CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

Terrorism and Technology

Dr. Afzal Ashraf
Dr. Anastasia Filippidou

Terrorism and Technology

By

Dr Afzal Ashraf and Dr Anastasia Filippidou

Intentionally left blank

Table of Contents

Executive Summary

This paper was commissioned by the Centre of Excellence, Defence Against Terrorism to provide defence and security officials with an understanding of the relationship between terrorism and technology. It considers how technology is used by terrorists to provide an understanding of the processes and factors which drive terrorist innovation and the use of specific technologies. The range of technologies currently used in, or being developed for CT, was explored. Current technological trends were evaluated, along with other factors, to inform recommendations for more effective and efficient CT technology.

The current approach to understanding the terrorists' use of technology is an instrumental one. This approach responds to terrorists' use of technology and attempts to maintain a CT advantage through innovation, including through government funded R&D. An approach which considers also the symbolic, ideological and organisational factors affecting terrorists' technology choices can provide a valuable insight into terrorist groups as well as providing a predictive capability. Using this approach, it is possible to predict, for example, that terrorists are likely to:

- Make more use of drones, particularly to assassinate high profile individuals, to assist with coordination of a complex 'marauding' style of attack and in 'swarming' formations with small explosives to create confusion and panic
- Use 3-D printers to manufacture weapons inside security cleared areas and to produce replica objects to hide IED
- In some cases, groups will make a greater effort to acquire weapons of mass destruction, likely with insider help

This predictive approach can build on the current success of the Attack the Network (AtN) approach adopted by NATO and other countries at the operational level by adding strategic insight to better direct CT technology investment and intelligence efforts. The AtN approach could further benefit from technological developments in:

- Big data analysis supported by artificial intelligence
- Information fusion of social media intelligence with other forms of intelligence.

This highly data driven environment will require greater investment in equipment and human resources to store, analyse and action vast amounts of information in a timely fashion.

The challenge of developing and deploying suitable CT responses in a rapidly changing technological landscape requires a greater:

- Investment in research and development
    - The costs of these necessary investments can be mitigated by greater burden sharing, especially in technology development, between organisations and countries.
- Training and joint operations between the military, Police and intelligence agencies as well as with other government and international organisations.
    - Technology is already making an impact on more realistic CT training, but there is scope to further exploit its potential
- Any standardisation of data formats to allow quicker sharing of network diagrams between nations

Most equipment and capability advances arise out of the integration of discrete technologies. For example, developments in nanotechnology have triggered improvements in sensor technology and power system efficiencies. Other advances have allowed significant performance improvements in some old ideas, such as airships.

The full benefit of the rapid advances in CT technology cannot be realised without an equally agile procurement, legal and safety governance framework. Otherwise, terrorists will seize and maintain the initiative.

The investment in technology development, acquisition and the people to maintain and exploit it could lead to a technology 'arms race' where the terrorists have an asymmetric advantage over states. Consequently, strategies will need to be adopted which appropriately balance investment to the risk as well as balancing investment in CT with wider defence and security needs.

The importance of the link between technology and terrorism, the centrality of terrorism to current defence and security and the rapid evolution of both technology and terrorist techniques requires a change in military culture to think differently about the threat and to work differently with other CT organizations to counter it. Wide ranging education and training initiatives exposing the various issues relating to terrorism and technology can help achieve the new approach and cultural change needed to improve CT effectiveness.

Several recommendations are made based on the findings and conclusions of this research.

Chapter 1 Introduction

Technology has shaped and defined terrorism throughout history. From the dagger of the Zealot Sicarii, a Jewish terrorist organization from around 50 AD, to the current employment of improvised explosive devices delivered by increasingly diverse means including aircraft, it could be argued that terrorism has become more potent as technology has become more advanced. Counterterrorism (CT) has similarly relied on technology to fight terrorism.

Advances in technology, changes in global politics and other factors have meant that terrorism now plays an increasingly prominent role in warfare. Terrorism is a component of irregular warfare, which in turn is seen as a feature of asymmetric warfare. Conflict has become increasingly asymmetric meaning that terrorism is a far greater defence and security threat than before, requiring far more effort on the part of conventional forces to understand and confront the threat.

Technology has been an integral part of the military sciences for hundreds of years. It is one of the largest component in defence budgets. Figures for equipment spend by the UK and USA stand at around 23% and 25% respectively of the defence budget, second to expenditure on manpower, which is over 36% for both countries.[1] While equipment expenditure may include items not normally classified as technology, such as clothing, manpower costs may include training which may involve technology expenditure. Studies which segregate expenditure further indicate that the transatlantic expenditure by the US on both equipment and operation and maintenance (O&M), which should collectively include the total cost of ownership of technology, is significantly higher than personnel costs.[2] Similar figures for CT expenditure are not available but it would be reasonable to assume that technology will account for a large proportion of the costs. Consequently, it is surprising that the subject has received relatively little attention so far.

There is a difference in the way technology is used by militaries in war or in CT to the way it is used by terrorists. While conventional forces use technology in an instrumental manner to find and target terrorists, the terrorists use technology mostly in a symbolic manner, to coerce and deter through deliberately graphic acts of horror. The significance of technology and terrorism, therefore, deserves greater understanding by those responsible for military decision making.

Aim and objectives of the research

This paper aims to provide defence and security officials with an understanding of the relationship between terrorism and technology. It briefly addresses how that relationship developed before considering how technology is used by terrorists and finally explores the broad spectrum of technologies currently used or being developed to assist in CT. The research underpinning the paper evaluates the current technological trends of terrorists and provides an understanding of the processes and factors which drive terrorist innovation and the use of specific technology. This is necessary in order to be able to form effective and efficient CT measures.

This paper examines questions such as: what types of technology have terrorists preferred up until now; do terrorists use technology in a reactive or a proactive manner; are there factors that allow the prediction of future use of technology by terrorists; what do trends in terrorist innovation indicate for the future of terrorism; what have been the main global trends in terrorists' technological approaches and methods. Current technology and trends in technological development are considered in terms of how the terrorist threat may evolve and CT might also develop in response.

Research Context and Structure

The CT domain can be divided into domestic and international. While arrangements vary between countries, the primary responsibility for domestic CT usually rests with national Police services with the military, usually special operation units, being tasked with a supporting role. This is because some countries, such as Germany, legally preclude the military being used in domestic security and also because the emerging trend in terrorism is away from prolonged hijacking and hostage

taking situations to rapid mass attacks, such as the November 2015 attacks in Paris.[3] In such circumstances it is difficult for military units to respond in most urban situations and so, increasing the Police conduct the initial response. Military forces then act to stop terrorist attacks and actions by either kinetic engagement of terrorists or the rescue of hostages. Occasionally, at times of high threat, conventional military units are deployed within their own countries to augment the Police as a visible deterrent to attacks and to provide public confidence.[4]

In these scenarios the Police and military are supported by intelligence agencies. This convergence of roles and the increasing need to work together means that equipment and training requirements also converge between intelligence agencies, Police and the military. While this study only considers CT and associated technologies primarily from a military point of view, it is important to recognise the considerable advantage in greater joint operations and burden sharing in development, procurement and training between military and civil CT forces. The study unearthed few cases where this is taking place, indicating much untapped potential for efficiency and effectiveness in technology procurement and use.

When NATO forces are deployed internationally in peacekeeping roles, in combat, or in stabilisation or state building operations, they can be subject to a terrorist threat and so may need to conduct CT activities in their area of operations.[5] Even when legally CT is not part of their mandate, NATO forces can assist the host nation, with training, equipment and other support. In such situations, they are frequently the primary target for terrorists and therefore NATO forces need to maintain a significant organic CT capability, including the ability to rapidly interface with host and own nation intelligence and policing resources. This requires adaptable communications and information technology (IT), a challenge that continues to be only partially met due to the absence of standardisation in what is a largely commercial supplier base, the rapid evolution of technology and the procurement preferences of individual nations. Improvements in these areas could greatly improve NATO's CT capability.

Context: Terrorism Trends

In the West, there has been an overall decline in the number of recorded terrorist incidents over the last quarter century, although there has been an increase in the average number of casualties in those fewer episodes. This contrasts with the global trend, where both the number of attacks and casualties have been raising. The number of countries affected by terrorism is also increasing.[6] There are many reasons behind this trend, including the constant quest of terrorist groups for attention, the proliferation of ideologically motivated terrorist organizations, as well as the development of new means and the increasing sophistication of professional terrorism.[7]

The use of technology by a terrorist organization depends on internal and external factors. Internal factors include, but are not limited to, the strategies, tactics, methods, structures and typology of the organization. External factors lead a terrorist organization to adopt specific technologies. These include effectiveness of counter-terrorist measures, imitation of other terrorist organizations, accessibility to new technology and resources. Often, external and internal factors overlap, complicating an in-depth analysis of the use of new technologies.

For terrorists, the process of and the way in which they achieve an outcome can be as important as the end result. Consequently, the type of technology used in terrorist attacks can acquire an importance and, as such, technology can form part of the identity of the terrorist organization itself. However, this elevated role and importance of process poses the additional challenge that the selection of technological means is not the result of purely rational behaviour, which in its turn makes it even more difficult to predict and anticipate an organization's behaviour and actions.

Owing to the high security risks and the secretive nature of terrorism, in general terrorists appear to be conservative in their technological choices. They appear to use and improve existing dual-use technologies. In this sense technological innovation for terrorists is a result and a response to existing technologies, which Rosen calls 'technology push,' where advances in civilian technologies drive and push military innovation. This is in opposition to the 'demand pull,' where military innovations have, until recently, driven advancement in civilian technologies.[8]

As already mentioned, terrorism plays an increasingly prominent role in contemporary conflicts and as such it influences military operations. Terrorism is becoming increasingly global in its impact, not just in terms of attacks against Western citizens and infrastructure, but also in terms of influencing a huge displacement of populations from North Africa, the Middle East and South East Asia to Europe and North America. These by-products of global terrorism have begun to have a greater political and economic impact on the internal politics of NATO nations. There is a noticeable rise in extremist politics which, in turn, threatens cohesion and internal security within NATO member states and the Alliance as a whole. Collectively, these trends underline the need for more effective CT capabilities within NATO and partner nations, with technology playing a large part in achieving greater effectiveness.

Importance of the Research

The link between terrorism and technology has long been made and, in a general way, explored. For example, Martha Crenshaw identified trends such as improved transport and communications in the form of Russia's new rail system, without which the Narodnaya Volya would have been unable to attack the Tsarist state. Similarly, the Popular Front for the Liberation of Palestine could not have gained international attention through the tactic of hijacking, had it not been for the development of the commercial airliner.[9] Most assessments of future terrorism trends also forecast the significance of technology in its evolution.[10]

However, there appears to be little research exploring the relationship in detail and looking at how technology can be developed and deployed in effective counterterrorism. That is not due to a lack of recognition of its importance. The UK government acknowledged in 2013, that, 'We remain concerned about the use made by terrorists of new technologies and want to continue to invest in our own science and technology programmes to ensure we have adequate counter measures in place.'[11] The emphasis is on researching technologies and associated solutions rather than on researching CT technology as a subject in its own right.[12]

Research in this area tends to be funded through associated budgets rather than dedicated ones. For example, defence, scientific and research organizations in many countries contribute to CT related R&D. Various intelligence organizations also conduct R&D of equipment and techniques, which often have a dual purpose of supporting national intelligence and CT.

Various commercial suppliers conduct their own research and development to support the expanding defence and civil policing CT market.[13] This commercial investment is a welcome initiative in reducing the burden on nations' defence budgets, but it does not necessarily produce value for money. Those corporations which invest in CT related research and development (R&D) tend to charge a premium for their products when these come to market, given the relatively small size of the market.

Another factor is that those national organizations which invest in CT R&D have tended to spend more of their time and budget on activities which support current operations than on future technology to counter upcoming threats. This is to be expected to an extent, but in a CT technology strategy, as in any strategy, a proactive approach which anticipates threats and opportunities rather than reacting to them is likely to be more successful.

National Approaches to CT Technology Development

The national strategies, structures and resources for CT related technology R&D vary considerably between states but some trends have emerged as countries attempt to adapt. Analysis of how some key countries are adapting reveals that Canada and the UK, and to some extent, the US, are integrating what were once '*niche Defence S&T [science and technology] capability into national S&T programs for counter-terrorism and national (or homeland) security.*'[14] This is happening in parallel with a prevailing view that defence S&T is a critical component of the national response and not just for defence needs. Other trends and perceptions include:

a. Greater alignment of national policies and strategies on innovation and S&T between defence and national security,

b. Growing acknowledgement of the critical national role of niche defence S&T capabilities

c. More strategic coordination of national security capability management supported by national security S&T providers, including defence

d. Increasing effort in overcoming departmental stovepipes, particularly the military/civilian divide

e. More use of programmatic (or problem-based) approaches to funding development, management and exploitation of S&T in national security

f. More focus on cross-departmental collaboration, information sharing, and the promotion of enduring S&T 'communities of practice.'

These issues are largely being addressed at the national level and with limited success. Conceptually, the necessity and benefits of improved alignment, collaboration and coordination are widely accepted but organizations are slow to adapt for cultural and political reasons. The challenge is even greater at the Alliance level. NATO's own S&T organization has an ambitious approach to collaboration and research across the wide domain of collective defence but its activities are modest in the CT field with about 17 terrorism related past and present research programmes listed on its website.[15] Its 2015 Annual Report does not identify a single programme with direct relevance to CT, indeed the report does not use the word 'terrorism' at all.[16] Programmes included in it which intended to develop technologies to enhance situational awareness and augmented reality (AR) will, of course, improve CT capabilities. Also, it is correct that NATO should invest in research areas not covered by other entities and the commercial sector. Hence, for example, the justifiable prominence of maritime capability research in NATO's S&T plans. Moreover, CT is primarily a national responsibility and not a NATO core role and this may justify the lack of CT investment in NATO S&T.

However, as discussed earlier, modern combat invariably involves CT, at least in a defensive sense. Additionally, there is a call for NATO to expand its Special Operations Force's three current roles to a fourth one of CT, given that some member states lack an adequate CT capability.[17] As far as investment in technology is concerned, while some member states are making promising headway, it is unlikely that NATO sponsored R&D will make a significant contribution to CT in the near future. This is almost certainly a reflection of the reluctance of member states to sufficiently collaborate and contribute rather than that of the Alliance as a whole.

Collaboration and burden sharing in CT technology development seems to be impacted by cultural and economic drivers. Modern defence culture has evolved around the battle winning capability advantage of technology. As such, it is seen as a national asset and often guarded through secrecy. The highly lucrative defence export market also discourages technical cooperation due to fierce commercial competition. These factors have evolved in the defence environment but appear to have influenced the CT technology domain even though secrecy and commercial factors should have relatively less impact.

Limitations and Structure of the Research

This document does not aim to be exhaustive, or to offer solutions that will address all the challenges. Some issues have been left out as a result of a lack of time, space and appropriateness. For example, countering the threat from surface to air missiles to attack against aircraft, the threat to troops from mortar attack, the hardening of vehicles and buildings and explosive disposal are all areas excluded from this work. These, and similar areas of threat and protective measures, may be considered more an issue of conventional military conflict rather than being particularly confined to terrorism.

Many technologies used in CT are classified but this study will be restricted to discussing issues and associated technol-

ogies not covered by security restrictions. This is not a major limitation because increasingly, commercial off the shelf (COTS) technologies are being used by NATO forces. In many cases the technology and its ownership are not sensitive but only the details of performance and techniques of employment are issues of sensitivity. In such circumstances, the technology and its general area of employment can be safely discussed without encroaching on classified information. Care has therefore been taken to share information that is sufficiently relevant and detailed to be useful without compromising any security caveats.

In addition to a literature survey and web based research covering pertinent topics, a number of CT specialist units were visited along with associated S&T organizations, as part of the research. Unlike NATO's COE C-IED, which was also visited, most of these organizations are covert or semi-covert. Although much of what they do need not be classified, they have strict restrictions on access to the organization, their equipment and practices. Hardly any academic or public literature is available to reference their non-sensitive technology or their non-sensitive tactics or procedures. Consequently, some of these are shared in this document without reference, as contributions based on original research.

Chapter Two discusses the Terrorist Modus Operandi and examines the intrinsic link between the act, technology and message in the terrorist imagination and how that might help predict how terrorists may use technology. It considers terrorists' technology trends and ideological factors to expose further predicative possibilities. The chapter considers a number of typological factors and discusses how these might shape a terrorist group's use of technology and innovation. Finally, the exploitation of soft technology by terrorists to plan, implement, amplify and communicate their terror message is discussed. Chapter 3 outlines how technology is used in the various functions of CT. Chapter 4 explores some of the emerging technologies and the challenges associated with both existing and future technologies. Chapter 5 briefly summarises the findings and suggests fitting approaches for improving the approach to and development and use of CT technology.

Chapter 2 Terrorist Modus Operandi and Use of Technology

What are the factors that determine terrorists' approach to technology and innovation and how do they use technology? That is the primary question for this chapter. The importance of this question stems from the proposition that terrorism is about imagination. A pre-requisite to terrorism is the imagination of horror and of how an event or a number of closely associated actions can have a strategic impact through publicity. Understanding how terrorists imagine the combination of people, technology and actions to produce terror can allow CT practitioners to picture or predict what terrorists might do in the future.

Imagination and Prediction

This prediction cannot be in terms of where, who or when terrorists might attack, but how and what they might do. This claim is based on the fact that a terrorist ideologue, Karl Heinzen, who Walter Laqueur described as modern terrorism's '*great visionary,*'[18] imagined and attempted to inspire a number of technology based attacks a century and a half ago.[19] Heinzen imagined attacks and wrote about them. In his highly evocative short book, 'Murder and Liberty', he makes a vivid case for revolutionary violence based on terror. He concludes the book by asking his reader to imagine a number of newspaper headlines. The first is a report of an explosive attack on a train carrying the German Royal family. The second report claims that guerrillas had developed a projectile which when fired at a target, sprays a rain of poison shot. In the fictional incident, the shot resulted in the death of fifty of the German Emperor's men. The deployment of 'bomb-like shells' placed 'beneath the pavement unknown to the enemy' is described in the third fictional news report. The 'newspaper' describes the fictitious successful use of the technique by revolutionary terrorists against the army in a remarkably prescient manner, given the events in Iraq and Afghanistan involving Improvised Explosive Devices (IED). The fourth imaginary report describes assignations of key figures in churches using air guns firing poisoned bullets. The final report describes the bombing of Louis Napoleon's palace using a time bomb which killed his entire court.

Almost all of these attack methods were adopted approximately a hundred years later by terrorist groups who had never heard of Heinzen or come across his writings. This was because they, like Heinzen, thought about terrorism from first principles. Following the terrorist logic of creating maximum horror with minimum effort, facilitated by the creative possibilities of technology and magnified by the increasing reach of the media, they arrived at similar conclusions. The case reveals that it is eminently possible to predict how terrorists might act and what they might do.

In the contemporary context, thinkers like Samir Khan and Anwar Awlaki, who produced Al Qaeda (AQ) in the Arabian Peninsula's (AQAP) Inspire magazine, thought and wrote in the same way as Heinzen. They offered suggestions on 'How to Make a Bomb in the Kitchen of your Mom'[20] and to use vehicles to mow down pedestrians. Unlike Heinzen, the Inspire magazine had an existing global readership. For instance, one idea suggested in the magazine six years earlier, the mowing down of pedestrians using a vehicle, was put into practice with horrific consequences in Nice, France, in 2016.[21]

Unlike Heinzen, AQAP understood the power of CT and so they developed other methods in secret. Research and development was conducted in low signature explosives and associated detonation mechanisms. These were deployed in the Detroit underpants bomber plot,[22] the printer cartridges plot[23] and the Prince Nayef assassination plot.[24] The fact that none of these were fully successful owes more to good fortune than to a failure of planning or possibility.

Suicide and the Desire to be Mad

For Heinzen the most glorious killing is suicide. It is the ultimate act of violence and devotion to the cause by an individual, especially if it is in response to '*disgrace that would destroy his character*.'[25] This acceptance of the idea of self-destruction and the need to create greater terror with fewer deaths allows easier acceptance of the idea of what Conrad refers to as any '*act of destructive ferocity so absurd as to be incomprehensible, inexplicable almost unthinkable; in fact, mad?*'[26]

This mind-set transcends time, technology and culture. It has been found in the innovation of suicide bombing by the Liberation Tigers of Tamil Eelam (LTTE), in AQ's Awlaki and Khan authored Inspire magazine and in the actions of Mohamed Lahouaiej-Bouhlel, who drove a lorry into a crowd celebrating the Bastille Day holiday on 14 July 2016 in Nice, France, killing 84 and injuring many more. Understanding how a terrorist mind links the lust for horrific mediagenic violence with the power of technology can help CT practitioners predict what terrorists might do. The relationship between terrorist thinkers and actors also shows that most new techniques will have been written about before they are put into practice. However, limitations of time, funding and R&D facilities will drive most groups towards a conservative approach, using mostly existing technology and techniques.

Terrorism and Technology Trends

Two trends appear to emerge in terrorism and its use of technology. On the one hand there are those who advocate that terrorists always seek new technologies in order to be 'a step ahead' and to enhance the lethality of their attacks.[27] On the opposite side of the spectrum, there are those who argue that terrorist organizations are conservative in nature. Consequently, according to this school of thought, the use of technology is reactive and not a proactive approach. As Hoffman argues '*on the technological level, terrorist innovation takes the form of novel methods of weapon concealment, as opposed to adoption of new weaponry per se'*.[28] However, both trends hold true depending on the situation and the specific case, but also both schools of thought have their weak points.

A terrorist group will use technology in order to maximize its successes and benefits. On the whole, terrorist groups with clear aims and objectives and with a sense of urgency to attain their goals within their lifespan are likely to demonstrate a high level of technological innovation. This is because such organizations are generally more inclined to constantly improve their technological capabilities until they find the most fitting mode that will yield the desired results.

Ideology, Rhetoric and Technology

Some analysts confuse resistance to 'westernization' with resistance to modernity and globalization. As Kagan posits '*the forces of modernization and globalization have inflamed the radical Islamist rebellion and also armed them for the fight*.'[29] A detailed ideological analysis indicates that western cultural and political domination motivates Islamist[30] extremism rather than modernity or globalisation. Modernity and globalisation and the intimately connected advances in technology, have facilitated more than caused the growth of terrorism. Indeed, Demir and Varlık are persuaded that there is a direct correlation between '*boosted globalization, weakened nation-states and globalized terrorism.*' For Demir and Varlik '*contemporary terrorism is global in nature since it uses advantages and exploits vulnerabilities of globalization and creates global effects*.'[31] As such, in many ways, '*the contemporary wave of terrorism is a vicious by-product of the new environment*.'[32]

Political power subordinates theological and cultural aspirations in global so called jihadist decision making. Consequently, these terrorist groups repeatedly show themselves willing to act contrary to their own beliefs in order to increase their chances of success. For example, many extremist Islamist organizations initially opposed the idea of using women for suicide operations, but necessity made them adjust this belief to reflect their needs in order to achieve their goals.

Superficially, AQ's ideology, which is virtually identical to ISIL/DAESH' ideology, may be seen as conservative and overly traditionalist, rejecting modernity and globalization. However, deeper analysis indicates that AQ is based on a modern ideology[33] which exploits mythical interpretations of religion and history to motivate its primary recruitment pool.[34] AQ's strategic framework is informed by Western thinking and so it reaps the benefits of Western technological advances in order to attack the West. As a former AQ member argued '*the 9/11 attack was like taking the enemy's finger and poking it into his own eye*.'[35]

This stance is not irrational when seen from AQ's point of view. It is both pragmatism and an important element of the symbolic communication, which is essential to effective terrorism. The use of Western technology by AQ and ISIL/DAESH's,

such as aircraft and visual communication including filming and publicising attacks are a genre popularised by General Schwarzkopf during his Gulf War 1 briefings for international TV. These appear to have inspired similar video commentaries by terrorists of their attacks. Following news footage of AQ prisoners in the Guantanamo Bay prison dressed in orange jump suits, Western hostages of AQ and its affiliates were also shown in their propaganda videos similarly dressed in orange. These are all examples of 'reflective rhetoric'[36] and are inspired by the subliminal desire of terrorists to respond to the West's perceived strengths in symbolically similar ways in order to claim parity in power.

Empirical research confirms that in most cases there is a combination of several variables which provide the necessary impetus to adopt a specific technology. In general terms it is clear that technology is both a reactive and a proactive tool in the hands of terrorists. Their propensity to employ reflective rhetoric through technology provides CT forces the potential to predict likely future terrorist use of technology based on some of the prominent technologies and techniques being used against terrorists.

Group Typology and Approach to Technology

The typology of terrorist groups defines its modus operandi and consequently provides, at least partially, a sense of collective identity. Their typology is key in identifying the enemy and in providing the necessary justification for targeting. The particular type of an organization determines its aims as well as prescribing how and by what means these aims can be attained. The nature and type of an organization has an important role on the sort and amount of technology used. Moreover, the type of a terrorist organization also determines the group's perception of urgency for any armed action.

Group Raison d'être

If the raison d'être of a terrorist organization is to correct an injustice – perceived or real – instead of changing the world order, it is likely the organization will prefer limited or proportionate violence with more discriminate attacks. As a result, it is unlikely that such an organization will use unconventional weapons or will aim to cause mass casualties. A characteristic example of this is the 11 March 2004 attacks in Madrid. The then Spanish government quickly pointed the finger at Euskadi Ta Askatasuna (ETA). However, many experts doubted that a pro-independence ethno-nationalist organization which sees itself as correcting an injustice, would resort to attacks that cause mass casualties. The experts were correct. It subsequently became clear that the attack was inspired by AQ in response to Spanish military involvement in Iraq.

The amount of violence a group is likely to exert in terms of casualties and geography is linked to the degree of its territorial ambitions. A group with a totalitarian global ideology will have unlimited constraints on its use of violence. It will consequently employ all available technology to achieve its aims.

Operational Approach

The use of technology by terrorist groups is driven by the need to achieve the necessary capability to reach and sustain the level of intensity preferred by the specific terrorist group. Operational preferences are reflected in a group's overall ideology and typology, and a shift in organizational goals can also lead to technological modifications.

The Shining Path organization in Peru adopted Mao's model of '*numerical inferiority at the strategic level but a numerical superiority at a tactical level,*' which translated into an operational preference of quantity.[37] To this end the priority became the launching of as many attacks in as short a time frame as possible, irrespective of the effectiveness of their military outcome.

The type and ideology of an organization in combination with its accessibility to resources may lead an organization to choose a narrow and discriminate targeting approach. Groups with a nihilistic approach who claim to be fighting an existential struggle will favour an indiscriminate targeting tactic, and as such they are more likely to engage in a process of innovation in order to obtain a means of indiscriminate and of mass casualty attacks. The more extreme and apocalyptic the

ends of an organization are, the likelier that an organization will try to obtain mass-casualty capabilities such as chemical, biological, radiological and nuclear (CBRN). Consequently, the more indiscriminate the tactics of a terrorist organization, the greater the group's inclination is to technological innovation.

The Challenge of Accurate Targeting

A factor working against this logic is the rise in the likelihood of collateral damage or mistaken targeting by groups who aim to avoid indiscriminate casualties. For example, the Taliban are forced to use high explosive pressure plate activated IEDs to destroy coalition or government armoured vehicles. These groups try to use technology to increase precision and target discrimination, but they usually end up ignoring the high risks to innocents in favour of the possibility of a successful attack against their intended targets. This often results in innocent civilian casualties either through unintended initiation or through collateral damage.[38]

Internal and External Dynamics

Further factors impacting on a group's approach are internal and external dynamics, as well the availability of resources. For instance, when an organization is engaged in 'tit-for-tat' frequent attacks, this reduces the need and ability of terrorists to innovate. Moreover, groups with territorial strongholds can operate and train more freely than urban terrorist organizations. This can make the former more willing and able to innovate than groups confined to urban settings where there is a high risk of detection. For example, an accidental explosion of a new device at an isolated stronghold of the FARC (Revolutionary Armed Forces of Colombia) while training and preparing for an attack is unlikely to endanger the existence of the whole organization. However, a similar accident for an organization like that on 17 November in Greece, which assembled their devices in city apartments, would cause a devastating blow to the organization and could prove fatal for the organization. To be able to use technology, the members of an organization need to be technologically aware.

Group Structure

The structure of a terrorist group also affects the methods and approaches used. The more centralized and the more hierarchical an organization, the more the use of specific means will depend on the leadership of the group. If the leader commands authority and if the leadership is pro-technology then they may be a key determinant for the organization's preference for innovation and the use of specific technologies. Decentralised, non-hierarchical group structures allow a bottom-up decision making approach, where individual cells would come up with their own operational decisions to be executed with leadership approval. Such structures allow for more innovative approaches and tend to be keener to exploit technology.

Current terrorist groups operate within a nebulous network which makes accurate detection of operational decision making more challenging. As will be discussed, the improving ability to rapidly map networks using CT technology can allow insights into the terrorist group's structure and hence its approach to technology.

Technical Expertise

The availability of expertise in an organization - from the bomb-making experts to the media specialists – can have a decisive impact on an organization's willingness and ability to innovate. Therefore, the qualitative as well as the quantitative attributes of an organization shape its technological innovative capability. A terrorist group may stick with the use of a specific weapon and technology as a trademark. The attachment of an organization to a particular weaponry or method of attack can confer an advantage in symbolism, for example, but at the same time, it can become a predictable indicator of a group's modus operandi. This allows for easier detection and identification of the group involved using techniques such as biometrics etc.

Inter-organizational Relationships

A terrorist group's relationship with other organizations can have an impact on the use of technology. When terrorist groups cooperate there is a sharing of know-how and of technological capability, giving the impression that the group is capable of an unexpected and rapid technological leap. This, in turn, may lead to an overestimation and overreaction of CT measures. The organization Jamaah Islamiyah, for instance, gained a high level of operational knowledge through training and operating with AQ personnel.

Relationships among terrorist groups who operate in the same environment do not only lead to cooperation but also can lead to competition and rivalry. This is because the combination of competition, and the constant pursuit of security forces may put pressure on each of these groups to improve and innovate technologically in order to demonstrate superiority over rival groups. For instance, the Popular Front for the Liberation of Palestine (PFLP) lacked a distinct ideology and had a relatively small membership compared to other Palestinian organizations. This led it to favour spectacular operations, disproportionate to its size and support base in order to acquire a distinctive group identity among its peers. This competition between organizations with similar ideologies and causes is common and is motivated by the need to be able to claim legitimacy and monopoly over 'the cause.' Technological innovation can, in this way, become the means of gaining a competitive advantage over their peers.

External Support

Further factors having an impact on the adoption of new or different technology are the level of support within the organization, within the broader community as well as external support. The expertise, availability and accessibility of financial material as well as human resources, facilitates the use of technology. The more resourceful an organization, the likelier it is to innovate and adopt new or different technologies. Research shows that state-sponsored terrorist organizations are, on average, eight times more deadly than groups which do not get such support.[39]

Effectiveness of CT Measures

Successful counterterrorist measures and target hardening efforts make previous terrorist tactics ineffective, forcing terrorists to innovate and adapt their tactics in order to overcome the countermeasures. To paraphrase Herwing, a precondition of innovation is a concrete problem which organizations have a vital interest in solving, and the key determinant of innovation success rests in the specificity of the problem, the solution to which would offer significant advantages.[40]

Many terrorist organizations respond to effective CT measures by shifting their attacks to softer targets rather than innovating and adopting new technologies. Some organizations, mainly for symbolic and psychological reasons, choose to use their technological capabilities to overcome governments' countermeasures. For organizations like the Provisional Irish Republican Army and AQ the overcoming of governments' CT measures has been a matter of prestige, which has an internal and external psychological impact. Internally it raises morale within an organization and reinforces commitment to the 'cause,' while externally it maintains the fear and uncertainty necessary for terror.

Soft Technology

Weaponisation of Narratives through IT

The media has been characterized as the oxygen of terrorists. They have utilized all media outlets to great effect. Terrorist organizations such as ISIL/DAESH and AQ appear to be exceptionally adept at utilising information technologies and the media to exploit global interconnectivity and the vulnerabilities of a less-flexible state-centric international system. Joseph Nye emphasizes the limitations now placed on governments and the importance of narrative, by arguing that '*traditional analysts would predict the outcome of conflict mainly on the basis of whose army wins. Today, in conflicts like the struggle against transnational terrorism, it is equally important whose story wins*.'[41] This point has been understood by terrorists throughout the ages.

This is why Heinzen asked his followers to imagine newspaper stories rather than the terror act itself. It is also why AQ and ISIL/DAESH produce speeches and literature to support their horrific acts. Terrorism is always a part of a narrative, the success or failure of which determines the success or failure of the group itself. The ubiquity of information today, with its instant and mass access, makes owning the narrative and managing people's perceptions a key approach for organizations like ISIL/DAESH with its trans-border aspirations.

Social media has been used by terrorist groups as a way of disseminating their message to a global audience, to raise or maintain awareness about their so-called cause but also in order to recruit new members. The use of Twitter and other social media has inspired a younger generation to join ISIL/DAESH and a sub group of those joining, estimated at 10%, are females who join to marry members of ISIL/DAESH.[42] According to Atwan 'without digital technology it is highly unlikely that Islamic State would ever have come into existence, let alone been able to survive and expand.'[43]

Many terrorism analysts overstate ISIL/DAESH' innovation in media exploitation because they see it in isolation of the very effective media operations of AQ, the Taliban and other groups who preceded and inspired ISIL/DAESH. Atwan's comments are equally applicable to the Iraqi insurgency of 2004-2009, which comprised a number of non-aligned Sunni and Shia groups.[44] The Internet provided a means of disseminating information which simultaneously acted to increase the groups' terror impact, its public relations, its ability to recruit and to disseminate know-how to individuals and cells not in direct or frequent contact with the core leadership.

ISIL/DAESH' main innovation has been in the exploitation of the new social media sites, through which it was able to communicate its message, manipulate its brand and set the benchmark for other terrorist groups to imitate. It has extensively used technology to communicate, to gather intelligence and to promote its cause. In this way, the organization demonstrates its capability to operate like many Western militaries, through their reliance on Information Technology (IT) supported networks, albeit militaries avoid the Internet for operational purposes in favour of intranets and other non-public IT systems.

Cyber as a Weapon

ISIL/DAESH has not limited its technological capabilities to social media but has sought to use its IT skills as weapons on what has been labelled, Cyber Jihad. More precisely, in January 2015 the 'Cyber Caliphate,' a group of hackers associating themselves with ISIL/DAESH carried out a digital attack on a number of systems run by the US Central Command.[45] This too is an example of reflective rhetoric in that ISIL/DAESH is well aware that many of its plots and personnel are detected and targeted through the US' formidable cyber intelligence and attack capability. The attack on Central Command was, therefore, an attempt to send a message of mutual vulnerability. This attempt failed because its success was limited to possible minor embarrassment to the USA, compared to the significant losses ISIL/DAESH has suffered as a result of the West's superior exploitation of cyber capability.

Exploitation of IT by terrorists is not at the exclusion of more conventional methods of communication, such as printed material. Examples are 'Inspire,' AQ's magazine and Dabiq, which is ISIL/DAESH' equivalent. In these, among other things, a reader can find clear instructions on how to manufacture a Vehicle Borne IED (VBIED). While these are designed to be printed, they are distributed almost entirely through digital means and largely read on digital platforms. Cyber is, therefore, an increasingly prominent dimension through which terrorist groups deliver their components of fighting power: physical, conceptual and moral.[46] The realisation that cyber space is an integral part of modern warfare, that it requires a defensive capability and that it is an operational domain alongside the traditional maritime, land and air domains, has progressively developed in many countries. It culminated in NATO in 2016 with the official recognition of cyber as domain.[47] In CT, more so than in state-based conflict, cyber is a battlefield in which all components of terrorist fighting power need to be confronted, ranging from the dissemination of 'know how' on constructing weapons to countering terrorist narratives.

Chapter 3 Technology - Current and Future use in CT

Intelligence – The Challenge of Big Data

Analysis and Assessment

Technology has had a transformative effect on intelligence gathering. In part this is due to the proliferation of social media and mobile devices. However, the global explosion of social media usage is generating 2.5 quintillion bytes of data every day.[48] To put this in context, IBM estimates that 90% of the data that exists in the world today has been created in the last two years alone.[49] This represents a vast storage of information available to anybody with Internet access. Increasingly sophisticated equipment and software allows easy and fast acquisition and analysis of information on a previously unimagined scale. Thus, the provision of intelligence to decision makers requires a new understanding to effectively employ this rapidly evolving area of intelligence and benefit from the advantages it can provide.

Non-state actors have exploited social media technologies as a major means of recruitment, propaganda and generating financial and human support. ISIL/DAESH, for instance, systematically employs social media extensively as its main effort in seeking to set and control the narrative surrounding its raison d'être and their modus operandi. Therefore, social media is now being monitored and information from it gathered and analysed to identify extremists from the information they post online. However, as Hulnick emphasized a decade and a half ago, there can be a gap between information gathering and its effective and efficient analysis.[50] That gap has increased since Hulnick's claim and continues to do so.

The sheer amount of information generated daily outmatches the ability of the intelligence sector to comprehensively analyse and to disseminate in a timely manner to the correct people to action. The challenge is gathering the necessary information from the openly available data and thus identifying relevant information and processing it into intelligence that informs and is exploitable. Olcott describes this as the signal-to-noise problem.[51] Still, this is neither a new problem nor is it restricted to digital information. In 1969 Croom warned of the 'virtual tidal wave of publicly printed paper' which posed a growing problem for intelligence services through an increased volume of material, together with the proliferation of means by which it was gathered.[52] As in the past, today's enormous datasets are well beyond the capabilities of human analysts to fully and accurately process, thereby risking insightful intelligence being lost in the vastness of information.

In order to deal with this, intelligence services have asked the private sector to assist in the R&D of technologies in data analytics to tackle this automation versus human processing challenge. More precisely, the CIA recognising that the pace in the commercial sector of innovation of data management was clearly surpassing that of the national agencies, in 1999 set up its own outsourcing company called In-QTel as a way to leverage the innovation of technology start-ups to address some of its own information weaknesses.[53] Of the 104 companies currently listed on In-Q-Tel's portfolio, 41 are researching and developing technologies in the field of advanced data analytics in an effort to help the US intelligence community to close the gulf between information gathering and analysis**.** The bulk of effort is going into developing technologies which are able to process vast amounts of data, through automated and intelligent machine learning, otherwise known as artificial intelligence (AI).[54]

Social Media

In 2012 following the explosion of social media David Omand, Jamie Bartlett and Carl Miller introduced the term SOCMINT (Social Media Intelligence) and argued that the pervasiveness of social media throughout modern life, in combination with the level of detail people were uploading in a public forum such as Facebook, presented an opportunity to establish a new intelligence discipline to join the already existing intelligence fields.[55] Twitter posts are restricted to a maximum of 140 characters, but Application Programming Interfaces (APIs) allow for the bulk processing of great volumes of the 'tweetstream' and therefore, offer opportunities for event or sentiment detection surrounding a specific issue.[56] Omand *et al* identify a number of potential opportunities that SOCMINT can offer to law enforcement agencies and public security, as well as for

the military.[57] For instance, passive bystanders in a conflict zone can become active collectors of information through the real-time uploading of accounts, photographs, and videos of what they are witnessing. However, SOCMINT is just a tool and as always the usefulness of a tool depends on how it is used.

Increasingly military operations take place in complex multi-actor conflict spaces which mainly involve stabilisation operations amongst civilian populations rather than conventional force-on-force engagements. Within this context, winning the strategic narrative and understanding the complex human terrain environment are key to successful operations.[58] All of this requires the continued development of the currently nascent SOCMINT CT capability.

Data Storage and Bandwidth

The quality of current and emerging sensors, the size of information databases and the increasing demand of command and control communication systems has meant a vast increase in the burden of data management. While there has been a significant increase in data storage capacity, particularly in memory miniaturisation, there is still a challenge in transmitting and real-time sharing of the increasing level of data being generated. This is largely due to bandwidth limitations in commercially available radio-frequency communications such as those used by cellular phones as well as satellite communications. The increasing availability of compression technologies, which are now applicable to video files, has to an extent, mitigated the challenge. Nevertheless, there is and will continue to be a need for CT dedicated communication and data transmission channels to bypass the limitations of civilian networks. A number of solutions are currently being used and others are in development. Some of these are discussed in other parts of this document.

The main point is that CT technology procurement strategies should invest in technologies which both reduce the data transmission burden and also those which increase data sharing capacities. The strategies should also pursue data sharing technologies or capabilities that have some spare capacity to allow for the inevitable demand of data hungry sensors and software applications.

Big Data and the Big Human Resource Challenge

Much of what has been discussed above: the ubiquity of Open Source Intelligence (OSINT), the challenge of interrogating a huge number of databases containing massive amounts of data and the dissemination of intelligence in a timely manner has come to be known as the 'big data' challenge. The effective exploitation of big data to yield valuable intelligence is dependent on IT with high processing capabilities and sophisticated analytical software. This software needs a highly refined system of discriminating between relevant and irrelevant data, accurate and inaccurate data, true and false information etc. While recent developments in AI go a long way to achieving these objectives, the fact remains that big data still needs human intervention before it can be optimised in the CT context. There is a largely unmet need for highly trained individuals who can assimilate, analyse and assess, with reasonable confidence and accuracy, the information being gathered through big data analytical tools. Greater still is the need for informed, visionary and skilful leadership in this emerging intelligence field.[59]

Exploitation of big data inevitably requires the rapid and accurate sharing of information with appropriate individuals and organizations to make effective use of it. This requirement increases when applied in an alliance or coalition context. The challenge becomes greater still given the ready availability of technology needed to fuse information from a variety of sensors with intelligence from a variety of national and international sources.[60] These, mainly IT software tools, can deliver a far richer and quicker intelligence picture than has ever been available but the development of human resources, skills and aptitudes to fully exploit them are being outpaced by the capability of the technology.[61]

Currently these challenges are being mostly addressed by NATO member states' intelligence agencies. However, NATO's 'Attack the Network' (AtN) approach in countering Improvised Explosive Devices (C-IED) already depends on OSINT and other data analytical tools to identify networks in order to identify and target suitable nodes. An expansion of this proven

approach is being proposed to encompass a broad counter threat network concept for NATO. The Joint Analysis and Lessons Learned Centre has termed this proposal Network Identification and Engagement (NIE), to be applied to all threats including CT, COIN counter proliferation, counter cyber threats etc.[62] Consequently the demand for suitably trained and skilled individuals will become more acute as CT and other defence tasks become more reliant on near real-time big data exploitation. Currently there is little concern in defence circles over the paucity of this human resource because it is a capability enhancer rather than a barrier to current levels of success in operations.

IED Threat and Technology

The IED is still one of the most prolific and devastating weapons used by terrorists. IED types are numerous and limited mainly by the ingenuity and intent of the bomber or organization concerned, as an IED is often chosen by those without a weapon of choice. The appeal of IED as a mode of attack is that it gives the user 'value for money' and disproportionate success against more sophisticated and well prepared forces. The cornerstone of IED is technology and it distinguishes a capable group from a less capable one.[63] The effectiveness of an IED depends on the environment, access to finances, technology and key materials, know-how, and opportunity. Lethality of the main charge is often linked to technological expertise of the bomb maker. Higher scientific investment and access to key materials, therefore, equates to additional opportunities to target forces with a higher likelihood of success, resulting in serious injury and death.[64]

Highly trained and technologically advanced forces can struggle to defeat less capable forces because traditional modes '*do not work against such adversaries, as they tend to be less or not at all concerned about their physical well-being...*'.[65] In general an IED is cheap to produce, often consists of everyday items and requires minimal skill. In Iraq and Afghanistan, for example, terrorist groups effectively capitalised on the use of low-grade weapons, especially IED, in order to mitigate the relative advantage of their technologically superior adversaries. The Middle East is the epicentre of IED use, and the so-called IS is currently the most committed group utilizing IED. However, Al Qaeda in the Arabian Peninsula (AQAP) operating principally out of Yemen, Al Qaeda in the Islamic Maghreb (AQIM) operating in North West Africa, Boko Haram in mainly Nigeria and Al Shabaab in East Africa, all manufacture and deploy relatively crude IED.

Effective Counter-IED (CIED) is consequently a high priority for many forces operating in these regions. Several sophisticated detection devices ranging from refined versions of traditional metal detectors to vehicle mounted radar sensors have been developed and used with considerable success. However, technology tends to be effective against technology. Unsophisticated IED are less easy to detect with high tech solutions. For example, terrorists using electronic triggers can often be defeated through jamming but those who use simple wooden soleplates to trigger an IED can be amongst the hardest to detect and defeat. This has forced the development of the AtN approach which focuses on all levels to defeat IED systems by attacking the terrorist human networks, defeating the device, and preparing the force.[66] Although coordinated CIED is vital, the additional challenge is that each IED threat is unique to a country or a group. The complexities of CIED dictate the need for coordinated and inter-agency cooperation within and between states.

CBRN

Chemical and Biological Weapons

The use of chemical and biological weapons in terrorist attacks is nothing new.[67] As early as 1000 BC the Chinese used arsenical smoke. The ancient Greeks, Romans and the Zealots Sicarii all employed a primitive form of chemical or biological warfare. So far, modern terrorists have not utilised Chemical, Biological, Radiological, Nuclear (CBRN) weapons to the extent predicted and feared. The fear arises because the threat of such attacks has a disproportionate psychological impact on the public.

The main non-state groups to have caused casualties by such means are Aum Shinrikyo in Japan and the mysterious an-

thrax letter mailer in the USA.[68] Aum Shinrikyo, an apocalyptic cult, launched a sarin attack on the Tokyo subway in 1995 in which twelve people died and over a thousand were injured.[69] Even though Aum Shinrikyo was a wealthy organization with an estimated $1 billion in assets and a number of university-trained and experienced chemists and microbiologists within its membership, it had limited successes. Attempts by insurgents in the Middle East conflicts to use easily available chemicals such as chlorine in combination with conventional explosives have had even less success in terms of casualties.[70]

As an aside, it is worth considering that part of the failure of the Aum Shinrikyo attacks was due to the measured reaction of the Japanese government and media to the number of casualties and the shock use of a nerve agent. Had the media reacted more sensationally, as has sometimes been the case in Europe, Aum Shinrikyo and other groups may have been tempted to repeat or improve on their attempt. It is therefore important to remember that it is not just technology that limits terrorists' ability to achieve the success they crave, it is also the public response to their attempts, however unsuccessful, that will likely determine the degree of success that terrorists can claim.

The point to emerge from terrorist use of chemical and biological weapons so far is that even if they manage to obtain suitable material, terrorists still have to develop appropriate delivery systems effective enough to produce mass casualties. Also, it is important to not over react to any attempted attack so as to not grant sensational publicity, which is the objective of the terrorists.

Despite the relatively limited successes of chemical and biological (CB) attacks, CB capability remains attractive to terrorist groups. On the one hand, the acquisition of CB materials can be comparatively easy due to the wide ranging peaceful applications of these agents and materials. Once obtained, detection by CT forces can be difficult because of the nature of some agents. Groups or individuals can acquire CB weapons by stealing them or manufacturing them. However, to put things into perspective, to steal high-end CB, suitable for producing weapons and appropriate delivery systems, has proven quite difficult, as these materials are invariably secured.

Even if groups and individuals get their hands on suitable chemicals, empirically it is evident that they would struggle to successfully assemble high-end nerve agents. Keeping the precursors of nerve agents, for example, separate for a variety of security reasons, is necessary but not easy. Furthermore, the individuals need to have the necessary expertise to build CB weapons safely without killing themselves. In reality however, the handlers do not always have the necessary knowledge of what exactly they are using. Also, effective use of CB depends on where and how they are targeted. Things are different though, if terrorist groups choose to use low-end biological weapons, such as anthrax, which are easier to obtain and deploy. Therefore, terrorists tend to be drawn to low-end basic CB weapons.

Nuclear and Radiological Weapons

Acquiring nuclear materials is not as easy as chemical, biological and even radiological agents. Obtaining, for instance, highly enriched uranium fortunately remains a challenge for most non-state actors. That has not stopped certain organizations from making efforts to manufacture 'dirty' bombs, which involve using conventional explosives to disperse radioactive material. In one alleged plot, Jose Padilla and Binyam Mohammed planned to detonate a dirty bomb in a US. city, by stealing uranium from a passing truck and then enriching it by swinging it around in a bucket.[71] While the method was inspired by a hoax posting on a website and would not have worked, the mere fact that it was even accessed by extremists indicates their serious interest in the matter.

There are also reports of individuals who have had access to radiological material joining ISIL/DAESH.[72] Consequently, it may only be a matter of time before a radiological bomb is produced, although it is unlikely that it will be deployed in territory that is claimed as part of a future 'Caliphate.' That means the most probable target for such bombs is likely to be Western Europe and the Americas.

Given the international forces' ranged against it, survival of the so called Islamic State can only be realistically possible if it

had a nuclear deterrent.[73] It is therefore highly likely that ISIL/DAESH' senior leaders have a long term-plan for acquiring such weapons through a combination of insider influence, bribery and theft. In this venture, it is likely that AQ may assist or have its own parallel plan, given its proximity to possible sources of nuclear bombs.[74] Success in the operations to destroy ISIL/DAESH will reduce the likelihood of success in their venture. However, loss of territorial control may spur any significantly large remnants of the group to view the acquisition of such weapons as the most likely route to their re-emergence as a 'state.'

Radiological threats are most commonly considered in the form of a 'dirty bomb,' which is a device comprising an explosive surrounded by radiological material. When initiated, the explosive disperses the radiological material over a wide area causing dangerous and persistent contamination with significant danger to the health and safety of anyone within the vicinity. This threat is considered feasible because it requires relatively little skill to produce such a weapon and because radiological material is comparatively easier to find than nuclear weapons. Radiological material is used in many higher education institutions, in medical procedures and in some industrial processes. Very small quantities tend to be used at each location and the material is required to be kept in a controlled and accountable manner because of the health risks it poses. Nevertheless, it is possible in theory for a coordinated theft from several locations to form a device large enough to cause sufficient alarm, if not death and injury. There are also claims of radiologically contaminated industrial sites in former Soviet Union countries from where material could be gathered and used in a 'dirty bomb.' This option would require some detailed knowledge of where these sites still exist and instruments such as Giger counters to detect and confirm the location of the material. While the possibility of death or injury may not deter terrorists from handling the material, the likelihood that radiation illness could incapacitate them before construction of the bomb may encourage them to use suitable protective clothing and containers for transportation. So far, no such bomb appears to have been produced but the feasibility of this option makes it a potential threat for which CT measures should be in place. This could include radiation detector instruments for use at ports of entry and by explosive investigators. Radiation decontamination equipment, materials and training to deal with any use of a 'dirty bomb' should also be provided.

A possible future radiological threat may come from terrorists using focussed radio frequency transmitters, normally used for jamming purposes, against personnel, causing long term health issues. These types of weapons come under the designation of Directed Energy Weapons (DEW). While there is no evidence of this option being currently explored, it may become a possibility once anti-drone devices, some of which use high powered focussed radio signals to disable drones, become more widely available. While this is a real theoretical possibility, the lack of immediacy and visibility of the harm caused by such a weapon will make it an unattractive device for most terrorists, who prefer the shock effect of the spectacular and visible forms of attack. Nevertheless, the current R&D effort[75] into detecting and remotely disabling such devices should be accelerated, before the threat emerges.

The main benefit of obtaining and using CBRN for a terrorist organization is the kudos they confer and the disproportionate psychological impact they yield. This high psychological impact and the image of CBRN as 'weapons of mass destruction' make them unattractive for most terrorist organizations except apocalyptic organization ones. The perceived deterrence effect of such weapons, especially when faced with the likelihood of territorial defeat, and a desire to mimic the capability of its adversaries is likely to spur ISIL/DAESH to acquire, develop and deploy CBRN capabilities.[76]

CT Functions and Technology

CT, like conventional warfare, involves a number of functions or stages, the successful execution of which involves the use of appropriate technology. For the purpose of this study the functions can be listed as:

- Detection
- Surveillance

- Disruption
- Access
- Engagement

These functional stages are usually, but not necessarily, chronological. However, they also have circular feedback components. For example, the successful arrest or killing of a terrorist can, and usually does, lead to the detection of other terrorists and plots. Technology plays an important role in this system by, for example, using genetic fingerprinting to identify individuals involved in supplying and assembling any weapons found.

Detection

A wide range of technologies assist in detecting terrorists and plots. Most of these technologies are employed in the realm of intelligence and so are usually classified. In general, the more the terrorists use technology, the easier it is to use technology to detect them and to develop countermeasures against their use of technology. This advantage is greatest in the realm of communications monitoring, which involves a vast range of technical software and hardware tools used to infiltrate terrorist suspects' use of the Internet, intercepting their mobile phone calls and the classic bugging of the suspects' houses, cars and other areas where they might assemble or operate.

These measures require a high degree of technical expertise and constant updating of technical tools as both the Internet and mobile phones are constantly being updated in terms of hardware, operating systems and the applications software. The challenge is becoming greater as terrorist groups are beginning to use sophisticated encryption software, meaning that any successfully intercepted communication cannot be read until decrypted. Consequently, CT forces need to work with intelligence agencies to have an appropriately funded strategy to grow and maintain an effective communication intercept and decryption capability. Few government CT policy makers have adequately addressed this challenge so far. In particular, they have not fully met the challenge of attracting, developing and retaining skilled individuals in an economic environment where their expertise is in great demand within the private sector.

Given the prevalence of international and global terrorism, there is frequently a need for real-time translation of communication intercepts. Increasingly, this is provided by translation software tools coupled with voice recognition and speech to text software. However, these currently provide only a coarse level of accuracy and so linguists are necessary to provide reliable translations. Even linguists have their limitations. Unless they are grounded in the particular dialects of the suspects and they understand the culture of the individuals, they can only translate the words but not provide any subtle meaning and the underlying emotional intelligence.

Software network analysis tools are now being used to provide the most effective output from any communication intercepts by adding to the wider intelligence on the network and often giving early warning of any plot from its concept through to planning and execution. When these tools are combined with intelligence fusion and assessed by experienced and skilled analysts, they can provide powerful and timely information for disruptive action against terrorist groups.

There is a danger of CT forces becoming mesmerised by the promise of technology in detecting plots. Human intelligence, or HUMINT, still provides very effective actionable intelligence. This can come from traditional uses of 'agents' or HUMINT sources within or close to terror groups or from members of the public. In addition, public engagement has proven to be one of the most cost effective initiatives. There have been at least two high profile terror plots in the UK which were detected by members of the public before the authorities became aware of them.[77] [78] Some of the described technical means were subsequently used to confirm suspicions and gather evidence before the plots were successfully foiled. So, traditional intelligence methods have continuing utility and should be used in skilful combination with technical capabilities to confirm and disrupt plots.

The types of detection described above are primarily aimed at the detection of a terrorist plot. This is the best stage for CT forces to stop an activity as the threat is generally at its lowest level given that usually only an intent has formed and the necessary capability and planning has still to be fully developed. However, in cases where a plot has evaded detection, it becomes crucial to detect terrorists as they embark on their mission but before they can initiate their scheme. Many technologies in use aim to do this, such as x-ray scanners and swab and 'sniffer' explosive residue detectors. These are present in virtually all airports throughout the world and increasingly used at other points of entry to locations where large numbers of people congregate. In response to the terrorists' production of non-metallic initiators and low residue explosives, body scanners are now becoming more common. These machines bounce high frequency "millimeter" electromagnetic waves off an individual's body to detect hidden material that would not be detected by metal detectors or even by the manual "pat-down" search by security staff.[79]

Terrorists have learnt to avoid these detection methods and have changed their targeting methods by focusing on public assembly locations in cities where there are few or no checks. It is also possible that suicide bombers will in the future target the large queues which build up around security checks. There is therefore a need for detecting the presence of explosives from a distance. Universities have taken up this challenge, as they have many other technical challenges in CT, to develop suitable technology. Scientists at Loughborough University in the UK have developed a device that uses pulsed laser technology to detect tiny amounts of practically invisible explosive residue. The device can remotely and instantaneously scan crowds of people and automatically alert once traces of explosives are detected.[80] It is claimed that this technology could have thwarted some recent attacks in France and Belgium if it had been in use there. This is a typical example of how technology is being developed to meet the challenges of CT by academic institutions, especially in countries which invest in academic R&D.

Surveillance

Surveillance and detection overlap in operational terms. Detection of a suspect or a plot often leads to a surveillance operation and surveillance can lead to detection of other suspects and plots. Equally as frequent, surveillance confirms that suspects or suspected plots are innocent or pose no significant threat. Surveillance is probably the activity most impacted by technology. It includes all the technologies used in detection as well as others including manned and unmanned aircraft with visual and infrared cameras, CCTV networks and interception of mobile phone communications. These and other sensors are increasingly being augmented with facial and voice recognition technologies, the accuracy of which has achieved standards which more than rival human capability.

Nevertheless, human surveillance teams remain, and will continue to be, a primary surveillance capability on the ground. Their effectiveness and efficiency is being enhanced by improved communications and location equipment, allowing a controller to better deploy team members and reduce the risk of detection by suspects and to increase their ability to respond to unexpected threats or opportunities. Surveillance operatives can now become platforms for audio, visual and data sensors by carrying appropriate sensors on their bodies. Mini unmanned aircraft systems (MUAS) are increasingly being used to augment surveillance activities and provide the most promising area for development of capability in terms of audio, visual and electromagnetic monitoring of individuals of interest to CT. The endurance, range, payload, accessibility and usability of MUAS is growing on an almost monthly basis. Soon MUAS may become the primary means of surveillance, almost replacing human surveillance teams.

Disruption

Disruption involves the interruption of terrorist plans through means other than direct engagement through kill or capture. This can involve a variety of measures depending upon the situation, ranging from telling the parents of a youth that their son is not going to the Middle East to study Arabic as they believe, but is instead planning to join a terrorist organization,

to arresting terrorist facilitators on unrelated but real criminal charges so that they are unable to facilitate future attacks. Disruption can also mean interfering with terrorists' plans to make or initiate bombs through a variety of ways including technical means.

In the first form of disruption, relatively little technology is employed but in disrupting the making and initiation of explosives, a great deal of technology is used. This can include replacing potentially explosive material such as fertilisers with inert compounds that look like fertilisers or chemically modified fertilisers which cannot easily be converted to explosives. It can also mean using technical means such as electronic jamming to prevent the remote initiation of IED explosives using radio frequency transmitters.

This IED jamming activity has become a cat and mouse game. Once it becomes obvious that potential target vehicles are using electronic jammers, terrorists tend to revert to burying low tech pressure plate sensors to trigger the IED and run the risk of the device being initiated by a civilian vehicle. Recently, a number of Chinese made remote controls for garage doors have come on the market which operate over a wide frequency spectrum. These are harder to jam with current jammers and so terrorists are again beginning to use radio frequency remote initiation.

Disruption is best done as a part of an operational design. This means identifying the terrorist group network and having a systematic approach to disrupting and destroying it. A subset of this approach is attacking the IED network which includes the financiers of the activity, the suppliers of raw materials necessary to make bombs, the bomb manufacturers and those who emplace bombs. The technologies involved in this AtN approach are discussed in greater detail elsewhere.

Access

The ability to gain covert or swift access to terrorist locations for detection, surveillance or engagement is a critical feature in which much bespoke work is being done. This process often requires covert access to vehicles and locations. The technologies involved are usually sensitive and classified but they tend to be associated with sophisticated lock picking, overcoming burglar alarm systems and other means of entering terrorist vehicles, buildings and facilities.

Access related technologies are also used to allow rapid, often destructive, entry to buildings and vehicles to quickly eradicate or arrest terrorists and, where necessary, safely rescue hostages. Some very low tech but highly effective technologies are used to support this process. These include small hardened spikes attached to the tip of CT forces' rifles used to break windows; various types of axe designed for gaining access through doors, pyrotechnic cutting torches to cut through steel bars and a range of shaped cutting charges to break through doors, walls etc.

Engagement

Technologies used during the engagement process can be divided into three categories. The first are those used to eradicate or capture terrorist. The second are those which protect the CT force and the third are used to exploit the scene of the engagement. The first of these engagement categories is a critical area where few bespoke technologies have been developed. Standard military weapons, with the possible exception of stun grenades, are mostly used. However, mission planning tools show a great deal of promise. High resolution commercially available satellite imagery and maps are almost always used in locating and planning assaults or rescue missions. In an increasing number of cities, highly detailed three dimensional architectural images are now becoming available which allow the swift location of line of sight options to place observation posts or snipers and determine best approach and access to target options.[81] For unusual or complex tasks, 3-D printing could be used with such software to quickly make physical models of buildings, bridges and other structures to help with planning of actions such as emplacement of charges for demolition or explosives.

Personal protection equipment worn during engagement has benefitted greatly from investment in technology R&D. This is because of the ubiquity of the terrorist threat to military personnel during recent operations. The ever present threat

of snipers, RPG, indirect fire and IED attacks has meant that body armour, eye and ear protection has become standard kitting issue for most militaries. Much work has been done and continues to make the equipment as light, comfortable and effective as possible. Recent innovations include silk reinforced undergarments which are proven to significantly mitigate the severe damage which can occur from high speed impact of thousands of tiny dirt and grit particles caused by an IED blast wave. Such developments continue with significant benefit to the physical protection of CT forces as well as adding to their morale and confidence. These improvements, combined with the dramatic advances in medical care over the last decade or so, mean there is a great improvement in the chances of survival following IED attacks or gunshot wounds.

Successful arrest or death of terrorists during an engagement is no longer the end of a plot. Rather, it is the beginning of an intelligence and policing process which involves the rapid detection and disruption of other terrorists, their supporters and their logistical assets. There have been some powerful developments in technologies to assist with the rapid gathering and assessment of intelligence from terrorist action or engagement scenes. New equipment and procedures make the collection, analysis and assessment of terror scenes an almost real-time activity. It is now possible to swiftly identify the terrorist and possible accomplices along with any parallel or follow-on plots. Innovative technologies are being used in forensic chemical and biological analysis to help detect the extent of an individual's network and identify possible follow-on attacks. These include genetic sampling machines to identify individuals or human remains at the scene; chemical analysers for identification of explosive residue, and voice and facial recognition software, which is now available on CT forces' mobile phones. Technologies such as tamper proof seals and cyber forensic software tools are available and continually being developed to assist with evidence gathering, essential for successful prosecutions in the fight against terrorism.

Training

Another increasingly critical area is training. Most CT forces personnel may only ever engage a terrorist once in their careers in situations where there is an extremely high risk of death to the forces or to innocent civilians. Realistic, frequent and comprehensive training is the best way to increase the chances of successfully debilitating terrorists with the minimum possible casualties. New technological solutions are being used to allow realistic and comprehensive training to prepare for the high risk and high precision actions required of CT forces.

These include, but are not limited to, the use of simulation based on virtual reality software, laser attachments to standard weapons to simulate shots which are detected with laser sensors on clothing during simulated firefights. It is now possible to practice live firing using mobile targets or manikins that can be remotely controlled, allowing the more realistic simulation of scenarios where terrorists move rapidly amongst innocent parties who may also be in motion.

Apart from standard skills and scenario-based training, the increasing prevalence of technology and the rapid replacements or upgrades to equipment means that there is a greater need for technical aptitude and continuous training in CT forces. This requirement needs to be recognised and force level and training programmes adjusted accordingly.

Chapter 4 Technology – Opportunities and Challenges

Technology Development

Technology is developing in many areas, and especially in the digital domain, at an exponential rate. In some cases, it is no longer the R&D time of technology that is holding back the delivery into service but it is the speed at which a business case can be developed, marketing plans produced, manufacturing capability established and relevant government procurement procedures implemented. While there are many areas where new and emerging technologies have a great potential to assist in CT, traditional technology is also being developed and used in novel ways to enhance CT capability.

Traditional Technology

Technologies used in CT are not all new or complex; many are simple and old. For example, entry systems usually involve sliding hammer devices or specially constructed serrated axes. Electrical wire tie wraps are frequently used as temporary personal restraint systems. Torches used for night operations are basically old technology modified by improved batteries and more efficient and powerful bulbs. Consequently, when faced with challenges or the need for tools, traditional technologies should not be neglected.

One such technology being prototyped by manufacturers is hybrid airships capable of observation, ISR and carrying a platoon size force.[82] Such aircraft can also have a deterrent effect by loitering at sufficient height, outside surface to air missile range, over areas where terrorists are located. The persistent presence of such an aircraft can force terrorists to hide or curtail their activities and can, over time, create psychological stress, in the knowledge that either themselves or their group members may be attacked or arrested at any moment.

Autogyros are a form of helicopter where the main rotor blades are not powered and the aircraft flies because of thrust provided by a forward pushing propeller. These aircrafts are both simple and cheap to build and operate. Costing around the price of a large car, they can provide cost effective mobility and ISR capability to CT forces. Miniaturisation of ISR and communications' technologies and the unmatched capabilities of human observation, make the autogyro a promising platform for current and future CT capabilities.

New or Emerging Technology

Mini Unmanned Air Vehicle Systems (MUAS)

Several technological developments across the spectrum of electronic miniaturisation, power batteries, miniature lightweight motors and other areas have led to a burst in the availability, performance and affordability of mini unmanned air vehicle systems. These are typically less than 20 kg in weight and usually capable of carrying payloads of around 10-20% of their weight. UAV of less than 200g are sometimes classified as micro UAV and can be as small as a large insect, giving them the potential to fly into buildings through small openings. These UAVs are primarily used for intelligence and surveillance once coupled with cameras, listening devices and electronic emission sensors.

Miniature low energy autopilot circuits, GPS receivers and other developments are reducing the skill levels needed to operate these systems, increasing their safety and effectiveness. When skilfully operated within their limitations, these systems can be covert or near covert. They have a unique oblique angle observation capability, unavailable through satellite or surface level observation methods. When integrated with other ISR and communication systems, they can significantly enhance the situational awareness of CT forces. Furthermore, MUAS, like larger UAS, are capable of being armed and used to target terrorists. This is a development which is likely to become increasingly prevalent in the years to come with small, high precision weapons being developed especially for them.

Although commercially available MUAS can and do provide the performance and capability required by CT forces, few

manufacturers have the robustness of design and packaging for field operations. Those that do, aim their products specifically at CT forces and usually charge a high premium. Therefore, there is scope for NATO and other CT forces to influence the commercial market in order to reduce prices. In fact, in the near future MUAS will become standard equipment for all tactical level CT forces and thus all forces should have plans in place for procurement and training for these devices.

Terrorist groups have begun to use MUAS for their ISR operations and also to arm them as terror weapons.[83] As long ago as 1994, a Japanese terrorist group attempted to disperse chemical agents from an adapted UAV but failed owing to the unreliability of the design at the time. Nowadays, manufacturers sell UAVs intended to disperse chemicals for crop spraying, providing a ready made capability. In 2002 there was an alleged plot to disperse anthrax over London which was thwarted by the arrest of the alleged plotters. Therefore, the intent has been there for a while and capability has increased enormously since then. MUAVs have been used by Middle Eastern and South American groups to deliver IEDs and in swarming patterns to cause fear and disruption. There is great potential for terrorists to use them for assassination and other tactical purposes.[84]

This MUAS threat necessitates counter-MUAS technologies for deployable use by CT forces and for fixed use in point or area defence of sensitive sites. Most counter-MUAS devices operate by jamming the MUAS control link, but there are others which aim to 'burn' its circuits through high energy pulses, using what could be described as a directed energy weapon. There is much scope to develop these systems so that they can be used at an increased range, with greater reliability and with reduced impact on other users of the electromagnetic spectrum.

High Altitude Persistent Air Systems (HAPS)

HAPS are a new aircraft design based on solar powered ultra-light unmanned airframes, capable of remaining airborne for around a month with a payload of approximately 10kg. HAPS fly at high altitude, above weather systems, providing a cost-effective and responsive virtual satellite capability. These aircrafts are beyond the concept demonstrator stage and, apart from weather limitations for take-off and landing that are tighter than other aircraft, they provide a promising organic virtual satellite ISR capability for CT forces.

3D and 4D Printing

While 4D printing [85] is still to develop as a mass capability, 3D printing is a new technology that is having a significant impact in the civilian sector and has much untapped potential in CT operations. It can be used to rapidly produce bespoke casings for ISR sensors when these need to be attached to, or blend in with, unusual fixtures or surroundings. Models of buildings or structures can be quickly produced from diagrams to assist in planning or rehearsing assaults and bespoke tools can be produced for access or engagement activities. Currently 3D printing is limited by the strength of the plastics and powders currently used, but developments are underway to print with metallic material which will greatly enhance their utility.

As with other technological developments, 3D printing also represents an opportunity for terrorists. It is likely that in the near future they will be able to use this capability to manufacture components for IEDs. It is also conceivable that when these printers become more widely available, terrorists may attempt to use them to manufacture components for weapons such as hand guns. This will be a particular concern in locations inside security parameters, such as the airside of airports. Therefore, it would be prudent to build security safeguards into the printers or into their locations to prevent them being used to produce weapon components in restricted locations.

Sensor Technology

One of the greatest advances taking place and expected to continue in the future is in sensor technology. Electromagnetic spectrum sensors are becoming smaller and cheaper and their sensing range is becoming broader. These factors are

being assisted by improvements in signal processing allowing, for example, a single camera for visual and infrared imaging. Similar advances in radio frequency sensors are allowing the development of handheld devices for a broad range of communications and data intercept operations. Chemical and biological sensors, having already been considerably improved, represent perhaps the greatest potential for further development. Their potential in mobile and rapid identification of suspects through genetic fingerprinting, detection of IEDs, CBRN devices etc, is great.

Robotics

Robotics technology has been exploited by CT forces for over three decades in bomb disposal or counter-IED units. Recent advances in actuation, power systems and processing technology make for the possibility of smaller, more agile devices thereby increasing accessibility in difficult locations and greater precision of actuator arms and grips to allow for more delicate inspection or disabling tasks. It is now also possible to deploy armed robots into buildings containing terrorists. This allows a stealthier and safer option for CT forces to neutralise them. Again, terrorists' exploitation of robotics in the form of radio controlled cars carrying IEDs, for example, should be anticipated and suitable countermeasures need to be further developed and implemented.

Nanotechnology

Nanotechnology has already begun to make an impact on the world with a variety of applications. There is an expectation that many more dramatic applications will evolve in the near future.[86] The almost invisible nature of nanotechnology reflects the tiny size of nano products and processes such that most people are unaware of their presence and impact on their lives. Nanotechnology is analogous to a raw material or process employed in producing a usable technology rather than a usable technology in its own right. Nanotechnology has been responsible for some of the advances made and being made in the burgeoning field of the sensor capability already mentioned. Its ability to change the nature of materials is likely to make a significant impact on most technologies discussed in this paper including robotics and 3-D and 4-D printing. In CT terms, it will mostly be the products and effects produced by nontechnology rather than the technology itself that will most likely be useful.

Encryption

Encryption has been increasingly used by terrorists to hide content of their messages. It is now almost impossible to decrypt some of the more sophisticated encryption technologies employed by terrorists except possibly by the most sophisticated intelligence services in the UK, USA or Russia.[87] Consequently, other forms of communication monitoring have taken on a greater importance. This includes mapping of communication traffic which allows the building of terrorist network diagrams where communication nodes, the amount of traffic and other useful information is available without necessarily being able to intercept the content of the communication in itself.

Encryption of communications between CT forces and all surveillance data links used in devices such as UAVs is also an emerging requirement. Here, the increasing availability of encryption in commercial communications is a readily available source of assistance. For example, some organizations, including government bodies, allow the use of the communication application WhatsApp for communication to a moderately high standard of classification.

The systems approach

Quick, accurate and broad-source mapping of terrorists' networks has been a great leap forward in detecting, disrupting and destroying terrorist groups. Networks usually consist of many layers, which can include leadership, operatives, recruiters, fundraisers etc. Networks can also be depicted and targeted in terms of the threat they pose. Of these, the IED network analysis is one of the most detailed sub-networks often produced by CT agencies. This will include its own leadership, bomb makers, logistics, fundraisers, and bomb emplacers. Several tools are used in analysing these networks

and producing suitable visualisations. Most of them are software based and increasingly are able to automatically produce diagrams when interfaced with intercept data. Skilled analysts understand the weaknesses and limitations of these tools and use their judgment and additional knowledge to manually amend them to gain a more reliable picture of the network.

A network diagram should be a living depiction of the terrorist group and it should aid operations against the group and be updated with any post operation assessment or information as well as by intelligence as it comes in. One of the many uses of a network map is in intelligence sharing between national and international CT organizations. For this and the above stated reasons, it is important that CT organizations move towards adopting standardised mapping tools, or at least ones that can import and export between different software versions, ideally maintaining a capability to use older versions as some nations may be slower than others to upgrade or change their technologies. To do that, the relevant software houses in the commercial sector will need to be encouraged to cooperate on standards or code sharing arrangements.

Regulatory Challenges

Airworthiness and Flight Safety

The rapid ubiquity of UAV and their increasing performance has been a challenge for airworthiness regulators. The response has been to sensibly restrict flying of all but the very lightest models in built up areas and in close proximity to people and other aircraft. Training requirements have also been introduced to reduce the risk of accidents through lack of operator skill and awareness of rules. Militaries and Police forces in many countries have a duty of care to citizens and to their own personnel. They tend to operate even MUAS which are heavier, operate at greater ranges and for longer endurances than most civilians. In the CT context, such as in the surveillance of an individual thought likely to commit a potential terrorist act, there could be a need for flight in highly congested locations, along unfamiliar and rapidly changing routes. These factors, and others, pose a higher risk to safety. CT forces have, therefore, to ensure that any UAV used by them does not pose a danger to others and so they are subject to parallel regulatory frameworks to permit flying of UAV. These regulatory frameworks intend to mitigate the increased risk of military and Police UAV operations through stricter requirements for UAV airworthiness, for operator training and for regulatory oversight, to offset the reduced operational limitations they have in comparison to civilian operators.

Safety requires a cautious and considered approach rather than a swift reaction. However, full evolution of UAV-based capability has significantly outpaced the relevant regulatory frameworks in some countries. The freedom from regulation that terrorists enjoy has further given them a potential advantage over CT forces in developing and deploying this capability. It would be beneficial to CT forces if regulatory frameworks were more widely shared so that nations, which have yet to fully develop them can adapt existing ones rather than spending time to develop them from scratch. It is also a good idea if these frameworks were written in a way which would allow then to remain relevant to any anticipated technology developments. That would obviate the need for revision, without compromising safety.

Procurement

In the past, technology would take decades to evolve and equipment could remain in military service for over a quarter of a century. Nowadays technology is evolving in months rather than years. Equipment, especially commercial off the shelf (COTS), can be obsolete almost the moment it comes into service. Most defence and security procurement processes are optimised for large long-term programmes and so are insufficiently agile. There is consequently a need for procurement processes to adapt to the new reality, otherwise CT forces will lose their competitive advantage in the terrorism fight. While some countries have attempted to modify their procurement processes to make them leaner, it seems that rules on transparency, competitive tendering and other factors mean that processes are still time consuming for all but relative small amounts of purchases.

In CT particularly, there is a shift from organic defence development of technology to COTS or bespoke commercial solutions. While there is a growing desire to make CT related R&D part of a national security strategy, governments cannot divert the R&D priorities of a commercially driven market towards CT. The established large global military suppliers are exploiting this opportunity by taking relatively cheap technologies intended for the commercial market and adapting them slightly for the defence and security markets. In the process they charge a large premium, negating much of the benefits of COTS or commercial bespoke solutions. A new approach is needed to encourage more small companies involved in the design and manufacture of CT related products to supply direct to the defence and security market. This is important not just in terms of value for money but also to ensure new technology is quickly deployed for effective CT. An idea would be to employ government funded technology business advisors to help small enterprises navigate the quite complex procedures involved in selling to governments.

IT, Intelligence and Privacy

A further challenge for governments is the need to cooperate with information technology service providers attempting to balance law enforcement access with user privacy.[88] National security advisors have attempted, after recent terrorist incidents, to renew calls to undo surveillance reform and downgrade encryption technologies, in order to facilitate authorities in their pursuit of terrorists. However, this issue is not an entirely technological problem, it is more a political and a business model problem. It is complicated by the fact that the encryption applications most favoured by the so-called Islamic State are either based oversees or are open source. States and international organizations are constrained by having to work within a rules-based international system, while violent non-state actors do not need to abide by the rule of law. Governments often appear to be a step behind ISIL/DAESH, which has become adept at exploiting social media in order to generate multi-dimensional manoeuvre and in this way negate the governments' advantage provided by mass, platform technology.

Terrorist groups and extremists are capitalising on advances in technology to spread propaganda and radical behaviours, but traditional law enforcement techniques are insufficient to deal with these new, evolving trends in radicalisation.[89] Recent terror cases have demonstrated that IT companies will stick by their commitment to privacy and refuse to provide access to encrypted data even when they can. The state is forced to develop its own means to break into potentially useful sources of intelligence. This situation is likely to persist and therefore it would be prudent for CT forces to both, continue to develop mechanisms with the private sector that will allow them controlled ad hoc access and to develop their own access capabilities. As these are likely to be expensive, this process is ideal for burden sharing between nations, especially those within NATO.

Legal

All the safety, procurement and privacy issues discussed above are related to legislation of one kind or another. While the law can sometimes constrain CT forces from being more effective, its primary purpose is to protect the population from harm and to safeguard society's ethical values. As such, it is important that a proactive approach is taken with legislation in ensuring the swift but safe and appropriate exploitation of emerging technologies in CT. An example could be to anticipate the high likelihood of anti-MUAS weapons being deployed in cities in the near future. Laws may be required to use these weapons without causing harm to operators and to the public from any radiation hazard. As with procurement, the speed of change in technology requires a proactive approach from the legal regulatory sector.

The Attraction of Basic Technology and Tactics

The popularity rate of terrorist shooting attacks has remained almost constant over the last four decades and the Mikhail Kalashnikov developed AK-47 remains the most popular firearm among terrorist organizations. This is not surprising considering the fact that this weapon remains the most widely manufactured rifle of all time.[90] Across Europe in 2015 more

terrorist attacks have been carried out with Kalashnikov-type assault rifles than with any other device.

While technological advancements have made leaps in the last decades, many terrorist organizations still prefer more basic weapons. This is not necessarily because of a lack of accessibility to more advanced technology but because of the specific strategic advantages such basic methods provide. Visually, basic and crude methods such as throat-cutting, provide a very strong image and enhances the feeling of horror. Moreover, when the terrorists' chosen weaponry is primitive, it gives the impression that the fight is disproportionate and highlights the impotence of the state forces' superior technology against it. Terror groups try to exploit this image of an unequal fight to their advantage – internally and externally. Internally, to reinforce commitment to the claimed cause from existing members and externally, to enhance recruitment and raise awareness to their own version of the fight.

Another factor is the symbolic message that certain basic attacks send out. By using a knife to kill someone at close proximity, the terrorist may want to communicate to the public an obsessive commitment to their cause, their apparent courage and amplify the fear and horror element of their actions. Thus, the adoption of less advanced methods of attack is not necessarily due to a lack of operational capability but can be a calculated decision based on the advantages basic weaponry offers.

Regularly, terrorist groups demonstrate an apparent ability to develop and employ novel methods of attack. However, often these innovations do not really introduce new technologies, but rather just signify a different and original utilisation of already existent technologies. These constant efforts both from security forces and terrorist groups to stay a step ahead of each other have led towards a combination and synchronisation of existent methods and tactics in order to gain the best advantage and achieve the best results for them.

At the operational level, the current terrorist trend appears to be moving back towards a combination of old, tested and existent tactics in order to maximise effectiveness rather than towards the use of new tactics and weapons. Combined and synchronised attacks by terrorist groups give the impression of greater capability, greater deterrence challenge and gain more media attention. The 9/11 attack for instance, combined synchronised hijacking with the use of very basic weaponry, it involved a large number of hostages, and the planes became large explosive devices.

Current trends indicate a global rise of suicide bombings, preference for beheadings, and the hiding of improvised explosive devices in corpses of animals.[91,92,93] As a result, operationally the current global trend is not always moving towards high technology, verifying Hoffman's argument that '*terrorist devices will be innovative in their simplicity.*'[94] There are many internal and external reasons for this. On the one hand, effective counter measures limit the terrorists' choices of modus operandi. Secondly, limited human and material resources set boundaries on what means and modes terrorists can actually use. For instance, *Sendero Luminoso* (Shining Path) in Peru invented a home-made grenade made from drink cans packed with gunpowder and nails and launched from *huranos*, the traditional sling shots.[95] It is not that terrorists have stopped seeking new technologies to increase their lethality but effective CT measures and improved interstate cooperation has made it increasingly difficult for terrorists to get their hands on sophisticated technology. This is particularly the case for groups which employ small cells or encourage lone actors.

Another factor is that the larger terrorist organizations are monitoring drug and other smugglers' concealment methodologies. Indeed, there is an increasing interdependence and a growing symbiotic relationship between the two movements in approach, style and methodology.[96] Experts note that within a few days of a new concealment method used by criminals being made public, the same method can be discovered being attempted by terrorists for hiding weapons or explosives during transportation.[97]

Technology 'Arms Race'

Advances in technologies such as the development of commercial electronics historically have assisted both the author-

ities and the terrorists. Terrorist groups continually respond to effective CT measures by adapting their capabilities and approaches. During the conflict in Northern Ireland there was a kind of arms' race between British defence specialists and terrorist groups in Northern Ireland. British defence specialists for instance, developed a system of electronic scanners that would detect and neutralise a radio signal seconds after the radio control had been activated. [98] This measure in turn was countered by the Provisional IRA by using radar detectors, commonly used by motorists to provide early warnings of police speed traps, to activate their IED. These detectors were triggered by a laser gun, similar to the ones Police forces use to measure the speed of cars on highways. The security forces were unable to jam the light signal as easily as the radio signal, thereby restoring the initiative to the IRA.[99]

As already discussed, there is ample evidence that AQ and ISIL/DAESH are also engaged in a technology arms race against CT forces and their targets, primarily military and security forces. For example, improved armour used by military vehicles led to the development of shaped charge IEDs. Improvements in IED pressure plate detection equipment resulted in IED triggers being designed which reduced or eliminated metal components, the primary material used for detection. As CT agencies developed their Internet encryption breaking capabilities, terrorists have developed even more sophisticated encryption codes to hide their operational communications. These are just a few examples to illustrate the point that the CT fight is also economically asymmetric. It can be financially exhausting if allowed to continue over a protracted period. Indeed, economic exhaustion of the West is one AQ's declared strategic objectives.[100]

The asymmetric nature of terrorist conflicts in both combat and economic terms means that the longer a CT campaign lasts the more draining it is on states. As NATO's Supreme Allied Commander Transformation said, "…..*Huge amounts of money have been spent for instance in equipment to deal with '$5 IEDs' in Afghanistan*." [101] All the indications are that technology will drive the need for greater financial investment from states as time goes on. Winning such conflicts will require a more agile and aggressive approach in order to quickly defeat terrorist groups.

Chapter 5 Conclusion

The fundamental difference in the use of technology between terrorists and CT forces is that while the latter uses it instrumentally to counter the threat, the former tends to use it both instrumentally to plan and conduct attacks but also in a symbolic way to communicate a message of horror and coercion. Consequently, terrorists' use of technology and innovation is not just a means to an end but is also an indicator of the objectives, style and condition of the group. The relationship between terrorist thinkers and actors shows that the majority of apparently new techniques will have been written about or attempted before they are put into practice, sometimes several decades earlier. While it may be difficult to predict when and where a group might attack, historical insights can give some indication of what terrorists might do and how they might do it.

This is particularly true of global terrorists' desire to engage in reflective rhetoric through deeds that attempt to mimic their opponents' actions. For example, the cyber attack on Central Command was likely, in part, an attempt to send a message of mutual vulnerability. This characteristic may indicate, for instance, the greater future use of drones by terrorists to assassinate high profile individuals, reflecting the highly effective use of drones by the USA against these terrorist groups. Having used the marauding style of attacks in various cities involving gunmen attacking several locations almost simultaneously, using guns and bullets, it is likely that terrorists will augment future attacks with MUAS to provide a reconnaissance and coordination capability to increase the time they can avoid engagement with CT forces and to adapt to any unexpected changes of plan. It is also likely that they may use large numbers of MUAS carrying small IED as swarms to terrorise citizens and confuse the CT response. On a more worrying scale, it is similarly likely that ISIL/DAESH will use chemical weapons to respond to alleged use of such weapons against it or against civilians by Middle East regimes.

Terrorist groups exploit technology to maximize the means available to them to achieve their ends. Hence they will use soft and hard technology as well as new and old technology. They can be innovative and early adopters of emerging technologies but they can also be reactive, wanting whenever possible to adopt technologies used against them to demonstrate an ability to overcome or match the CT forces ranged against them.

Terrorists' attempts to use chemical and biological weapons have been frustrated by difficulties in weaponising biological and chemical agents. Recent technological developments mean that sufficient incentive and capability exists for them to develop an effective deployment mechanism. It is also likely that ISIL/DAESH' senior leaders have a long term plan for acquiring nuclear weapons to ensure their survival. While on their own they are unlikely to succeed, if there are a small number of individuals guarding nuclear weapons who have ideological sympathies with such groups then there is a realistic chance of them acquiring a few weapons to form the nucleus of what they might believe to be a deterrent.

Technology has provided new tools, techniques and tactics to terrorists. It is also a key element in CT. On the whole, CT technology approaches have tended to be reactive, conceding the initiative to terrorists. In recent years a more proactive approach was adopted in targeting IED networks, allowing greater initiative to CT forces. There is scope to take an even more proactive approach in order to disrupt terrorist use of technologies before they are able to exploit them. National level R&D effort and investment is understandably focussed on current operational challenges but a proactive approach that anticipates threats and opportunities rather than just reacting to them is likely to be more successful in the future. Greater and more specific R&D investment is needed. That investment should be in a proportion that is more reflective of new and future realities and threats than is currently the case. There is scope to defray additional cost through burden sharing of expertise and investment between nations. Even within countries, there is scope for a more joint approach to CT technology development, use and training between the militaries, Police and intelligence agencies. This will not only save costs but should improve the coordination and operational effectiveness of these organisations as they work together to defeat the threat. Effective CT requires a joint approach between most parts of civil and military power.

Big data, AI and information or intelligence fusion presents both the greatest promise and challenges in CT technology. Big

data and intelligence fusion technologies are able to provide unprecedented levels of speed and richness in intelligence. Successes in this field will, amongst other things, help in the battle of the strategic narrative and in understanding the complex human terrain environment. This depends on the continued development of the SOCMINT capability which, in turn, requires constant upgrading of tools and techniques to stay abreast of the evolving social networking applications. All this is expensive and so CT budgets must reflect the link between investment, capability and effectiveness.

An enabling challenge is the need for technologies to reduce the data transmission burden and also those that increase data sharing capacities. Procurement strategies in this area should purchase spare capacity to allow for the inevitable future development of data hungry applications and equipment. Human resource strategies should address the need for highly trained individuals who can get the best out of the information being gathered through big data analytical tools.

Network mapping is an increasingly useful targeting tool which benefits from big data and other technology developments. Network diagrams should be more sharable between organizations and international partners. It is important for governments to encourage the relevant software companies in the commercial sector to cooperate on standards or code sharing arrangements.

Technology is impacting training through improved simulation in both a physical and virtual sense. The increasing amount of technology being used by CT operatives leads to a rising need for CT operators to possess technical aptitude and undergo continuous training. This may require adjustment of force levels, recruitment and training programmes.

There are some dramatic advances in sensor technologies which are already improving the speed and accuracy of information in the electromagnetic, chemical and biological spectrums. These developments, coupled with advances in processing power, miniaturisation and power efficiencies of circuits, along with breakthroughs caused by nanotechnology, are likely to make major improvements in detection capability in the next few years. The ready availability of encryption is, like many other technological advances, proving to be a double-edged sword. It is being used by most CT forces to protect their sensitive communications, but it is equally exploited by terrorists to hide their intent and plans. This mitigates the many advances in intercepts by making it harder to interpret messages and so reduces the ability to detect and disrupt plots. Decryption tools and alternative detection methodologies should be developed to meet this challenge.

3-D printing technology has the potential to help CT forces while also being creatively exploited by terrorists in their weapon manufacture or concealment activities. This example illustrates the need for CT organizations to develop a predictive capability on how terrorists may use emerging technologies. Technical or procedural safeguards should be developed in advance to deny terrorists the opportunity to abuse new technologies for their purposes.

MUAS is proving to be both the most ubiquitous and promising of the emerging CT technologies. Existing exploitation by terrorists indicates several potentially serious threats and is pointing to a currently poorly developed area of counter-MUAS technologies. The development of counter-MUAS technology may have to be a priority for most nations in the months ahead.

The MUAS is an example of how the world of technology is being shaped by the convergence and integration of several technologies. While remotely piloted vehicles have been in existence for decades, their size, endurance, stealth and utility has been radically improved in the last few years through developments in the efficiency of power sources, propulsion systems and structures as well as the effectiveness of control systems and sensors. This trend of technological efficiency and effectiveness across a range of sciences is allowing old ideas to be revisited. Traditional technologies could be cheaply and reliably used in CT operations when updated with new developments to produce cost effective solutions. Updates to airship and autogyro technology are just two examples of old designs which could become more potent ISR and attack platforms when combined with new developments in electronics, software, structures and power systems.

Notwithstanding the advances available through integration of several new technologies, there are a few areas where

specific technology development effort needs to be prioritised. Encryption and remote sensing of explosives are the most important and urgent for improving CT. The R&D effort required for developments in such fields should involve not just government scientific capabilities but also research institutions such as universities and the commercial sector. At the same time, there is a need for a creative approach to the scientific and technology advances being made, on an almost daily basis, to see how these may yield opportunities for improving CT capabilities.

Many new developments are a potential safety hazard and so regulatory frameworks need to anticipate technology advances to become more agile, without compromising safety. Slow development of regulatory frameworks have given terrorists the advantage in cases such as MUAS, where they are able to adopt new methods before CT forces get suitable clearances to do so. In procurement, small designers and manufacturers need to be encouraged to serve the CT sector so that they can improve value for money and ensure new technology is quickly deployed. Government funded technology business advisors helping small enterprises navigate the somewhat daunting procedures involved in selling to governments may help achieve this. In the field of intelligence, the challenge for governments is the need to balance law enforcement access with user privacy through cooperation with information technology service providers. Laws may also be required to control the use of anti-UAV weapons to avoid harm to operators and to the public from any radiation hazard.

Notwithstanding the relatively low cost of CT technology compared to conventional forces' equipment, and the benefits of COTS, there is a potentially draining effect of an arms race with terrorists. In this race, the terrorists have an asymmetric advantage because they can use cheaper equipment, they do not have expensive regulatory frameworks and they need fewer items. New CT strategies which exploit the states' continuing, albeit diminishing, technological advantage and greater resources along with relevant political measures, will be needed to avoid the draining effects of a technology arms race between nation states and terrorist groups.

At the same time, the role of technology in both the threat and in countering it, is rapidly increasing, being driven by exponential developments in technology. Difficult decisions may need to be made by governments to balance budgets for CT and conventional defence capabilities more appropriately. This factor and the fact that CT is a joint activity drives towards greater alignment of equipment and training requirements between intelligence agencies, Police and the military as well as greater burden sharing between nations.

The intrinsic link between terrorism and technology, the increasing complexity of the terror threat, the raising burden of CT equipment and training and the rapid evolution of technology indicates a need for wider and more in depth understanding of the subject. This understanding can be achieved most effectively through education and training courses, aimed at the terrorism and technology relationship, at relevant schools, colleges and Centres of Excellence. Such education and training should produce more capable CT forces at all levels and should also drive the cultural change, new approach and capabilities necessary for more effective CT.

Recommendations

It is recommended that NATO and its member states:

- Strengthen the nexus between the social sciences and physical sciences to develop a predictive approach to the terror threat, allowing improved prioritisation of R&D and to target specific capability developments such as more powerful analytical tools
- Continually review the balance of investment, priority and capability development between CT and other defence and security needs to ensure that risks and capabilities are appropriate to the threat
- Make CT priority setting a necessity because terrorist attacks are likely to involve multiple complex systems

such as: multiple critical industrial infrastructures, multilevel state responders, and complex data mining. Modelling and simulating attack and responses can facilitate priority setting

- Recognise that decryption of messages, remote sensing of explosives and anti-MUAS should be amongst the priority areas for urgent CT technology development. These and other priority technologies should be developed using a more collaborative approach between government and academic research institutions.
- Enhance the AtN approach with an improved predictive approach and with technology to support big data analysis, artificial intelligence and information fusion of social media with other forms of intelligence
- Agree to more standardisation of data formats to allow quicker sharing of network analysis information between CT organizations and nations
- Explore more aggressively ways in which the talent, knowledge and skills can be recruited, developed and retained for the highly data and technology driven CT roles
- Work to mitigate the effects of commercial competition and perceived security issues from being a barrier to the greater sharing of best-practice and capabilities in CT technology.
- Appreciate that advances in technology allow significant performance improvements in some old ideas, such as airships. A new imaginative approach is required to avoid the seduction of complexity over the reliability of simplicity
- Should contribute a wide range of expertise not just on new technologies, but also on older technologies which can provide cheap and effective solutions as well as upgrading old equipment designs with higher performance materials and systems to produce effective CT capabilities
- Underpin the above recommendations with an educational and training programme aimed at providing an understanding of terrorism and technology. This should provide the necessary expertise with a flexible, agile and creative approach to effective CT.
- Develop agile procurement, legal and safety governance frameworks to avoid terrorists seizing and maintain the initiative
- Beware of the dangers of a technology ‘arms race’ where the terrorists have an asymmetric advantage over states. Implementing the recommendations of this paper can, to some extent, avoid this danger.

Notes

(Endnotes)

[1] NATO Press Release COMMUNIQUE PR/CP(2016)116, Defence Expenditures of NATO Countries (2009-2016) dated 4 July 2016

[2] Becker, Jordan, 'Security vs. Austerity: An Instrumental Variable Analysis of the Effect of Fiscal Rules and Sanctions on Defense Spending,' King's College London, International Development Institute, November 9, 2016, p.23. Accessed via: http://tinyurl.com/zu98lgl.

[3] A series of coordinated terrorist attacks occurred on 13 November 2015 in Paris, France and its suburb, Saint-Denis. Three suicide bombers struck outside the Stade de France in Saint-Denis, during a football match, followed by several mass shootings, and a suicide bombing, at cafés and restaurants. Mass shooting took place at a concert in the Bataclan theatre. The attackers killed 130 people, including 89 at the Bataclan theatre. Most of the attacks too place within about 20 mins. The French police CT forces arrived on the scene about 35 minutes after the first attack. A final assault on the Bataclan theatre ended the attacks at around 00.23hrs the following morning meaning that the incident lasted around three hours from start to finish.

[4] The Huffington Post, Brussels Lockdown Photos Show City In Surreal Light As Armed Troops Patrol Empty Streets, 24 November 2015. http://www.huffingtonpost.co.uk/2015/11/23/brussels-lockdown-photos_n_8628774.html.

[5] In Afghanistan, terrorism was used as a tactic by certain groups/actors but NATO officially chose not to conduct CT operations. However, in reality the borders of COIN, CT, stability and security operations are blurred and frequently overlap, meaning that elements of CT were an unavoidable activity, if only in a defensive sense. See: NATO's Counterterrorism & Counterinsurgency Experience in Afghanistan Lessons Learned Workshop Report NATO Centre of Excellence Defence Against Terrorism, COE-DAT 2015. P.4.

[6] The Institute for Economics and Peace, Global Terrorism Index 2015.

[7] See Hoffman Bruce, Inside Terrorism (New York: Colombia University Press, 2006)

[8] Rosen, Stephen P., Winning the Next War: innovation and the modern military (London: Cornell University Press, 1991), p.52

[9] Martha Crenshaw, `The Causes of Terrorism', Comparative Politics 13:4, (1981), 379-80

[10] For example, see: Chin, Warren. NATO and the Future of International Terrorism and Counterterrorism, COE DAT, Ankara. 2015.

[11] Contest, The United Kingdom's Strategy for Countering Terrorism Annual Report on counter-terrorism, 2013.

[12] Notable exceptions are an edited volume by David Clarke, Technology and Terrorism (2004) and Michael Mates' Draft Interim Report Technology and Terrorism for NATO's Sub-Committee on The Proliferation of Military Technology, dated 11 April 2001. Both make pertinent observations but their work needs to be taken forward and updated following the dramatic advances in certain technologies.

[13] For example, Northrop Grumman opened a centre new centre in Charlottesville,
in 2009, intended to support the "war on terrorism through a variety of cutting-edge biometrics and analysis programs that allow the Army to better identify, track and counter terrorists and insurgents." See https://globenewswire.com/news-release/2009/03/18/394301/161581/en/Northrop-Grumman-Opens-New-Charlottesville-Research-Park-Office.html

[14] R Nunes-Vaz and L Chim, 'Science and Technology Support for National Security: An International Review,' DSTO Defence Science and Technology Organization (Edinburgh, Australia 2009) p.11-12. Accessed at: http://digext6.defence.gov.au/dspace/bitstream/1947/9994/1/DSTO-TN-0888%20PR.pdf on 16 Sep 16.

[15] https://www.sto.nato.int/publications/Pages/activities_results.aspx?sq=1&k=terrorism&s=Search%20Activities&start1=1

[16] NATO Science and Technology Organization Annual Report 2015, March 2016.

[17] Matthew E. Miller, 'NATO Special Operations Forces, Counterterrorism, and the Resurgence of Terrorism in Europe', Military Review, July-August 2016.

[18] Bessner, D., & Stauch, M. (2010). Karl Heinzen and the Intellectual Origins of Modern Terrorism. Terrorism and Political Violence, 22(2)

[19] Heinzen, K. (1853). Murder and Liberty. New York: Self‐Published by Author. Reproduced in: Bessner, D., & Stauch, M. (2010)

[20] Inspire Magazine, September 2010. Accessed at: https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf on 20 Sep 16.

[21] BBC News, 'Nice lorry attack: Five suspected accomplices charged,' 22 Jul 2016. Accessed at: http://www.bbc.com/news/world-europe-36859312 on 22 Sep 16.

[22] CNN.Com, Underwear Bomber, dated 17 Feb 2012. Accessed at: http://edition.cnn.com/2012/02/16/justice/michigan-underwear-bomber-sentencing/ on 24 Sep 16.

[23] BBC New, 'Printer cartridge bomb plot planning revealed,' dated 22 Nov 10. Accessed at: http://www.bbc.com/news/world-middle-east-11812874 on 22 Sep 16.

[24] Aljazeera.com, Al-Qaeda claims Saudi prince attack, dated 28 Aug 09. Accessed at: http://www.aljazeera.com/news/middleeast/2009/08/200982816332563115 5.html on 22 Sep 16.

[25] Op. Cit., Bessner, D., & Stauch, M. (2010). p. 155

[26] Conrad, J. (1983). The Secret Agent: A Simple Tale. Oxford and New York: Oxford University Press. p.31-32.

[27] Brian Jackson A., 'Organisational Learning and Terrorist Groups', National Institute of Justice Working paper # WR-133-NIJ, February 2004

[28] Bruce Hoffman quoted in Paul Wilkinson, Terrorism and Technology (London: Frank Cass, 1993)

[29] Kagan, Robert, The Return of History and the End of Dreams (London: Atlantic, 2009), p.81

[30] The term Islamism is used here in the sense of movements that see Islam primarily as a political construct rather than primarily a theological value system. The Muslim Brotherhood and the Jamaat-i-Islami are the two main Sunni Islamist political movements. Both have several splinter groups of extremist parties that believe their version of a 'sharia' based political system will only prevail through a violent jihad. There are also Shia Islamist parties.

[31] Sertif Demir and Ali Bilgin Varlık, 'Globalization, Terrorism and the State', Alternatives: Turkish Journal of International Relations 14, no.3 (2015), pp. 49-50

[32] Rohan Gunaratna (ed.), The Changing Face of Terrorism (Singapore: Times Publishing Limited, 2005), p.1

[33] John Gray, 'Al Qaeda and what it Means to be Modern' (London: New Press, 2003)

[34] A Ashraf, 'Al Qaeda's Ideology Through Political Myth and Rhetoric (Doctoral thesis, University of St Andrews, Scotland 2012) Retrieved from: https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/3222/MohammedAshrafPhdThesis.pdf

[35] Quote in Gunaratna, Rohan, Inside Al Qaeda (New York: Colombia University Press, 2002), p.103

[36] Op Cit A Ashraf (2012)

[37] Gorriti, Gustavo The Shining Path (Chapel Hill: University of North Carolina Press, 1999), p.137

[38] For example, see Abdul Qudos Ziaee, 'The Challenge of Pressure Plate IEDs (PPIEDs) And ERW Contamination in Afghanistan' Counter-IED Report, Autumn 2015 (Delta Business Media Limited), p.23.

[39] Hoffman, Bruce, quoted in Jackson, Brian A., 'Technology Acquisition by Terrorist Groups: threat assessment informed by lessons from private sector technology adoption', Studies in Conflict and Terrorism, Vol. 24, No. 3 (2001), p.199

[40] Hewring, Holger H., 'Innovation Ignored: the submarine problem – Germany, Britain and the United States 1919-1939' in Murray, Williamson R. and Millet, Allan R., Military Innovation in the Interwar Period (London: Cambridge University Press, 1998), pp.311-312

[41] Joseph S. Nye, Understanding International Conflicts: An Introduction to Theory and History, 6th ed. (Harlow: Pearson Longman, 2007), p. 63

[42] Sherwood, Harriet et al. 'Schoolgirl Jihadis: the Female Islamists Leaving Home to Join ISIS Fighters', The Guardian, 29 September 2014

[43] Atwan, Abdel Bari, Islamic State: The Digital Caliphate (London: Saqi Books, 2015), p.ix

[44] Ashraf, M. A. 'Iraqi Insurgency and the Internet,' in D. Hansen, & M. Ranstorp (Eds.), Cooperating Against Terrorism. (Vallingby, Sweden: Centre for Asymmetric Threat Studies, 2007)

[45] Atwan, Abdel Bari, Islamic State: The Digital Caliphate (London: Saqi Books, 2015), p. 27

[46] AJP-01(D) – Allied Joint Doctrine dated 21 December 2010 p.1-10.

[47] The evolution of NATO's Cyber Defence is outlined in: http://www.nato.int/cps/en/natohq/topics_78170.htm

[48] IBM, "What is Big Data?" http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html [accessed 16 September 2016)

[49] Ibid

[50] See Hulnick, Arthur S. 'The Downside of Open Source Intelligence', International Journal of Intelligence and CounterIntelligence 15, no. 4 (2002), pp.565-579

[51] Anthony Olcott, Open Source Intelligence in a Networked World (New York: Bloomsbury, 2013), p. 133

[52] Croom, Herman L. 'The Exploitation of Foreign Open Sources', CIA Historical Review Program 13, (Summer 1969): 129-136, p.129

[53] In-Q-Tel, 'About IQT – History', https://www.iqt.org/about-iqt/ [accessed 16 September 2016]

[54] In-Q-Tel, 'Portfolio' https://www.iqt.org/portfolio/ [accessed 16 September 2016]

[55] Omand, David, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence (SOCMINT)', Intelligence and National Security 27, no. 6 (2012), pp. 801-823

[56] Simon Wibberly, Carl Miller, 'Detecting Events from Twitter: Situation Awareness in the Age of Social Media' in Christopher Hobbs, Matthew Moran and Daniel Salisbury (eds), Open Source Intelligence in the 21st Century, (Basingstoke: Palgrave Macmillan, 2014), pp. 147-167

[57] Omand, David, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence (SOCMINT)', Intelligence and National Security 27, no. 6 (2012), pp. 801-823, p.804

[58] United Kingdom, Developments, Concepts and Doctrine Centre, Security and Stabilisation: The Military Contribution, Joint Doctrine Publication 3-40 (Shrivenham: DCDC, 2009), xiv – xvi

[59] P. B. Symon and A. Tarapore, Defense Intelligence Analysis in the Age of Big Data, Joint Force Quarterly 79, National Defense University Press, October 01, 2015.

[60] A-C. Boury-Brisset, Managing Semantic Big Data for Intelligence, Defence Research and Development Canada, STIDS 2013 Proceedings p.4. Available at: http://ceur-ws.org/Vol-1097/STIDS2013_T06_Boury-Brisset.pdf

[61] Ibid, and more detail on the skills gap in the commercial sector: Big Data Analytics Adoption and Employment Trends, 2012-2017, Report by e-skills UK. November 2013.

[62] Attack the Networks (AtN) Project Overview Report dated 11 May 2015. Available at: http://www.jallc.nato.int/products/docs/factsheet_atn.pdf

[63] Prescott Neil, Submission to APPG on Explosive Weapons – the use of Improvised Explosive Devises (IEDs) and their impact on the humanitarian space, Defence Academy of the UK, 30 January 2016 p.5

[64] Ibid

[65] Bartosz Stanislawski, "A More Secure World? In Some Ways Yes; In Some Ways No," Cato Unbound, http://www.cato-unbound.org [accessed 16 September 2016]

[66] NATO, Allied Joint Publication 3.15(A)

[67] Smart JK. History of Chemical and Biological Warfare Fact Sheets. Aberdeen Proving Ground, Md: US Army Chemical and Biological Defense Command; 1996. Special Study 50

[68] These attacks occurred in 2001, just days after the 9/11 attacks, killing five people and poisoning many more. In February 2010 the FBI closed its investigation into the case alleging that the attacks had been carried out by Dr Bruce E Irvins who had committed suicide in 2008. Some claim that the FBI allegations do not amount to conclusive evidence and so

other possibilities might exist. See New York Times, 'F.B.I., Laying Out Evidence, Closes Anthrax Case,' dated 19 Feb 2010. http://www.nytimes.com/2010/02/20/us/20anthrax.html

[69] Kaplan, David E., Aum Shinrikyo, in Jonathan Tucker (ed) Toxic Terror (London: MIT Press, 2000), p.207

[70] Most victims of chlorine bomb attacks are killed or injured by the explosive rather than the chemical. These few who are affected by the chlorine can suffer considerable distress and injury. See Damien Cave and Ahmad Fadam, 'Iraqi Militants Use Chlorine in 3 Bombings,' New York Times, dated 21 February 2007.

[71] See: http://www.forbes.com/sites/danielfreedman/2011/09/26/al-qaedas-dumbest-terrorists/#25133512cc62

[72] See: http://foreignpolicy.com/2016/02/29/the-islamic-states-plot-to-build-a-radioactive-dirty-bomb/

[73] Tom Batchelor, Pakistan's nuclear weapons stockpile could be Stolen by ISIS terrorists, Express Newspaper Apr 1, 2016

[74] Farhad Rezaei, Shopping for Armageddon: Islamist Groups and Nuclear Terror, Middle East Policy, 23: 112–132

[75] U.F. Aydoğdu, Technological Dimensions of Defence Against Terrorism, IOS Press 2013. p.20.

[76] Prime Minister David Cameron warns of one such capability in: Ben Riley-Smith, 'ISIL plotting to use drones for nuclear attack on West.' The Telegraph, 1 April 2016.

[77] Prevent Strategy, The UK Government June 2011, p.56. Available at: https://www.gov.uk/government/publications/prevent-strategy-2011

[78] Fertiliser bomb plot: The story, BBC News Report dated 30 April 2007. See http://news.bbc.co.uk/1/hi/uk/6153884.stm

[79] For more information, see: https://en.wikipedia.org/wiki/Full_body_scanner

[80] Tech Times, 'Explosive Residue Detector Uses Laser Technology to Foil Terrorist Attacks,' dated 15 April 2016. http://www.techtimes.com/articles/150016/20160415/explosive-residue-detector-uses-laser-technology-to-foil-terrorist-attacks.htm

[81] Vertex Modelling is one of many suppliers: http://vertexmodelling.co.uk/products/3d-city-models/

[82] Lockheed's airship gets the green light: FAA approves massive hybrid vehicle that could launch in 2018, The Mail Online, dated 19 November 2015. See: http://www.dailymail.co.uk/sciencetech/article-3326046/Lockheed-s-airship-gets-green-light-approves-massive-hybrid-vehicle-launch-2018.html

[83] Robert J. Bunker, 'Terrorist and Insurgent Unmanned Aerial Vehicles:
Use, Potentials, And Military Implications,' Strategic Studies Institute
and U.S. Army War College Press, August 2015.

[84] Ibid

[85] 4D printing is a technology that prints a 3D object which then changes its shape in a predefined manner when exposed to a medium such as water or heat. In simple terms 4D printing allows the manufacture of more complex 3D objects such as hollow spheres.

[86] U.F. Aydoğdu (ed), Technological Dimensions of Defence Against Terrorism, IOS Press 2013. p.121-138.

[87] Ewen MacAskill and Patrick Wintour, UK under pressure to respond to latest Edward Snowden claims, The Guardian 14 June 2015

[88] See for instance http://tech.firstpost.com/news-analysis/whatsapps-end-to-end-encryption-should-not-provide-safe-havens-to-terrorists-says-fbi- 307871.html [accessed 14 September 2016]

[89] European Commission. Secure societies – Protecting freedom and security of Europe and its citizens. HORIZON 2020 - Work Programme 2016 – 2017. (n.p: European Commission, 2015), 22. https://ec.europa.eu [accessed 14 September 2016]

[90] 'Why has the AK-47 become the jihadi terrorist weapon of choice', The Guardian, 29 December 2015

[91] Suicide Attack Database, The Chicago Project on Security and Terrorism (CPOST). See http://cpostdata.uchicago.edu/search_new.php?clear=1

[92] R. A. Pape, M Rowley and S. Morell, 'Why ISIL Beheads Its Victims,' Politico Magazine, 7 October, 2014

[93] The Times, Retreating Isis leaves behind deadly detritus, dated 4 October 2016. See: http://www.thetimes.co.uk/article/retreating-isis-leaves-behind-deadly-detritus-wt568w2jt

[94] Hoffman, Bruce, 'Terrorist Targeting: tactics, trends, and potentialities', Terrorism and Political Violence, Vol. 5, Issue 2 (1993), p.12

[95] Rapoport, David C., Inside Terrorist Organisations (London: Frank Cass, 2001), p.117

[96] D. Winslow, 'Terrorism, Drug Trafficking, and ISIS: When Wicked Worlds Collide,' The Daily Beast, dated 9 December 2015. See: http://www.thedailybeast.com/articles/2015/12/09/terrorism-drug-trafficking-and-isis-when-wicked-worlds-collide.html

[97] Assessment of a Senior Scientist at a World Leading CIED Centre dated September 2016.

[98] Hoffman, Bruce, 'Terrorism: trends and prospects', in Lesser et al Countering the New Terrorism, (Santa Monica: RAND, 1999), pp. 31-33

[99] Ibid

[100] Osama bin Laden's Message to Iraq, dated 11 Feb 03. Compilation of Usama Bin Laden Statements 1994 - January 2004, p.250 accessible at: *https://fas.org/irp/world/para/ubl-fbis.pdf*

[101] General Jean Paul Palomeros, at the Chiefs of Transformation Conference on December 2013.

Centre of Excellence Defence against Terrorism
Devlet Mah. İnönü Bul. No: 65
Kirazıdere, Ankara . TURKEY
Phone: +90 312 425 15 82
Fax: +90 312 425 64 89
info@coedat.nato.int
www.coedat.nato.int