Fragmented terror threat

Terrorism: A fragmented threat

by Bill Udell **and** Jonathan Wood**.**

Companies face a more fragmented, less predictable global terrorism threat in 2017. Alongside persistent threats from left-wing, right-wing and ethno-national militant groups, the Islamist extremist threat continues to evolve. The eventual collapse of Islamic State (IS) territory in Iraq and Syria will force a global exodus of experienced militants. Foreign IS affiliates – as well as al-Qaida's network – will compete for local and regional influence. Jihadist propaganda, potentially accentuated by changes in US foreign policy, will continue to motivate and inspire violent incidents, both by Islamist extremists and by people with personal grievances.

In response, companies are adjusting risk management practices. They are augmenting threat intelligence and monitoring programmes to leverage technology, while updating crisis management and risk mitigation planning to account for new scenarios. Companies are also revisiting insider threat programmes in light of the convergence of self-radicalisation with traditional workplace or personal grievances. Finally, companies are selectively beefing up physical security and training around assets and personnel, particularly travellers.

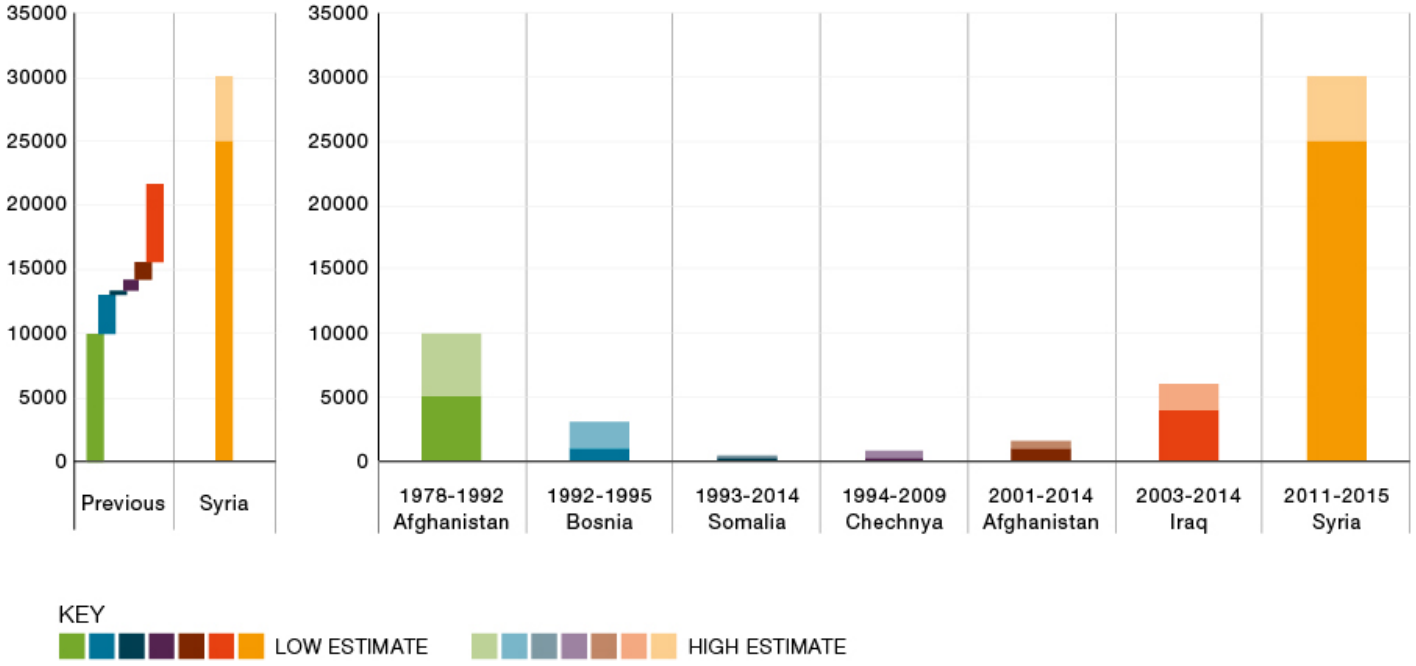
Territorial collapse

The collapse of IS territory in Syria and Iraq will transform terrorism threats in 2017 and beyond. IS will lose much of its financial and military resource base; its safe haven for training militants and producing propaganda; a convenient platform for launching transnational attacks; and – crucially – the geographic pillar of its ideological influence. As a case in point: the prophesied climactic battle between jihadists and 'crusaders' in Dabiq will not occur after IS gave up the symbolic Syrian village in late 2016 without a fight.

But IS will not be eliminated as a threat. As it loses territorial control, we expect core elements to retreat back into an asymmetric, guerrilla insurgency in Iraq and Syria, feeding on lingering Sunni grievances. It did this before, assiduously rebuilding strength in the wake of the US military 'surge' and Anbar Awakening in Iraq during 2007-08. IS thrives in political and security vacuums, and Syria and Iraq will provide plenty of both in the coming years. IS and its successors – though depleted – will certainly live to fight another day.

Nor will the suppression of IS dramatically clarify the global threat environment. If anything, IS's short-lived 'caliphate' – in the wider context of post-Arab spring instability – unleashed dynamics that will drive significant fragmentation of the Islamist extremist threat in 2017.

ESTIMATED NUMBER OF FOREIGN FIGHTERS



Sources: International Centre for Counter-Terrorism (ICCT) 2015, UN 2016

Fragmenting terrorism risk

The following dynamics are likely to drive the evolution of the global Islamist extremist threat in 2017:

- **The collapse of IS territory is likely to prompt a global exodus of foreign fighters**. IS specifically – and Syrian militant groups generally – has benefited from an unprecedented influx of foreign fighters (see Figure 1). As IS falls, many will be killed in battle, some captured trying to escape and others recruited into other groups – including rival al-Qaida affiliate Jabhat Fatah al-Sham (JFS). Of more concern, the trickle of foreign fighters returning home, especially to Western Europe, could become a flood, imbuing local extremist networks with experience and capability.

- **IS is likely to shift further towards transnational terrorism**. In Western Europe, a series of IS cells have been disrupted since the March 2016 attacks in Brussels, while 'virtual' IS controllers operating via encrypted chat apps have been linked to several small-scale 'homegrown' attacks. IS is also believed to have relatively dense networks in Turkey, a major target. Throughout the Gulf countries, IS affiliates have mounted a series of attacks on security forces and Shia Muslims, seeking to aggravate sectarian tensions. Meanwhile, al-Qaida's turn towards high-impact attacks, chiefly around the Sahel periphery, is likely to persist as it seeks to reassert its influence as a jihadist vanguard.

- **The collapse of IS is likely to provoke a new round of fragmentation within jihadist groups** as formal allegiances are reconfigured and scores settled. The loss of the 'caliphate' will deprive IS 'provinces' of legitimacy and even raison d'être, giving local or al-Qaida-affiliated groups an opportunity to rebound. Factional infighting will continue to promote high-profile attacks, including against foreign assets and personnel. In Syria, JFS will undoubtedly emerge strengthened as a leading actor in the rebellion, credible heir to the al-Qaida legacy and potential source of transnational attacks.

- **A dense library of high-quality, vernacular jihadist propaganda will persist indefinitely online**, serving as a source of inspiration and incitement for jihadist sympathisers and other threat actors. Just as the sermons of al-Qaida ideologue Anwar al-Awlaki and the bomb designs of al-Qaida's *Inspire* magazine remain potent reference points even for IS-inspired jihadists, IS spokesman Abu Muhammad al-Adnani's incitement to conduct small-scale improvised attacks at home is being canonised. Indeed, the opportunity to support and promote the so-called 'caliphate' appears to have driven a sharp rise in plans and attacks based on propaganda guidance since late 2014.IS's sophisticated media strategy and apparatus – though blunted by relentless coalition air strikes since mid-2015 – raised the bar for jihadist groups worldwide, many of which have sought to replicate its toxic blend of online distribution, production polish, language localisation and violent atrocity. These 'media jihadists' need only an internet connection to operate. (And other types of violent political actors – from right-wing militants to ethno-national insurgents – are likely to be absorbing these tactics and strategies as well.)

- **Extremist methods will continue to colour violent acts by disaffected, attention-seeking, aggrieved or mentally disturbed individuals**. Motivations in many violent acts are more likely to be ambiguous and potentially more precipitous, defying easy categorisation or apprehension.

- **Sources of threat will emerge within large populations of refugees and displaced people – especially in Europe but also in the Middle East**. The small but rising number of incidents linked to recent migrants in 2016 underscores the nascent threat, and it is still early days in the overall social, cultural and economic shock. Over time, whether through alienation from host societies or dedicated outreach by Islamist extremists, these populations are likely to become more susceptible to recruitment or amenable to facilitation.

The public response

Few governments are ignorant or idle in the face of shifting terrorism threats. The US, Europe and allied countries such as Canada and Australia will remain involved in counter-terrorism operations in many theatres in 2017. This will continue to supply intent for both jihadist groups and homegrown extremists to carry out retaliatory attacks. The US in particular may adopt an even more aggressive global counter-terrorism posture under the Trump administration.

Indeed the year so far has seen capitals, major cities and other sites around the world come under attack. Control Risks' proprietary database of terrorist fatalities shows 5,326 deaths from terrorist

incidents around the world in the first quarter of 2017. Of interest, this is the lowest quarterly death toll since the second quarter of 2013.

However, most countries will continue to face resource and capability constraints that compound the counter-terrorism challenge.

At a basic level, small-scale, homegrown terrorism – either in line with IS and al-Qaida propaganda or actively directed from abroad – undermines traditional law enforcement and intelligence mechanisms that rely on infiltrating (using informants) or conducting technical surveillance into conspiracies. As well as 'lone wolves' operating independently, IS recruitment among criminal circles in particular has allowed recruitment, facilitation and operations to develop below the counter-terrorism radar. Security and intelligence officials widely agree that the shift in jihadist communication to encrypted apps further reduces opportunities to detect threats.

Counter-terrorism co-ordination continues to face institutional and resource deficiencies. In Europe, significant deficiencies persist in routine information and threat intelligence sharing between countries and agencies (even in the same country). Efforts launched by Europol in early 2016 may eventually improve international co-ordination, but remain far from being an integrated regional counter-terrorism system. No European police or intelligence service currently has the resources to monitor all potential threats all the time. The situation is more favourable in the US, which faces smaller domestic and foreign extremist networks, and is geographically more difficult for foreign militants to access.

Finally, countering violent extremism (CVE) programmes remain in their infancy, and are being undermined by xenophobic backlashes against Muslim communities in the wake of terrorist incidents and as a result of high levels of migration. Increasingly hawkish domestic and foreign policy responses may further polarise community relations, making CVE programmes increasingly difficult to operate. Furthermore, mental health support is broadly lacking in most countries, particularly among minority communities.

The corporate challenge

The fragmenting terrorism threat is transforming – perhaps permanently – the challenge for those whose role it is to mitigate terrorism risk within companies. At a basic level, this increases and complicates a company's basic duty of care obligation. In fulfilling duty of care, the litmus test consists of identifying risks to employees that are 'reasonably foreseeable' and putting programmes in place to mitigate such risks.

The changing threat environment radically expands the scope of a 'reasonably foreseeable' risk. Whether working at home or travelling abroad, employees face a more diverse array of threat scenarios against a wider set of venues while performing a broader range of activities. Put simply, companies now have a larger share of responsibility for a problem that is also harder to define.

There may be legal consequences for failing to expand mitigation measures in line with the threat environment. Continuing civil litigation by victims' families against San Bernardino County

(California state, US) – the site of a jihadist mass shooting in December 2015 – generally claims that the county failed to put in place measures that might have prevented the attack. In this regard, the changing threat environment is of increasing concern to executives and other corporate security leaders.

Company responses

Companies have started to tackle threat intelligence as a ‘big data’ problem. The types of information sources available and the volume of potentially relevant threat data – especially via social media – have exploded in recent years, prompting companies to adjust both threat assessments and monitoring programmes. The most robust efforts go well beyond aggregating raw information feeds: companies are increasingly bringing on analytical capability to prioritise, operationalise and act on information in real time based on their footprint, personnel and business context. Technology is helping to substantially automate and optimise this process, particularly via the spread of the virtual global security operations centres (GSOCs) model, as well as the application of machine learning to threat intelligence.

Based on a more specific understanding of the evolving threat, companies are assessing whether their overall security and risk management programmes are fit for purpose and often finding that they need to take action in the following areas:

- **Companies are taking a fresh look at insider threat and workplace violence programmes**, particularly by incorporating self-radicalised violent actor threat scenarios. This reflects rising concern about the convergence of self-radicalisation with workplace disputes, personal grievances and mental health issues – including among contractors and suppliers. These individuals often display perceptible risk indicators ahead of an incident through behaviour, tone or actions in the workplace and via online activity. Risk mitigation can exploit such indicators through a combination of management engagement, workforce awareness and technical monitoring.

- **Companies are selectively beefing up physical security precautions for personnel and assets**. Key activities include benchmarking and recalibrating physical security requirements against the changing geographies and tactics of terrorist groups; strengthening perimeter security and access control at global facilities; instituting executive protection programmes in new jurisdictions; stress-testing travel security plans and infrastructure; and revisiting personnel tracking and mass notification capabilities. The new threat environment has also imposed new training requirements on security managers, both in terms of new jurisdictions and new threat scenarios, such as active shooters. It has also forced multinational companies to address the challenges of training across borders, cultures and a diverse employee base.

- **Companies are recalibrating impact mitigation planning to reflect the changing threat environment**. Crisis and incident management programmes have been adjusted to reflect diffuse terrorism risks and involve relevant intelligence and law enforcement stakeholders. Crisis management plans and training are shifting from spectacular and sophisticated

attack scenarios – such as a large-scale truck bomb – to active shooter threats, barricade hostage incidents and other methods favoured by IS-inspired homegrown extremists. Business continuity planning is being adjusted to reflect the potential for disruption as a result of either attacks or security force lockdowns in commercial centres.

- **Companies are finding value in information-sharing among peer organisations** and conducting formal third-party benchmarking against those peers. As they struggle to allocate scarce resources in the face of a fast-moving threat, many are concerned about falling behind not only that evolving threat but also analogous corporate trends. Official links between government and the private sector, such as the Overseas Security Advisory Council (OSAC), remain critical, as do partnerships with law enforcement and providers. But companies are increasingly looking for a more formal approach to sharing information – particularly actionable information in real time – with each other in the form of crisis management and security forums that allow co-ordination across a large group of contributors.

Image accreditation: Press Association - Kurdish PKK fighters on the front lines against Islamic State, Apr 2016 (Credit Image: © Kurdishstruggle/Planet Pix via ZUMA Wire).