber blackout scenario – economic losses



Source: Centre for Risk Studies, Univ of Cambridge

Insuring cyber terrorism

There are clearly inherent risks for (re)insurers intending to cover cyber terrorism, in spite of the unlikely development of a destructive cyber capability over the next five years by a terrorist organisation. The principal risk stems from a lack of a comprehensive cyber risk profiling system for potential policyholders. Additionally, vulnerabilities and attacks are often discovered well after the date of attack and in many cases involve the compromise of millions of individual machines, harnessed to attack a specific organisation or system. These 'bot nets' of compromised machines can also exist across multiple organisations with different cyber policies and risk profiles. Insurers would need to clarify the meaning of 'occurrence' in order to protect against each machine compromise, or each business impacted, being considered as a separate claim in a single act of cyber terrorism. ▶

Cyber

Conclusions

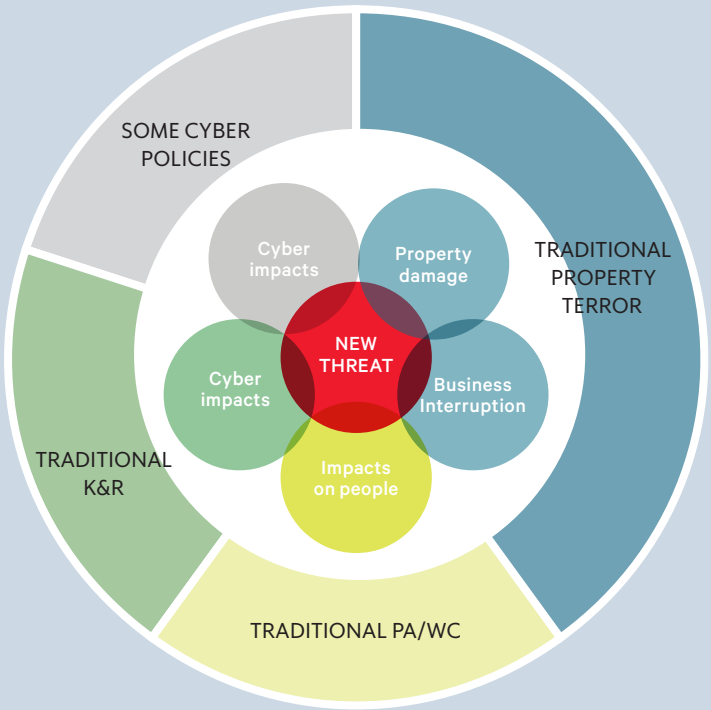
However remote some of these threats may seem, the pace at which technology can and does change creates difficulties in predicting future developments. There have already been significant developments in malicious software, which increasingly innovates and adapts to cyber security controls. The nature of the peril is also significantly different to others. Cyber, for example, could theoretically affect most, if not all, insurance classes. This is highly unusual as most catastrophe loss drivers affect one or two classes of insurance – floods affect property; asbestos affects liability, for example. This significantly impairs (re)insurers' ability to allocate capital and model loss accurately. It should be noted that there have been significant improvements to cyber security controls, as well as improved incentives for the identification of software exploits. The importance, and potential effects on cyber security, of a robust cyber insurance product should not be underestimated, in spite of the difficulties of underwriting the peril. Such a product could influence consumer behaviour to adopt recognised standards and increase the UK's resilience to the contemporary terrorism threat. In many areas of the current terrorism landscape, governments and business are reacting to the recent changes in terrorist behaviour. In this vital area there is a real opportunity to pre-empt future tactics. ●

Quarterly Threat Report

Spotlight

Insurance and the new face of terrorism

Terrorism impacts and gaps in existing insurance cover



Traditional property terror

Property damage
Business interruption
Non-physical damage BI
Contingent BI
CBRN
Loss of attractiveness

Traditional PA/WC

Life
Injury

Cyber

Property damage
Business interruption
Non-physical damage Bl

Traditional K&R

Kidnap
Extortion
Detention
Hijack
Hostage crisis
Response fees
Additional expenses
Legal liability
PA
Disappearance
Personal evacuation
Threat
Assault
Cyber extortion
Cyber BI

Source: JLT

The nature of terrorism has clearly changed since Pool Re was created as a response to the PIRA's mainland bombing campaign.

Until recently, the primary loss driver was property damage, with any business interruption resulting as a direct consequence of the physical damage. The changing nature of terrorism is putting into question the strategy of focusing mainly on property damage for terrorism reinsurance. This has come into question after losses from recent attacks in France, Germany, and Belgium have not fully come under the remit of their respective terrorism pools. This has led to calls for the reinsurance industry to expand coverage for terrorist attacks to include life and to clarify and expand BI losses to include non-damage BI.[20, 21] The table below demonstrates how effective the reinsurance offering has been for the traditional threat paradigm in assisting with disaster recovery. Significant sums were met by a combination of commercial and state-backed pools in the 1990s and early 2000s, the largest of which was the 9/11 attacks, with (re)insurers incurring $23,870 million in losses.[22] ▶

20. 'Political risk and crisis management insurance, opportunities for growth', KPMG, July 2016

21. 'Terror attacks prompt changes in insurance', 'Financial Times', 7 August 2016

22 Original losses, have not been scaled for inflation.

Insurance and the new face of terrorism

Ten most costly terrorism attacks to (re)insurers

Date	Country	Event	Insured ($m)	Fatalities
11/09/2001	US	New York/ Washington	23,870	2,982
24/04/1993	UK	Bishopsgate bomb	1,152	1
15/06/1996	UK	Manchester bomb	946	0
10/04/1992	UK	Baltic Exchange bomb	852	3
26/02/1993	US	WTC bomb	794	6
24/07/2001	Sri Lanka	Colombo airport	507	20
09/02/1996	UK	South Quay bomb	329	2
19/04/1995	US	Oklahoma bomb	185	166
22/03/2016	Belgium	Brussels bombs	185	32
11/04/1992	UK	Staples Corner bomb	122	0

Source: Pool Re

In today's threat environment the differences between lines of business traditionally covered by the terrorism market and the lines of business that have incurred economic losses are becoming more noticeable. Although the full economic effects of a terrorist incident are difficult to measure, owing to the varied associated effects across multiple lines of business, there are identifiable gaps in current risk carriers' products that could be capitalised on by expanding lines of business.

The most salient appears to be loss of attraction and non-damage business interruption. Non-damage business interruption is traditionally covered under denial of access extensions; however, these are often sub-limited and restricted to a radius of 250m. Recent attacks have led to city-wide lockdowns, which have resulted in economic losses due to denial of access that have not been covered due to these restrictions. This calls into question the sufficiency of insurance offerings in relation to the changing current threat.

After the November 2015 Paris attacks, Brussels was put into a five-day lockdown as authorities conducted a number of raids across the city. This lockdown alone is estimated to have cost €51.7 million per day in terms of increased security and lost business income.[23] Total costs for the lockdown are estimated at €350 million, with tourist numbers in December 2015 down by 20 per cent.[24] The Centre for Risk Studies, part of

23. Pool Re's 'Market Review of Contingent BI Extensions (Damage and Non-Damage)', May 2016

24. Ibid

the University of Cambridge Judge Business School, has also estimated the associated economic losses from the Paris attacks to have impacted the French economy in the order of $9-12 billion. The initial estimates for the Nice attacks are also equally bleak. With little or no direct damage to property, the principal economic loss drivers have been non-damage and contingent business interruption, as well as loss of attraction.[25]

Many of these losses impact the SME sector (small and medium size enterprises) the hardest, as they are the least likely to be insured against terrorism. UK Government figures show that more than 99 per cent of UK businesses are SMEs – employing 0-249 people.[26] Additionally, 95 per cent (5.1 million) of UK businesses were classified as micro-businesses – employing 0-9 people.[27]

Daesh and other actors have clearly realised the economic impact of their attacks, which to date have primarily targeted people in crowded places. The effects on the tourism sector in Tunisia and Sharm el-Sheikh, after the shooting of tourists at the Port El Kantaoui resort (June 2015) and the downing of a Russian passenger jet (October 2015), have had a severe destabilising influence on the local economies and further serves to enhance Daesh's reputation as an international terrorist organisation. Unfortunately, it appears only a matter of time before a terrorist group prosecutes a successful attack in the UK. Currently the SME sector is the least able to deal with, and will be most affected by, such an attack.

The fusion of risk

Insurers have traditionally split the components of terrorism risk into elements of pre-existing cover to manage the impact on different lines of business. In the case of terrorism, this ranges over property, personal accident and workers' compensation, kidnap and ransom, and cyber (see graphic at the top of this section). Some might say that the fusion of risks calls for a fusion in the product being offered. However, this is largely prohibited for three reasons: a justified fear of the potential aggregation of risk, the deployment of insurer capital, and the demand for highly specialised 'crisis-management' products which are better able to deal with complex, geographically isolated and fast-moving situations.

The creation of new lines of business for terrorism insurance are where state-backed reinsurance pools can play a vital role by mitigating against the systemic risks associated with aspects of the threat landscape. Groups such as Daesh, among others, have displayed the intention to deploy destructive cyber attacks against critical national infrastructure, and continually seek to develop 'exotic' attack methods such as deploying a newly found expertise in chemical and potentially radiological weapons (CBRN). The creation of new lines for cyber terrorism and CBRN are two such examples that will enable the market to innovate and create new insurance products to provide coverage for the changing peril. The London market also contains a wealth of risk mitigation and management expertise and is likely to be the one sector, in both the private and public sphere, which has the ability to create agile risk products, capable of adapting and mitigating against an evolving terrorism threat. ●

25. These are areas in which the insurance market could capitalise to increase effective coverage in an attack.

26. House of Commons Library, Briefing Paper (06152), 7 December 2015

27. This represents a significant market for insurance companies to expand into with increased denial of service offerings.

Belgium's extremist networks

The road to Paris and Brussels

Police guard a checkpoint during a raid in the suburb of Schaerbeek, Brussels, on 25 March 2016 (AP)

The most significant actors on the European threat landscape have been Belgium-based jihadi networks, responsible for the Paris attacks in 2015 and the 2016 Brussels bombings.

An estimated 451 foreign fighters have travelled to Syria and Iraq from the country, making Belgium the highest contributor of fighters per capita of any European country.[29] The reasons for this do not lie in any exceptional failure on the part of the Belgium authorities. Neither are radicalisation rates there markedly higher than in other European countries. The principal reason was the emergence of three radical networks during the early stages of 2011, all interconnected and led by a cluster of radical preachers who enabled and encouraged travel to Syria at the start of the conflict.

Initial fighters came from the Antwerp-based network called Sharia4Belgium, led by Fouad Belkacem a local radical and petty criminal.[30] This network hid its real agenda through public activism and controversial publicity stunts. Much of the group's structure and organisation was modelled on Anjem Choudary's UK-based group Islam4UK. This tactic of public activism caused many to dismiss such groups out of hand. However, an estimated 75 Belgium nationals, who travelled to Syria and Iraq, have been directly linked to this network.[31] ▶

29. Combating Terrorism Centre (CTC), June 2016

30. "Head of Belgian Group Said to Recruit Fighters for Syria Gets 12-Year Term", New York Times, 11 February 2015

31. CTC, June 2016

Belgium's extremist networks

Parallel to this network were a group of smaller networks, all gaining support because of the conflicts in the MENA region. While Sharia4Belgium concentrated its activities on the Flemish areas of the country between Antwerp and Brussels, another group, Resto du Tawhid, led by Jean-Louis Denis, was active around the Gare du Nord area of Brussels, home to a large North African francophone population.[32] One of Denis' key roles was to provide a link between Sharia4Belgium and Khalid Zerkani, leader of a far more dangerous and clandestine network based in the Molenbeek district of Brussels. Members of the Zerkani network became key figures in the Paris and Brussels attacks of 2015 and 2016. They included: Abdelhamid Abaaoud, the co-ordinator of the Paris attacks; Salah Abdeslam, the surviving gunman from the Paris attacks and childhood friend of Abaaoud; Chakib Akrouh, who detonated a suicide vest during a French special forces raid in Saint-Denis, after the Paris attacks; Najim Laachraoui, the bomb maker for the Brussels attacks; and Reda Kriket, a French national who was arrested in Paris with weapons and explosives in the days after the bombings in Brussels.[33]

From as far back as 2012, the Zerkani network gained vital experience fighting for Daesh in Iraq and Syria. Their efforts become focused on Europe in the autumn of 2014, after a declaration of war by Daesh's spokesman Abu Muhammad al-Adnani on 11 September 2014. Before and after this announcement, the network was connected to a series of successful and attempted attacks across Europe, which included the attack on the Jewish Museum of Belgium in Brussels (May 2014)[34], a plot halted by police in Verviers, Belgium, in January 2015[35], an attack on a Paris church in April 2014 and the attempted attack on a Thalys train in August 2015.

While Abaaoud was described as the 'ground commander' of the Paris attacks, subsequent investigations have shown that Mohammed Belkaid, an Algerian national, had overall control. Belkaid was killed during the police raid immediately before the Brussels bombings on 15 March 2016 during an exchange of fire with police, which enabled other cell members to escape, including Abdeslam, the surviving gunman from the Paris attacks. On 18 March, Abdeslam was arrested in Molenbeek, while the remainder of the cell[36], fearing further arrests, carried out the Brussels bombings, resulting in 32 deaths and 340 injuries.

These three networks have been responsible for the planning and execution of Europe's two most deadly terror attacks in recent history. Subsequent investigations have revealed that these three networks had ties to a minimum of 174 Belgian fighters who travelled to Syria and Iraq.

As the tragic example of Nice shows, inspired attackers are occasionally capable of inflicting large numbers of casualties. However, it is the traditional forms of terrorism that should concern us most. These are the people with the means and experience to direct and support attacks with tactics and weapons they have trained and fought with on today's battlefields. As Daesh loses its hold in Iraq and Syria, it is these networks that will pose the greatest threat. Armed and experienced, they will seek to continue and improve on previous attacks. ●

32. Ibid

33. Ibid

34. Abaaoud had communications with Mehdi Nemmouche, the gunman of the attack, in the months leading up to it.

35. This attack was allegedly co-ordinated by Abaaoud, who was in Athens at the time.

36. Najim Laachraoui (the bomb maker and suicide bomber at Brussels airport) and Khalid and Ibrahim el-Bakraoui (suicide bombers at the Brussels metro and airport respectively).

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
T @poolreinsurance

POOL RE

REINSURING TERRORISM RISK