DECODING TWO DIFFERING RESPONSES TO A COMMON THREAT

Camilla Scrimgeour
Senior Analyst, Pool Re

HOW DO THE UK AND US COMPARE?

The UK's revised Counter Terrorism Strategy (CONTEST) was published in June 2018.

The importance of working closely with the private sector, including the insurance sector, in counter-terrorism was highlighted as a theme across the four pillars, and Pool Re was recognised as an excellent example of how Government and industry can work together to mitigate the effects of a terrorist attack in the UK.

CONTEST was first published in 2003 to "reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence". 15 years after the original report, Pool Re asked Sir David Omand, who was instrumental in developing the original strategy, for his thoughts on the success of the strategy and its latest edition.

CASE STUDY

CONTEST 2018: Partnership with Pool Re

The insurance industry has the potential to shape behaviour and improve safety, security and resilience, including helping to promote security-minded behaviours in areas where there is less regulation. The Home Office works closely with insurance providers to explore areas where they might support our counter-terrorism objectives.

Pool Reinsurance Company (Pool Re) is an excellent example of a public-private partnership set up specifically to mitigate the financial impact of a terrorist attack.

Pool Re and the police have worked together to develop the Loss Mitigation Credit: a discount on insurance premiums for businesses implementing the Government's accredited Protective Security Improvement Activity. This benefits both businesses and security.

As well as working closely with the private sector, the UK has deep ties with its allies in counter-terrorism. To compare the approaches of UK and USA counter-terrorism strategies, Pool Re has compared Sir David's thoughts with those of Ali Soufan, a former FBI agent and CEO of The Soufan Group, including on the US's counter-terrorism strategy.

UK

Sir David Omand GCB
One of the original authors of the CONTEST strategy

Q
What are your thoughts, 15 years after the original CONTEST, on the 2018 revised strategy?

Looking back, I am very glad to see the strategic continuity between then and now, with the same underlying strategic aim of maintaining normality in domestic society in the face of a continuing terrorist threat. During the 15-year duration of CONTEST we have already seen four Prime Ministers of different political persuasions embrace it, and no less than eight Home Secretaries and seven Foreign Secretaries. You cannot have effective strategy at national level that changes with each change of political personality. Sometimes major changes of direction in public policy are called for, that is the direct product of our democratic system of government. But there is a price to be paid for the discontinuity of effort whilst the efforts of the very many organisations involved in any major public policy are reoriented to the new direction of travel. That has not happened with counter-terrorism and we are all safer as a result.

You cannot have effective strategy at national level that changes with each change of political personality.

What has ensured the continuity of approach, which is essential, is the strategic logic of CONTEST. Of course there have been course corrections along the way, and shifts of emphasis not least as the threat has mutated under pressure from the security forces. But the underlying aim has not wavered, and that makes it much easier to generate an 'all of nation' effort and to garner support from all the communities affected by terrorism.

The CONTEST strategic aim of reducing the risk from terrorism so that people can go about their lives, freely and with confidence, in other words to maintain conditions of normality, is certainly still right. The new version of CONTEST, however, sensibly widens the definition of threat to include the extreme right. The important qualifiers of the strategic aim, freely and with confidence, are also still there (freely meaning that the citizen has not had to give up essential freedoms and individual rights to achieve the objective; with confidence meaning that the citizen trusts the authorities to manage the risk, aviation and public transport including the London underground are used, tourists still visit the UK, there is inward investment, the public is not in fear of the terrorist).

The operationalisation of the aim through keeping the 4Ps, Pursue, Prevent, Protect and Prepare is sensible since that connects implementation of the strategy directly to the well-understood original risk management logic of CONTEST. The risk from terrorist attack is the product of likelihood, by vulnerability, by initial impact if the terrorists get through our defences, and the duration of any period of disruption the attack causes. Each of those factors can be influenced by Government, the private sector and the public working together thus reducing the overall risk. Of course, the detailed measures under each P will change as programmes are completed and new needs arise, as we see with the latest work on Prevent.

Q
Was the AQ threat post-9/11 so different from anything that had gone before that a new approach was needed (there had been no CONTEST type strategy to counter NIRT)?

Many (perhaps most) of us involved in the design of the original CONTEST strategy had worked on Northern Irish terrorism in previous years. The Northern Ireland experience did influence our approach. For example (and these may seem very obvious points but we now know that the architects of the US war on terror had a very different approach):

- Be seen to act in ways that reinforce not undermine the values of law abiding society
- Have a strategic objective: deny the terrorists what they most seek which is to disrupt through placing the public in terror; prevent the terrorists destabilising public confidence in the authorities
- Encourage fortitude when attacks take place and to prepare for such set-backs harness in advance the strengths of all sectors and communities in society behind the strategy
- Understand the terrorists in order to frustrate them through a clear unified counter-strategy
- Accept the need for patience, and avoid the temptation of extra-legal short-cuts

There was very wide and active participation in the research behind the strategy and there were lively discussions in an official Cabinet committee as to how best to set out the strategic aim (which has not changed in the latest version of CONTEST) and to operationalise it (though the 4P programmes of work – Prevent, Pursue, Protect and Prepare). The strategy was presented to the Home Secretary's CT Cabinet Committee and then to the full Cabinet, which endorsed it. After that the implementation began in earnest.

Q
If, with hindsight, you could add one additional element to the original CONTEST, what would it be?

With hindsight we could have made more in public of the cross-cutting supporting themes, for example the acquisition and use of pre-emptive intelligence that involved substantial investment, not least in the emerging field of digital intelligence, as now regulated by the Investigatory Powers Act 2016. That essential step, now eventually endorsed by Parliament, could have been better explained to the public at the time. Another such theme was public information and awareness of the strategy itself, and with hindsight we could have developed this strand, not as a separate pillar but underpinning the whole strategy as intelligence does.

Although not a separate strand, with hindsight we should have explicitly included the domestic reaction from the extreme right as one of the threats to be countered under both Pursue and Prevent. It was certainly not ignored in the early work on CONTEST but was not made explicit. That gap has now been remedied in the 2018 version of CONTEST.

Q
To what extent can the current CONTEST deal with emerging, unconventional threats (such as CBRN and cyber terrorism)?

The original CONTEST strategy and its subsequent revisions and updating did provide for defence against CBRN threats. After 9/11 the allied operations in Afghanistan to dismantle the AQ infrastructure revealed that terrorist operatives passing through the AQ training camps were being trained in chemical and biological means of conducting terrorism. CONTEST therefore included: under the Pursue programme a high priority to be given to tracking down terrorist suspects interested in such vectors of attack, under the Protect programme investment in the development and deployment of analytical capabilities for CBRN defence and under the Prepare programme the development of a joint CBRN training centre at Winterbourne Gunner for the emergency services to learn together how to tackle such threats. Regular live exercises are held to practice procedures.

Countering radiological dispersal devices was also a focus of attention in CONTEST given what intelligence revealed of the terrorist intentions. The response included developing and installing radioactive detection portals at UK ports and airports to detect any attempt to smuggle such material into the UK and action by police and security authorities to ensure adequate security for radioactive sources used in medicine and engineering in the UK and safe disposal of unwanted devices.

Cyber terrorism was not considered a major threat in the original CONTEST strategy given the then state of global digital technology. What has emerged in the subsequent years is of course the ability of adversary states and non-state actors to damage and disrupt through cyber means, ranging from simple denial of service attacks using criminally provided software available on the dark net to highly sophisticated malware such as the 2017 NotPetya attack that Russia aimed at Ukraine but which spread through the Internet and, for example, totally destroyed the computer network of the giant global shipping company Maersk. So far terrorist groups have used digital technology for secure communications with their supporters and to recruit and mobilise for attacks, but not as a direct vector to disrupt society by attacking critical infrastructure. But this could quickly change and the latest version of CONTEST does have this threat identified as does the National Cyber Security Strategy.

Q

How successful would you assess CONTEST to have been over the last 15 years?

The essential strategic aim – to reduce the risk from terrorism to the UK and our interests overseas so that people can go about their normal lives, freely and with confidence – has been achieved in respect of the UK. The risk is being managed, including by highly successful intelligence operations to generate pre-emptive intelligence to frustrate terrorist plots, although tragically not without some terrorist successes over the years. That state of normality has been achieved whilst maintaining our essential freedoms and liberties – and confidence has been maintained in the UK – tourists come, public transport and aviation are busy, the public is not in a state of fear. So the terrorists are failing, not winning.

The threat has therefore mutated, but the aim of strategy in CONTEST in countering the threat remains apt.

All that said, the threat remains high and has evolved and internationalised well beyond that from AQ against which the original CONTEST strategy was pitched. We were all surprised, and perhaps we should not have been, when Sunni extremists in Iraq that had been part of AQAP under their former leader Abu Musab al-Zarqawi took the opportunity offered by chaos in Syria to seize territory in Syria and Iraq to form the so-called Islamic State. That provided them with the ability not just to have a sanctuary but to raise and command significant financial resources. It has taken considerable military effort, and cost many lives, to dismantle that construct. A very necessary operation, but one that has inevitably left Daesh survivors, some of whom have already entered Europe bent on revenge and furthering their ideology. The threat has therefore mutated, but the aim of strategy in CONTEST in countering the threat remains apt.

Q

Considering the global terrorism threat we face, to what extent could there be a global CONTEST strategy where allies unite?

There is already now, helpfully, considerable convergence of strategy on tackling the risks from terrorism on both sides of the Atlantic. As the thinking developed in London that became the 2002/3 CONTEST strategy, the UK and US set up a jointly chaired Homeland Security Contact Group to share experiences and technical expertise in how to improve domestic security, including taking concerted action to boost aviation security and develop new technology for protective security. Such cooperation continues and includes work conducted under well-funded EU research and development programmes.

The UK has also deepened its global CT intelligence cooperation, not just with the US and Five Eyes allies[1], but also European partners and many other friendly states around the world. The UK has been active in offering support and training to countries afflicted by terrorism and to help them build up their domestic capabilities.

UK law enforcement also cooperates closely with EU partners on countering terrorism, organised crime and cyber crime and sharing evidence to bring suspects to justice. Such active cooperation is mutually beneficial and takes place at an EU level under EU justice and home affairs arrangements, and with recourse by the citizen to the Courts and when necessary ultimately to the European Court of Justice. The UK has, however, been warned by the Commission that outside the EU after Brexit it will be unable legally to enjoy the same level of law enforcement cooperation, including membership of Europol, information sharing under the Schengen agreements and use of the European arrest warrant.

The UK is nevertheless a major European nation (and will always be so, regardless of our exact status vis a vis the EU after March 2019 and Brexit) and will have to continue to face, as EU partners do, the common threat of Salafist-Jihadist terrorism. When in 2005 the UK held (under Tony Blair) the presidency of the European Council, the EU adopted its own counter-terrorism strategy based closely on the CONTEST model. There has been close cooperation on strategy ever since. Having the UK continue to be able to work as an active security partner with EU member states is essential for the future security of the continent as well as for the British Isles. So, some legal framework (such as an EU/UK Security Treaty as proposed by the UK Prime Minister) is needed to allow current law enforcement cooperation to continue after Brexit, and to develop as the threat evolves, as it surely will. At the time of writing it is not at all clear whether the EU negotiators will recommend such an approach to the Council.

1 The Five Eyes is an intelligence alliance between the United Kingdom, the United States of America, Australia, Canada and New Zealand.

US

Ali Soufan
Chairman and CEO of The Soufan Group and former FBI Agent

Q

To what extent have the US Administration's CT strategies evolved over the past 16 years?

During the past 16 years, counter-terrorism strategy in the United States has evolved considerably. The initial years of the Global War on Terror were dominated by the relentless efforts to dismantle AQ's leadership, undertaken in tandem with Operation Enduring Freedom in Afghanistan. Less than two years later, however, the United States committed to one of its most significant foreign policy decisions in the post-Cold War era by invading Iraq and soon becoming mired in a bloody insurgency, caught in the middle of an escalating sectarian conflict that would reinvigorate the global jihadist movement and give rise to al-Qaeda in Iraq (AQI), which would eventually morph into the so-called Islamic State, or Daesh.

The Obama administration continued many of the policies of the Bush administration's two terms, and even adopted a more aggressive posture with respect to the use of drones. Under President Obama, the United States even expanded its interpretation of the authorisation of the use of military force to include broader authorities to strike other groups affiliated with AQ, including al-Shabaab, the militant Islamist group operating throughout the Horn of Africa.

For the United States, countering terrorism has witnessed both progress and setbacks over the past 16 years. President Obama acknowledged as much in a speech in December 2016 when he asserted that, while the US has made great strides against both AQ and Daesh, terrorism would remain a threat to the US for the foreseeable future. Indeed, the threat posed by Salafi-Jihadists specifically, and terrorist groups more broadly, continues to pose a range of challenges for the US across the globe.

For the United States, countering terrorism has witnessed both progress and setbacks over the past 16 years.

The Trump administration is attempting to keep pace with terrorist abilities to adapt to US countermeasures while maintaining a high operational tempo punctuated by aggressive counter-terrorism strikes. However, the United States still lacks a broader strategy for conflicts in which it is engaged, including both Afghanistan and Syria, meaning that the Global War on Terror continues on in perpetuity. In short, counter-terrorism itself has supplanted a more comprehensive US grant strategy, which is myopic and counter-productive in the long term.

Continued reliance on unmanned aerial systems, special operations forces and a limited military presence can be expected. One major question is whether Trump, who has been critical of Obama's handling of Daesh, will change the role of the US military in Iraq and Syria from "advise and assist" to full-fledged combat operations. Another open question is whether the United States will be able to increase its leverage in Syria to play some kind of meaningful role there in a potential post-conflict reconstruction scenario, or whether a political solution will be dominated by Russia, Iran and Turkey, while the US remains on the sidelines. Few countries are as tactically proficient as the United States when it comes to counter-terrorism but, without question, Washington has struggled to translate counter-terrorism success into strategic victories.

Q
Is the US CT strategy suitable for emerging, unconventional (such as CBRN and cyber) threats?

The United States counter-terrorism strategy is better suited to deal with threats external to the homeland, as it is more offensive than defensive in nature. No gaps in US CT strategy are more important than those relevant to the responsibility to prevent CBRN and cyber-terrorism. Of the range of possible WMD-attacks, of particular concern is bio-terrorism, for several reasons. First, there is an increasing availability of "bio-chem" agents. Second, the United States Government retains only limited means to control this science, market and industry. Third, there is a desire among some terrorist groups like AQ and Daesh to commit the most lethal attacks possible, and these groups are not limited by norms that might give other groups pause before committing an attack generally considered 'beyond the pale' – the attacks of 9/11 proved this nearly two decades ago. Fourth, and finally, there is the danger of contagion and the difficulty associated with detecting and preempting preparations for attack, since these conspiracies can involve lone individuals or small cells of terrorists.

While AQ, Daesh, or a lone-actor motivated by Salafi-Jihadist ideology might attempt to conduct a CBRN attack, there is also the possibility that a terrorist group or cult with apocalyptic views could be motivated to do so. Because so much of the focus in the United States has been dedicated to Sunni terrorists, there is a blind spot when it comes to right-wing extremists and other individuals and groups that could engage in political violence. Still, it is important to recognise that the difficulty of preparing and conducting a CBRN attack and the consequences of an attack, vary dramatically among different types of weapons. In terms of cyber, there is less of a threat from terrorists conducting a cyber-attack against critical infrastructure than there is from terrorist groups harnessing social media and encrypted communications to enhance their ability to recruit, fundraise and spread their propaganda online.

An attack using a chemical weapon like sarin gas or chlorine is perhaps the least difficult to pull off. An attack using a radiological device or 'dirty bomb' could result in substantial casualties, but would be difficult for a small group to assemble. Accordingly, the bigger the group and the more elaborate the preparation, the greater the chance of detection. Acquiring, much less building, a nuclear-fission weapon is for now something only determined nation-states can do, though it cannot be ruled out that a nefarious nation-state would arm and instruct a terrorist group, even if the odds remain miniscule, for a number of reasons. A terrorist attack using biological agents, however, could be planned, implemented and executed by a relatively small group. The fall out could be disastrous, particularly considering the difficulty of containing the second and third-order effects, including psychological impact and public health emergencies.

Q
What do the next three years of Islamist extremism look like in the West?

The threat of Islamist extremism in the West over the next three years will be driven by the continued collapse of the Daesh Caliphate. Even though the main objective of the Coalition to defeat Daesh was targeting and effectively defeating it, the degradation of a terrorist organisation can lead to organisational fractures or splintering. As such, thousands of Daesh fighters from the West could move to other battlefields, with a small portion seeking to return home to their countries of origin in Europe, North America, Australia and elsewhere.

Dismantling Daesh is a necessary strategic objective, but policymakers, Government officials, and military leaders must also be prepared to deal with splinter groups as they emerge in the aftermath of what seems to be a relatively successful campaign against the parent group.

While causing Daesh to break apart might seem like a positive outcome – it is a double-edged sword in the truest sense, clichés aside. The fracturing of Daesh could lead to the emergence of new, and in some cases more violent and operationally capable, splinter organisations. Dismantling Daesh is a necessary strategic objective, but policymakers, Government officials, and military leaders must also be prepared to deal with splinter groups as they emerge in the aftermath of what seems to be a relatively successful campaign against the parent group. With Daesh, these splinters could form their own, new organisation, or be absorbed into existing franchise groups or affiliates from North Africa to Southeast Asia. The follow-on franchise groups could ultimately develop to be highly operationally capable and focused on attacking the West, as we have seen before with the evolution of AQAP in Yemen.

Daesh's ability to plan and execute attacks, against both conventional and unconventional forces on the battlefield, as well as abroad in Western cities, makes it a relatively unique organisation in terms of its operational capabilities. Its fighters have mastered a diverse array of tactics, from vehicle-borne improvised explosive devices (VBIEDs) to ambushes and hit-and-run attacks. Moreover, the leadership's exhortation for its followers to conduct attacks abroad, including so-called vehicular terrorism or ramming attacks, is a tactic pioneered by Daesh that has emerged as a new trend in terrorist attacks directed at the West. There is no reason to believe that these attacks will diminish and, indeed, they may increase in frequency as Daesh becomes less relevant in the Middle East. To remain relevant, as Daesh loses its last remaining territory in Iraq and Syria, it may seek to rely on launching spectacular terrorist attacks in the West to maintain group morale and burnish the group's brand.

Daesh's unique contribution to tactical evolution has been impressive. Daesh has pioneered the use of the virtual planner model for external operations. This innovation allows terrorists in one location to direct attacks in another part of the world with only an Internet connection and reliable encryption. In many cases, jihadists can leverage local criminal networks that act as facilitators to help acquire the logistics and resources necessary for an attack. Even as Western nations have devoted substantial resources to countering this threat, savvy tacticians within the global jihadist movement will continue to rely on encrypted online messaging applications to identify local recruits and provide them with directions and technical expertise to attack targets, a development that poses a formidable threat to countries with less than adequate military, intelligence and law enforcement capabilities. The devastating Paris November 2015 attacks could serve as the model operation from the terrorists' point of view.