Terrorism Online: A New Strategic Environment

Stuart Macdonald and David Mair

Cyberspace is a source of enormous opportunities. It also presents many critical challenges. Indeed, it is now widely recognised as a new strategic environment and is expected to become a major front in future conflicts: both irregular and traditional (United States Joint Force Command, 2010). A range of International Governmental Organisations (IGOs) have launched policies, strategies and other initiatives specifically on cyber security. These include the Commonwealth, Economic Community of West African States (ECOWAS), European Council, European Union, NATO and United Nations (for a recent example, see European Commission 2013). In 2013, NATO produced the Tallinn Manual – the world's first military policy document that detailed the governance of cyber warfare and cyber operations (Schmitt, 2013). States and their executives have also been active in addressing cyber security challenges. In the UK, for instance, the National Cyber Security Programme was launched in June 2011, accompanied by £650m of new investment and the establishment of a new National Cyber Crime Unit within the National Crime Agency. An additional £210 million has been earmarked for investment in UK Cyber Security between 2015 and 2016. The government has also established cyber incident sharing partnerships (CISPs) to allow businesses to share information on current cyber threats and recently launched the new cyber emergency response teams (CERTs) to respond to on-going malicious cyber incidents. CERT-UK, the UK's cyber response force, became operational in March 2014.

The focus of this volume is the convergence of cyberspace with another of the top tier threats identified by the United Kingdom's National Security Strategy (2010): international terrorism. Whilst the chapters that follow each examine specific issues relating to terrorists' use of the Internet and questions of response, this chapter contextualises their discussions by charting the full range of terrorists' online activities. One of the objectives of the chapter is to move beyond the debate surrounding old versus new terrorism, which has generated much attention and comment in the past fifteen years. The new terrorism thesis states that the organisational structures, motivations and lethality of contemporary terrorist groups are fundamentally different from those of the old terrorist groups of the past. We begin by expressing our doubts about this claim, and argue that in any event it is more fruitful to focus on the changing environment in which terrorist groups operate. The chapter then explains that the Internet has produced a number of changes in both terrorists' objectives and their operations, and concludes by urging that a thorough understanding of the changes catalysed by the cyber realm is necessary for the effective formulation and evaluation of counterterrorism strategies, laws and policies.

'New Terrorism' and/or a New Environment?

Several commentators have argued that a "new" terrorism began to emerge in the 1990s (e.g., Hoffman (1998); Lacqueur (1999); Benjamin and Simon (2003); Neumann (2009). New terrorist groups, it is suggested, differ from the old terrorist groups of the past in three key respects. First, the organisational structures of new terrorism are thought to be different and lacking the hierarchy of old terrorist groups such as the Provisional Irish Republican Army (PIRA). Members of PIRA had ranks, and operations were planned and coordinated by senior leaders, with soldiers carrying out orders as they were received. Horgan and Taylor (1997) discuss the leadership structures of PIRA; noting that it incorporated command and control groups such as the General Army Council and General Headquarters; and that all operations had to be sanctioned by senior members of these groups. Within these organisations lay senior members of staff with overall responsibility for paramilitary activities both within Ireland and against foreign targets, such as in England. The existence of these job roles illustrates the chain of command said to characterise 'old' terrorist groups and the importance of national militaries as an organisational model and influence. By contrast, new terrorism - according to advocates of this thesis - is decentralized; members are grouped into cells by geographical location, skill set or objective. This networked structure makes the organisation more resilient; even if one cell is disrupted or destroyed the others are able to continue their operations (Tucker, 2001). Moreover, in contrast to old terrorist groups like the Irish Republican Army (IRA) and the Basque group *Euskadi Ta Askatasuna* (ETA), new terrorism is de-territorialised and transnational in orientation. For example, whereas members of the IRA were predominantly drawn from young catholic males living in Northern Ireland, members of Al-Qaeda inspired terrorist groups are drawn from a global network; an individual's background does not necessarily act as a constraint to their membership. Horgan and Gill's (2013) analysis of PIRA membership found that of 1,240 identified volunteers, 82.7% had been born in Northern Ireland and 13.9% had been born in the Republic of Ireland. 3.4% of PIRA members – a grand total of 17 identified volunteers – had been recruited from 'foreign' countries, such as England and the US. When compared to the numbers of foreign fighters in more recent conflicts such as the Iraq War and Syrian Revolution, there is a marked difference. For example, the Sinjar Records – official Al-Qaeda documents that recorded foreign fighters joining operations in Iraq – identify nearly 700 individuals who volunteered to fight in the conflict or engage in suicide bombings (Felter and Fishman, 2007).

Second, the perpetrators of new terrorism are said to have different motivations and justifications for their actions. Whilst old terrorism was characterised by political motivations, with most perpetrators identifying as either nationalists or Marxists, new terrorism is presented as being religiously motivated. Al-Qaeda, Lakshar-e-Taiba and Al-Shabbab have all sought to justify their actions with religious texts and doctrines (Juergensmeyer, 2003). Other suggested examples include the sarin attack by the Japanese Aum Shinrikyo sect (Duyvesteyn, 2004) and Timothy McVeigh, the Oklahoma City Bomber (Michel, Herbeck and Telles, 2001). This logic also lies at the heart of Rapoport's 'four waves' theory (2012), which depicts contemporary terrorism (1979-present day) as the religious wave, following the anarchist wave (1880s-1930s), anti-colonial wave (1920s-1960s) and 'new left' wave (1960s-1990s).

Third, new terrorism is said to be more lethal than the old terrorism that preceded it. Old terrorism was more restrained and targeted, lest excessive violence cost them political support and a place at the bargaining table. As Brian Jenkins famously remarked in the 1970s, 'Terrorists want a lot of people watching and a lot of people listening, and not a lot of people dead' (Jenkins, 1975, p15). By contrast, new terrorists are dedicated to causing the largest possible number of casualties. As a result, it leads to far more victims and fatalities (Morgan, 2004). New terrorism is more indiscriminate, and no longer regards violence as a means to an end but as an end in itself. Also significant is the fact that new terrorists are less interested in self-preservation than their predecessors. With the promise of reincarnation, paradise and spiritual rewards, perpetrators are said to embrace martyrdom (Atran, 2006). New terrorists are also thought to be more inclined to use weapons of mass destruction (Stern, 1999). For example, as well as the sarin attack mentioned above, Aum Shinrikyo also attempted a cyanide gas attack against the public transport infrastructure in May 1995 However, the device used to disperse the gas throughout the transport network was discovered before anyone was harmed (Enders and Sadler, 2012). Whilst incidents involving the use of chemical, biological, radiological or nuclear (CBRN) weapons have so far been rare, some terrorist organisations have expressed an interest in utilising weapons of mass destruction. Al-Qaeda, for example, has stated that it would use nuclear weapons against the US and its allies if it gained access to such materials (Paz, 2005).

The extent of these claimed differences between old and new terrorism – and, indeed, whether there are in fact any differences at all – has been much debated. For some, the differences are so great as to shatter "some of our most basic assumptions about terrorists and the violence they commit" (Hoffman, 1998, p204) and render "much previous analysis of terrorism … obsolete" (Lesser et al, 1999, p2). Others suggest that the differences should be understood not in qualitative terms, but as differences of degree (Neumann, 2009). On this view, the concepts of old and new terrorism are best understood as Weberian ideal-types. Weber himself explained that ideal-types do not represent historical or empirical reality. They are conceptual constructs, which are formed by accentuating particular features of a phenomenon (Weber, 1949). An example is the economic notion of a free market. By comparing them to the actual reality, ideal-types allow us to see changes and differences more clearly. They therefore are valuable as both analytical tools and expository aids.

On the other hand, there are others who question whether the terrorism of the twenty-first century really is any different to the terrorism of earlier periods. They query each of the three respects in which new terrorism is said to be distinct from old terrorism. In respect of organisational structures, they point out that a number of so-called old terrorist groups had networked structures. Tucker (2001) argues that the Palestine Liberation Organization and Hezbollah operate fundamentally as networks with little formal central control, whilst Duyvesteyn (2004) gives the example of the anarchist movement in the nineteenth century. She also questions whether new terrorist groups truly are de-territorialised and transnational. Al-Qaeda, she argues, has decidedly territorial and national objectives and its base and sanctuary in Afghanistan was territorial in orientation. Other examples include Al-Shabaab and the Islamic State of Iraq in the Levent (ISIL) whose objectives are geographically

focused. Al-Shabaab seek an Islamist Africa and ISIL seek an Islamist Middle-East, most notably in Iraq and Syria.

In respect of motivations, critics point out that many old terrorist organisations had religious connections. For example, the IRA was predominantly Catholic, whilst *Ethnikí Orgánosis Kipriakoú Agónos* (EOKA) in Cyprus was inspired by the Greek Orthodox Church. Conversely, new terrorist groups frequently have political motivations. For example, bin Laden's intellectual origins lie predominantly in a political interpretation of Islam (based on the specific teachings of Sayyid Qutb) (Duyvesteyn, 2004). In fact, Abrahms (2002) points out that bin Laden was often more concerned with political objectives – such as the presence of US forces in the Middle East – than he was with Western culture. Crenshaw (2008) argues that "Just as secular nationalist groups such as ETA and even the IRA took on a Marxist-Leninist veneer when it was ideologically fashionable to do so, nationalistic or revolutionary groups today may take on an Islamist cast" (Crenshaw, 2008, p.125). So, for example, the Moro National Liberation Front became the Moro Islamic Liberation Front. It has also been suggested that to describe the objectives of new terrorists as religious in nature perpetuates a skewed understanding of religion in general and of Islam in particular. For example, Gunning and Jackson (2011) argue that a causal link does not exist between an individual's beliefs and their behaviour, pointing out that secular terrorist groups are just as violent and uncompromising in their beliefs as religiously motivated terrorist groups and that "Islamic terrorism" is more a product of history and politics than of religioun. Additionally, to suggest a connection between Al-Qaeda and Islam is offensive to the vast majority of Muslims and risks alienating religious communities (Hardy, 2011). As Fawaz Gerges (2009) points out, most Muslims worldwide have rejected Al-Qaeda and religious leaders have often spoken out against Osama bin Laden's use of religious terminology to encourage acts of terrorism.

In respect of lethality, critics point out that small group or individual access to destructive technologies and knowledge of target vulnerabilities has grown over time. Indeed, the number of victims of terrorist attacks has been on the rise since the 1980s, which does not coincide with the claimed emergence of the new terrorism in the 1990s (Duyvesteyn, 2004). New terrorist groups also rely largely on conventional explosives; incidents involving CBRN weapons have been rare. Moreover, the use of CBRN weapons has not been limited to new terrorists; Spencer (2006) points out that 'old' terrorist groups including the Tamil Tigers and Turkey's Kurdish Workers Party or *Partiya Karkerên Kurdistan* (PKK) have been accused of having used chemical weapons in the past. Additionally, in 1972, members of an extreme right-wing terrorist group were arrested while in possession of typhus pathogens which had been intended to have been used to poison a water supply (Spencer, 2006). Furthermore, there are numerous examples of indiscriminate violence perpetrated by old terrorist groups, including the European anarchist movement and various nationalist groups, would-be revolutionaries and far right extremists (Crenshaw, 2008).

Duyvesteyn (2004) concludes by arguing that, before any claims of the newness of new terrorism can be accepted, careful historical investigation and empirical testing is required. In the absence of this empirical data, Burnett and Whyte (2005) suggest that the new terrorism paradigm imposes "a set of common characteristics upon an enemy that enable it to be

known" (p6). These characteristics then create the rationale for a precautionary approach to counterterrorism and are used to argue for burgeoning resources, expanded police powers and even extra-legal responses. A misdiagnosis of terrorist typology can therefore be used to legitimise strong counterterrorism responses for a threat that has been theoretically identified, but not effectively measured.

Importantly, however, even those who doubt whether the terrorism of the twenty-first century is new do recognise that the world in which terrorists operate has changed. Pointing out that terrorists have benefitted from the fruits of globalisation – including international travel and communications – Duyvesteyn (2004, p.449) states:

> In order for terrorism not to be considered new it is implied that they [terrorists] should not have moved with the times. It could very well be the case that because of a change in the external factors a change in the phenomenon of terrorism is perceived to have taken place and not because of the terrorists' own making or conscious choice.

Similarly, Crenshaw (2008) argues that, whilst "Differences among groups and differences in patterns of terrorism over time do exist … Many of these shifts may be due to a changing environment" (p.135). She points in particular to three aspects of globalization: advances in communications; access to weapons and explosives; and, individual mobility.

Today there are an estimated 1.7 billion Internet users (UK Government, 2010). In the years since the Internet was created there have been significant changes in how governments, commerce and society operate. The Internet not only offers increased communication capabilities, it also provides access to the largest repository of information ever collated. Moreover, it offers users the potential for anonymity. This is beneficial when engaging in actions such as political protest, which may result in negative consequences to the protester from oppressive governments, and when creating an online community based on equality in which factors such as gender, ethnicity and age are unknown and therefore unable to bias discussion and debate (Kennedy, 2006). Particularly notable is The Onion Router (Tor), which provides its users with anonymity for both legitimate and illegitimate activities. In December 2013, a Harvard student used the anonymity offered by Tor to email a hoax bomb threat to his campus in order to delay an exam he wasn't prepared for (BBC News, 2013). He was caught after investigators traced who had accessed the Tor network just before the threats were sent.

Terrorists and other individuals and groups with nefarious intent have not ignored the benefits of the Internet. On the contrary, the use of the Internet for terrorist purposes is a rapidly growing phenomenon (United Nations Office on Drugs and Crime, 2012). In the next three sections, we describe a range of terrorists' online activities. For the purposes of exposition, these activities have been grouped into three categories: outreach (terrorist groups' interactions with members of the general public); logistics (activities which are necessary for terrorist groups to function and perpetrate attacks); and, attack. We do not mean to suggest that the different activities we describe are entirely separate and independent from one another. They are mutually reinforcing. It is their combined effect that enables terrorist groups to operate in an effective and efficient manner. For example, when terrorist groups

produce publications that detail how to build improvised explosive devices, one aim is to encourage potential terrorists to engage in a terrorist act. Another motivation for doing this, however, is to engage in psychological war by reminding the public that perpetrating terrorism is easy and that they could be a victim of a terrorist atrocity at any given moment. Similarly, acts such as recruiting individuals to join terrorist groups and encouraging members to finance the organisation are fundamental to the process of co-ordinating terrorist attacks – a terrorist group without the capitol of manpower or money is very limited in the actions that it is able to undertake.

Outreach

Here we focus on three different forms of interaction with members of the general public (both sympathetic and unsympathetic to the terrorists' cause): recruitment and radicalisation; networking; and, publicity and propaganda.

Recruitment and Radicalisation

The worldwide reach of the Internet provides terrorist organisations with a global pool of potential recruits. So it is unsurprising that recruitment is amongst the top priorities for terrorist organisations online (Goodman, Kirk and Kirk, 2007; Weimann, 2004; Denning, 2010; Keller, DeSouza and Lin, 2010). In the days prior to the Internet, terrorist operatives were largely recruited from individuals with certain backgrounds based in specific geographical locations. The German Red Army Faction (RAF), for example, recruited the majority of its members from communists living in West Germany who felt ostracised from their families and culture due to their sense of horror at their parents' involvement in Nazi atrocities during World War Two (Hudson, 1999) Similarly, Post (1984) discusses Palestinian terrorist groups that recruit young people from the West Bank and Gaza whose anger at Israel has been passed onto them by their parents. By using the Internet terrorist groups are now able to access countries and territories that were previously closed to them. Similarly, the Internet allows individuals who sympathise with the aims and objectives of a terrorist organisation, but are based outside the traditional geographic recruitment locations, to make contact with and potentially join the organisation. For example, Shiraz Maher has estimated that there are 366 Britons fighting in Syria (HASC, 2014, p.22). This compares to other, less conservative, estimates of up to 700 (The Telegraph, 2014a). These individuals may have been influenced by online recruitment campaigns to join the fighting in Syria, such as the call to engage in a "five star jihad" that advertised the luxury lifestyle a foreign fighter could experience (The Telegraph, 2013). This wider geographical reach also enables terrorist organisations to outsource their operations. This is a tactic that Al-Qaeda has employed on a number of occasions. The actions in Bali, Spain and the UK are each examples of local operatives teaming up with Al-Qaeda representatives to carry out atrocities against civilians (Bobbitt, 2008).

One of the reasons the Internet is an effective recruitment forum is the demographics of its users. Studies have found that young people are the primary users of the Internet, with the

numbers of younger users far exceeding the numbers of older ones (Dutton and Blank, 2013; ONS, 2012; Fox and Madden, 2006). This is important given that research has found that young people are more prone to radicalisation. The UK PREVENT strategy identifies young people, and people from lower income and socio-economic groups as being the most at risk group for radicalisation, alongside those that distrust parliament, the police and have a disconnect between their cultural identity and that of the nation they reside in (HASC, 2012). Horgan and Gill's study (2013) (mentioned above) found that the average age at which individuals undertook their first PIRA-related operation was 24.9. Similarly, in Sageman's study (2004) the average age of those involved in international Jihad was 25.7. Also significant is the type of young person that is likely to spend large amounts of time online. Young, socially deprived, marginalised males tend to spend more time online than any other group and often find solace with one another in online environments (Frieburger and Crane, 2008). Frustrated at their communities, angry at their ostracism from society and seeking social acceptance, these individuals are key targets for recruiters (Sageman, 2011). Having identified these potential targets, recruiters introduce these angry young men to terrorist literature and romantic ideas of involvement in the terrorist cause. Following a period of grooming, these young men become more and more extreme in their beliefs until they view terrorist groups as righteous and their own government as morally bankrupt, corrupt and rotten. In their study of viewers of Al-Qaeda inspired YouTube content, Conway and MacInerny (2008) found that the primary consumers were males under the age of 35 who were motivated by romantic notions of heroism and religious sacrifice. Recent reports suggest that Al-Qaeda has started a new "invasion", led by second-generation women members, which targets young men and women who surf websites, particularly sports and music sites (Al Arabiya News, 2014).

Further examples of terrorist organisations' success in recruiting via the Internet can be found in recent incidents of UK home grown terrorists who have rebelled against their culture, upbringing and homeland. Andrew 'Isa' Ibrahim, angry at what he regarded as an unfair, racist and exclusionary society was fuelled by terrorist recruiters who encouraged him to take the path of violent extremism and provided him with friendship and camaraderie. Several months later, Ibrahim was arrested after having constructed a home-made suicide vest which he planned to detonate in a packed shopping centre in Birmingham (BBC News, 2009; Nesser, 2014). Another example is Mohammed Gul, a Law student in London who in 2011 was imprisoned for five years for disseminating terrorist publications after he reportedly self-radicalised online (BBC News, 2011). The notion of self-radicalisation has been examined by a recent RAND study (von Behr, I. et al 2013) of 15 UK-based extremists. This found that the internet provided more opportunities for individuals to encounter online extremists and thus more scope for radicalisation to occur. It also found that the internet could act as an 'echo chamber' in which extremist beliefs could be sounded out and repeated back to the original individual, thus cementing these beliefs more firmly. Interestingly, however, this report did not support the argument that the internet can result in self-radicalisation. In all the cases examined extremists had their views shaped and built on by others, whether virtually or in the real world.

Networking

In 2007 it was reported that there were as many as 50,000 extremist websites on the Internet (Chen and Larson, 2007). The number is likely to have grown since then. Since 2010, the UK has blocked or removed over 18,000 websites containing extremist content (Cabinet Office, 2013). The most popular sites receive tens of thousands of unique visitors each month (Conway, 2002). Many of these sites have an online message forum or real-time chat client which allows site visitors to post messages, build relationships with other parties, and maintain friendships. Terrorist sympathisers and antagonists thus have much closer access to terrorist organisations than before. For example, before he was killed by his ex-comrades from al-Shabaab U.S. born Jihadist Omar Hammami often utilised Twitter. His interactions with scholars, counterterrorism agents and sympathisers were frequently peppered with friendly remarks and banter (Ackerman, 2013a).

These forums are also often hotspots of extremist activity – with radical militants sharing images and publications produced by terrorist sympathisers, writing messages that glorify past or current acts of terrorism, and encouraging each other to engage in violent acts (Conway, 2002). An example is Samantha Lewthwaite, also known as the White Widow on account of her ethnicity and her marriage to 'martyred' 7/7 suicide bomber Germaine Lindsey. Lewthwaite penned a love poem to Osama Bin Laden, which police found on her computer (Independent, 2013). This poem has since been published on pro-terrorist websites to encourage others to engage in or support terrorist causes. Having experienced acceptance and approval of their extremist beliefs (as opposed to being socially ostracised for holding them), potential terrorists may regard these interactions as a positive life experience. Importantly, however, affirmation is often conditional on the individual's willingness to engage with an atrocity or to support terrorism in some other manner such as creating and disseminating terrorist materials or by providing financial support. Moreover, by engaging in dialogue with other extremists, terrorist sympathisers may experience group polarisation: the psychological phenomenon in which groups come to more extreme conclusions and decisions than they would as individuals (Janis, 1983). This process can operate to provide extremists with the justifications that they require to continue to believe in the righteousness of their cause.

So, virtual environments have dramatically increased the size of potential 'imagined communities' (Anderson, 1983). It is also important to note, however, that as web forums often have few controls over membership some online forums have inflated numbers of users when in reality only a few real members exist. In a process known as astroturfing, fake profiles enter into the same conversations and have discussions with one another, giving the impression that there are a number of different individuals that share the same beliefs and values (Zhang, Carpenter and Ko, 2013). Thomas Hegghammer (2014) argues that it is very hard to establish trust in online terrorist forums due to the difficulties in determining whether individuals are who they proclaim themselves to be or whether they are members of the security service. As a result, the explicitly stated or implied existence of security service and law enforcement personnel on these forums can act as a barrier to their effectiveness as a networking tool.

Publicity and Propaganda

Propaganda has long been a tool used by terrorist groups to discredit their enemies and increase morale amongst supporters. Today, many terrorist groups maintain websites and use mainstream social media – including Twitter, Facebook and YouTube – to engage in publicity, disseminate their media productions and engage with individuals (United Nations Office on Drugs and Crime, 2012). Their presence on social media is designed to maximise their impact and bring them into contact with as many members of their target audience as possible. Indeed, the Animal Liberation Front (ALF) and Earth Liberation Front (ELF) – both of which are regarded as domestic terrorist organisations by the U.S. Government – not only maintain operational websites and produce newsletters on their activities, but also recognise public presentation and education as one of their key objectives (Leader and Probst, 2010). Al-Qaeda also has a number of websites dedicated to the publication and dissemination of propaganda relating to its Jihad against the West. These publications are available in multiple languages and utilise various media formats including: magazines detailing how to join the Jihad; videos of successful militant operations and executions of captured enemies; speeches by spiritual leaders; video games that allow the player to play as a Mujahideen protagonist fighting Western soldiers; raps that glorify martyrdom; and, interview transcripts with martyred combatants and suicide bombers (Piper, 2008). Recently, an English language magazine was published by Al-Qaeda affiliated groups containing details of how to improvise explosives and suggested potential targets within the United Kingdom that would guarantee the maximum number of casualties and media exposure (Bosco, 2013). Many of these productions are professionally made and edited, creating a slick final publication which provides the terrorist group with an appearance of legitimacy.

The Internet allows terrorist propaganda to be shared and disseminated more widely and easily than before. Producing a magazine was once a costly, labour intensive process. Financial and geographical constraints meant that the individuals who received these publications were usually within a very specific geographical location. For example, Al-Qaeda's terrorist propaganda was once only shared in certain mosques and madrasses within an intended and focused region (Kaplan, 2009). Now information can be shared freely across borders and accessed by a wider array of individuals. This has impacted the content of terrorist publications, which are now targeted at a wider audience instead of specifically focussing on individuals in a particular location. It also means that terrorist publications are far more difficult to remove from circulation. Hard copies of a magazine can be destroyed and removed from circulation, but when a host website is taken down others appear to re-host the information (Davis, 2006).

There is a further reason why the use of the Internet by terrorist groups to spread their own ideology is significant. Prior to the Internet, terrorist groups had to rely on traditional news media outlets to convey details of attacks and the motivations behind them. Traditionally, media outlets portrayed terrorists' activities and motivations in a negative and unsympathetic manner (Clutterbuck, 1981). But the Internet provides terrorist groups with the power and

ability to narrate their own struggles and actions and present themselves in the manner they feel is most appropriate (Weimann, 2004; Tsfati and Weimann, 2002). This gives them the opportunity to focus on the righteousness of their cause, the need to use violence against an enemy with superior fire-power, and the atrocities committed against them – or the population that they are defending – by their enemies. This provides a more sympathetic light to the activities perpetrated by the terrorist groups.

Logistics

Here we focus on three types of online activity which are necessary for terrorist groups to function and perpetrate attacks: training; planning and co-ordination; and, financing.

Online Training

The Internet is the world's largest information depository. Terrorist groups have attempted to capitalise on the ability to share information online quickly and efficiently by seeking to create 'virtual training camps' (Stenersen, 2008). Al-Qaeda, for example, created its first online digital repository in 2003. This hosted a wide array of information, including how to avoiding the intelligence community, bomb-making, marksmanship, survival skills and tips on how to select targets (Weimann, 2004).

There are examples of online training materials being used to devastating effect. David Copeland, the London nail bomber, utilised online resources to build the bombs he used in his campaign against homosexual and minority ethnic communities in 1999 (Ramsay, 2009). Anders Behring Breivik utilised an online manual to construct the device he detonated in Oslo (Stenersen, 2013). Both Copeland and Breivik lacked any prior experience of explosives, yet were able to construct them using easily obtained materials. At the same time, there are also examples of unsuccessful attempts to construct explosive devices using downloaded materials. The men that attacked Glasgow airport, for example, downloaded schematics for their failed device (Kenney, 2010). Similarly, the bombs that were used in the attacks on London on 21st July 2005 failed to detonate correctly, as a result of the attackers using low quality hydrogen peroxide (The Telegraph, 2007b).

Constructing a bomb from an online resource is clearly a dangerous activity. The vast majority of individuals who attempt to construct bombs by following online materials have no prior experience at bomb-making. Not only might the individual make mistakes. They might have no idea that the mistake has been made. An Irish bomb-maker recently caused himself a severe injury when he forgot about daylight savings time and his device exploded prematurely (The Telegraph, 2014b). Individuals following online materials also do not have the benefit of experienced tutors that can guide their learning and steer them away from dangerous errors (Denning, 2010). As such, learning is slow, fraught with difficulty and is not guaranteed to result in the creation of a successful device. Compounding this, those that publish terrorist manuals may have limited experience in bomb-making themselves. When

following a flawed manual, would-be terrorists run the risk of their device detonating during construction, or not at all. Additionally, online bomb-making manuals may have been tampered with by the security services to prevent individuals from creating explosive devices. In 2011, the Secret Intelligence Service, known as MI6, and the Government Communications Headquarters, GCHQ, worked together to disrupt an online terrorist publication that contained a method for producing an improvised home-made explosive device. When users attempted to download this publication and access this recipe, they were instead directed to a webpage that contained recipes for making cupcakes (The Telegraph, 2011).

The importance and accuracy of marksmanship and survival manuals hosted online have been similarly criticised. Coll and Glasser (2005) argue that manuals cannot teach military skills. Accuracy with a firearm is a skill and so must be honed through rehearsal, i.e., learning by doing (kinaesthetic learning), rather than by simply reading. In the same way, survival skills must be practised for the individual to achieve competence. Reading a manual on how to survive in the wild does not give an individual the ability to do so. Kenney (2010) accordingly describes training manuals as aspirational, not operational, a sentiment echoed by Stenersen (2013).

Planning and co-ordination of physical attacks

Large scale terrorist attacks may involve a number of preparatory acts, including: target selection; reconnaissance; selection of entrance and exit routes; gaining knowledge of local peak times; and, acquiring information on emergency service response time and effectiveness. Many of these tasks involve visiting the site of a proposed attack to take pictures, conduct surveillance, identify any issues that might jeopardise the attack and extract local knowledge from the population of the target. This presents a high level of risk, with multiple opportunities for intelligence and law enforcement agencies to apprehend the individual and/or disrupt the activity. Moreover, multiple trips could be required which is both costly and time-consuming. The Oklahoma City Bombing, for example, took approximately seven months of planning which included target selection across a number of cities and states, prototype bomb creation, dry runs and, eventually, the terrorist act (Grand Jury Indictment, 1995).

Since the creation of the Internet, however, terrorist groups have benefited greatly from the vast volume of data available online. Information on public transport, critical national infrastructures, shipping lanes, maps, building blueprints, flight paths, sites of cultural importance, the security services and counterterrorism strategies are all available (Best, 2008) reducing the need for multiple, high-risk fact-finding missions. In fact a recovered Al-Qaeda training manual encouraged attackers to utilise online resources, stating that up to 80% of the data required to plan a terrorist attack is available online (Weimann, 2004). During a raid in Afghanistan in 2007, Google Earth printouts were found showing in detail the British bases in Basra (The Telegraph, 2007a). Google Earth may also have been used during the attacks in

Mumbai in 2008 (Ramsay 2009). Similarly, extreme right wing groups have used the internet in order to collect and disseminate information of use in the planning and co-ordination of violent attacks. Redwatch is an anti-left website containing the photographs, names, home addresses and telephone numbers of anti-facists, socialists, left wing activists and their known associates including family and friends. This information is freely available to any interested party and could be used for the planning of acts of violence and vandalism against the people and property listed. There have been a number of violent attacks associated with the publication of a victim's details on Redwatch (The Guardian, 2006). Similarly, in 1999, anti-abortion activists created the Nuremberg Files website, an online collection of abortion centre locations and the personal details of the members of staff that worked there. This information was available for use by anyone with intent to plan acts of violence or vandalism (Azriel, 2005).

Advances in communications technology also make it easier for the commanders of terrorist attacks to stay in contact with their actors, using such means as email, satellite phones, voice-over-IP chat clients and video-conferencing. The 2004 Madrid train bombers communicated via dead-dropping, utilising the drafts folder of email accounts in order to maintain secrecy and cut down on the chances of having their communications electronically intercepted (NY Times, 2006). The Mumbai attackers even received real-time information on the location of the security services and other actors throughout their attack. Significantly, advances in communications technology not only enable masterminds to co-ordinate multiple groups at once, but also to direct attacks from overseas (Kohlman, 2006). As a result, known terrorist leaders, who may be known to intelligence communities, border agencies and law enforcement organisations, do not have to risk capture by entering dangerous territories. They can co-ordinate and direct attacks from the safety of their bases, giving groups like Al-Qaeda a global reach.

Financing of terrorist groups

The operational and logistical costs associated with terrorism can make it expensive. Purchasing weapons, obtaining raw materials for the construction of explosive devices, training suicide bombers and marksmen, compensating the families of those killed or martyred for the cause, manufacturing and obtaining false documents in order to cross borders, hiding fugitives, protecting wanted individuals and carrying out attacks: these activities all require significant funds (Weimann, 2004). For this reason, terrorist groups need to engage in fundraising. For many groups – including Al-Qaeda, Hamas, Lashkar e-Taiba, and Hizballah – the Internet is now central to their fundraising efforts (Denning, 2010; Jacobson 2010).

There are a number of methods terrorist groups use to raise funds online (United Nations Office on Drugs and Crime, 2012). Websites, chat rooms and advertisements have been used to solicit and arrange donations (Hinnen, 2004). Internet user demographics have also been used to identify potential sympathisers, who are then emailed a request for donations (Brunst 2010). Terrorist groups have used websites to sell CDs, DVDs, T-shirts, badges, flags and

books (Weimann 2004). The IRA, for example, at one point maintained an electronic shop on Amazon in which supporters could purchase republican themed items and books, a percentage of the profits of which went into the IRA's coffers (Conway, 2006). Donors could also purchase items for terrorist groups directly; the Ulster Loyalist Information Service had options for supporters to buy bullet-proof vests for members of militias, such as the Loyalist Volunteer Force (LVF) (Conway, 2006). It is also well-documented that terrorist groups engage in cybercrime – including credit card fraud, counterfeiting and identity theft – to finance their activities. In fact, it has been reported that cybercrime now surpasses the illicit drug trade as the primary source of income for terrorist organisations (Theohardy and Rollins, 2011). A notable example is Younes Tsouli, who it is estimated raised £1.6 million. Tsouli intercepted credit card details by creating fake financial websites. Having obtained these credit card details, he bought the domains to 180 websites which were used to host Al-Qaeda propaganda, extremist videos and forums for terrorist sympathisers (Krebs, 2007). Similar to this is the case of Brahim Benmerzouga and Baghdad Meziane, who in 2003 were jailed for 11 years for plotting to raise funds for terrorist activities. They had collected the names and credit card details of almost 200 different bank accounts. The cards were sent to associates across Europe, allowing them to amass more than £200,000 for terrorist causes (BBC News, 2003).

The anonymity granted via the Internet also allows terrorist groups to pose as legitimate organisations, such as charities. Not only do charitable organisations enjoy public trust, they are also often subject to lighter regulatory requirements and in some cases have a global presence which provides a framework for national and international operations – often in the areas most exposed to terrorist activity (Financial Action Task Force, 2008). Posing as a charity is also particularly effective in the context of Islamic terrorism as giving a portion of one's income to charity is one of the Pillars of Islam. As well as terrorist groups posing as legitimate charities, there are also examples of otherwise legitimate charities diverting funds to support terrorism and of charities raising money for charitable purposes but fulfilling these objectives through a terrorist group (Financial Action Task Force, 2008). Indeed, the list of individuals and groups targeted by the UK government with financial sanctions for supporting terrorism includes groups with obvious terrorist objectives, such as 'Al-Qaeda in Iraq', but also ones with innocuous names such as the 'Global Relief Foundation' and the 'Benevolence International Foundation' (HM Treasury, 2014).

It is also important to note that the Internet makes it easier for sympathisers to donate to terrorist groups, and offers these sympathisers the possibility of anonymity (Hinnen, 2004). So whereas terrorist groups once had to specifically target individuals or groups for donations, now they have sympathisers prepared to actively seek them out to provide financial backing.

Attack

Here we focus on two different forms of attack which can be perpetrated online: cyberattack; and, psychological warfare.

Cyberattack

One of the global threats identified by the US Intelligence Community's 2014 Worldwide Threat Assessment was cyber (Clapper, 2014). This document explains that governments, commerce and society continue to increase their use of, and trust in, digital infrastructures and technologies, which raises a number of potential issues. Large segments of critical infrastructure retain legacy architecture, which is the result of organisations purchasing computers in bulk on contracts that do not keep up to date with the speed of technology. This means that the organisations are often left to work with outdated software that can be exploited by hackers when new vulnerabilities are uncovered or patches fail to be implemented. The presence of legacy architecture means that the systems used in government communications, water management, oil and gas pipelines and electrical power distribution are vulnerable to attack. The increase in cross-networking of personal data devices, medical devices and hospital networks means that health care services are also vulnerable. Smart objects – such as networked vehicles, industrial components and home appliances – offer efficiencies but also create even greater dependencies upon information technology. Virtual currencies are increasingly being used for criminal financial transfers. Emerging technologies such as three-dimensional printing also have enormous potential but could equally be exploited by those with malevolent purposes, as evidenced by the recent arrest of a Japanese man for manufacturing five handguns using a commercial 3D printer (Thomson 2014).

Increasing attention is being paid to the threat of cyberattack. The United Kingdom's Intelligence and Security Committee (2013) has warned that private groups of skilled cyber professionals are being paid to launch attacks on a diverse range of targets, including financial institutions and energy companies. In November 2013 the heads of the FBI, Department of Homeland Security and National Counterterrorism Center told Congress that cyberattacks are likely to eclipse 9/11-style terrorist attacks as a domestic danger over the next decade (Ackerman, 2013b). These attacks, they predicted, will come from individual actors as well as nation states (Homeland Security News Wire, 2013). One particular concern is the potential for malware to be used strategically as a weapon. This possibility was illustrated by Stuxnet, the first known malware to cause physical damage to critical infrastructure (Farwell and Rohozinski, 2011). Allegedly developed by the CIA in cooperation with the Israeli Government, Idaho National Laboratory and other US agencies (Gorman 2012), it was introduced to the Natanz Uranium Enrichment Plan in Iran by USB flash drive causing 1000 centrifuges to fail. Importantly Symantec has estimated that it took a dozen programmers at least six months to write Stuxnet, at a cost of more than $3 million (Bayshore Networks, 2010). This gives some indication of the level of effort and sophistication required to remotely sabotage critical infrastructures for large-scale impact. Indeed, the fact that no major cyberterrorism attack has occurred to date has previously been attributed to an unfavourable cost-benefit trade-off (Giacomello, 2004), especially given that the 9/11 attacks cost an estimated $400,000 – $500,000 (9/11 Commission 2004). But whilst a very high level of sophistication and resources were needed to develop Stuxnet, malware for sabotage may be expected to become more prevalent and mainstream in the future. Not

only is the idea now in the public sphere for others to build upon, future cyber-physical attacks would most likely focus on targets which are easier to attack, such as critical infrastructure installations, and importantly would not require nation-state resources (Langner, 2013).

There have been stark warnings of the vulnerability of critical infrastructure to cyberattack. Nicholson et al (2012) state that networking critical national infrastructure over the Internet allows hackers to gain control of Supervisory Control and Data Acquisition (SCADA) systems which exist to monitor, control and alarm operating systems within critical national infrastructure. Similarly, Wilson (2014) draws on the examples of Flame and Stuxnet to argue that critical infrastructures look like easy targets for possible cyberterrorist attacks. In marked contrast, Conway (2014) has argued that, whilst from a technological perspective there is the potential for terrorists to launch cyberattacks, when other factors are considered the threat is not a credible one. She identifies four reasons in support of this conclusion: the costs of cyberattacks are vastly higher than those of non-cyber equivalents; cyberattacks require levels of skill and expertise which terrorist groups typically lack; the destructive potential of non-cyberattacks can be more readily materialised than that of cyberattacks; and, cyberterrorism lacks the theatricality of more conventional attacks. Thomas Rid (2013) has been equally critical of the dangers posed by cyberwar and cyberterrorism, arguing that the role of internet enabled espionage, sabotage and subversion is limited and cannot be defined as violent acts of war. These contrasting views raise issues of risk management and resource allocation. Even if the likelihood of cyberterrorist attacks is low, would the government be prudent to ignore the possibility? Importantly, some authors who do not regard cyberterrorism as a significant threat do believe that countermeasures are nonetheless necessary – in order to guard against the risk posed by cyberwarfare and cybercrime which, they suggest, do pose a significant threat (Jarvis, Macdonald and Nouri, 2014, p78). Questions of response are complicated in this context, however, by the tension between the public interest in protecting (privately owned) critical infrastructures and the profit-maximizing instincts of the private sector (Legrand, 2014).

It has also been suggested that terrorist groups may use cyberattacks as force-multipliers, to assist and increase the effectiveness of a traditional physical attack (Goodman, Kirk and Kirk, 2007). For example, disabling the control rooms of the emergency services could significantly increase the harm caused by an attack by slowing response times and delaying access to medical care. Indeed, the FBI has predicted that terrorists will exploit the emerging capability for network-based attack by developing or hiring hackers to launch cyberattacks to complement large conventional attacks (Theohary & Rollins 2011).

Psychological Warfare

Brian Jenkins once described terrorism as theatre (Fletcher, 2006). It is the dramatic and shocking nature of terrorist attacks that are intended to intimidate governments and the public at large. Such intimidation can have a significant impact on a country's economy, for example

by reducing tourism and affecting how people travel. Coshall (2003), for example, found that terrorist threats have the effect of reducing international and domestic travel. The theatricality of terrorism also impacts the way decision makers and the public assess the risk it poses. When thinking about risk people rely on certain heuristics, one of these being the availability heuristic. When people use this, they assess the magnitude of a risk by asking whether examples come readily to mind (Sunstein, 2005). By reinforcing the availability and salience of past attacks, dramatic and shocking images can lead to exaggerated perceptions of the terrorist threat. They can also result in probability neglect, which occurs when a person's emotions are intensely engaged causing them to focus on a bad outcome and neglect the likelihood of it occurring (Sunstein, 2003). These psychological processes are reinforced by the round-the-clock media attention that terrorist attacks receive and by political rhetoric which employs the politics of fear (Altheide 2006). Even when well-intentioned, reminders of a threat can operate to heighten public anxiety. For example, one study found that overt CCTV installations did not assuage the public's fear of crime but increased it (Minton and Aked, 2012). As Coaffee, O'Hare and Hawkes (2009, p.507) state; "devices and designs for safety can achieve quite the opposite effect – fearfulness, suspicion, paranoia, exclusion and ultimately insecurity."

It is unsurprising, therefore, that as well as recruitment and propaganda terrorist groups also use the Internet to engage in psychological warfare. This can take the form of glorifying past acts of terrorism. By glorifying these actions, terrorist groups present themselves as powerful and successful, their opponents as weak and helpless, and remind opponents of the damage they have caused previously (Brunst, 2008). Terrorist groups have also posted direct threats against potential future targets online. Recently, for example, forum members on an Al-Qaeda affiliated message board made threats against New York City (Berger, 2012). Such threats are designed to cause fear and anxiety in the target population by reminding them that they are vulnerable to attack and can experience the horror of terrorism at any moment. They also seek to erode public confidence in governments' ability to keep them safe from acts of terrorism (Baldwin, Ramaprasad and Samsa, 2008). In addition, such threats hold the possibility of being taken seriously by the intelligence and law enforcement community, effectively tying up investigative resources and providing every-day city commuters with the sight of a fortified police presence on their city's streets. This could further increase the public's fear of an imminent attack or incident.

As well as glorifying past acts and issuing future threats, terrorist groups post images and videos online showing such things as car bombs, suicide bombs and executions (Weimann, 2004). These are frequently very graphic– showing dismembered body parts, blood and screaming bystanders – and are designed to shock and intimidate the target population and reinforce the brutal reality of terrorism. A significant example of this is the videotaped execution of the journalist Daniel Pearl. A journalist for the Wall Street Journal, Pearl was working on a story in Pakistan when he was abducted. In the video Pearl was forced to condemn US foreign policy before having his throat slit and being beheaded. The video was uploaded to a number of extremist websites in addition to at least one American shock site and the Islamic news channel Al-Jazeera. Following these uploads the video went viral and

was viewed several million times, with many shocked by its brutality and the lack of dignity shown to Pearl (Furnish, 2005; Grindstaff and DeLuca 2007). More recently, the 2013 murder of Fusilier Lee Rigby on the streets of London was recorded by passing pedestrians at the encouragement of the culprits Michael Adebolajo and Michael Adebowale. Rather than record the incident themselves, the attackers carried out their murder in broad daylight under the knowledge that passing vehicle and pedestrian traffic would stop and intervene, allowing them the opportunity to pause and give an impromptu interview to the citizen journalists and their smartphone recording devices (Nesser, 2014). News stations and terrorist websites were quick to broadcast the grisly images captured of the slain soldier and the blood-stained suspects (McGarry, 2014). It has been argued that the fact that a beheading can be recorded and shared via the Internet might be the very reason it takes place (Roger, 2013). In other words, the possibility of disseminating recordings of such acts online is influencing the types of violence terrorist groups choose to commit.

Finally, it is important to note that terrorist groups may use the Internet to inflame ongoing disputes in territories that they operate within. They may seek to incite fear or hatred by provoking sectarian, racial or religious disputes that already exist. In doing so, terrorist groups are able to destabilise regions and tie up security resources, creating vulnerabilities that may not have existed previously. The Assam Riots were an example of this, where ethnic tensions between indigenous Indian Hindus and migrant Muslims boiled over and resulted in violence that quickly followed into neighbouring areas, killing 77 individuals. Images of these riots were shared on social media, both warning and threatening Muslims to stay away lest they become victims of the next bout of violence. However, these images were not of the Assam riots, but instead were doctored and manipulated photos from other unrelated riots elsewhere in India. The publication of these images sparked fear and panic in the Muslim community, leading to a belief that violence was imminent and unavoidable (Goolsby, 2013). Three weeks after the first incident of violence, 300,000 people had fled their homes due to the panic that had gripped their communities (Gundecha, Feng and Liu, 2013).

Conclusion

The terrorists of today may not be new in terms of their organizational structures, motivations or lethality, but they do operate in a very different environment to their predecessors. The Internet has given them a far greater reach than ever before. As well as a global pool of potential recruits, operations can now be directed from overseas and training can be provided in a virtual environment. Terrorist groups now have greater opportunity to disseminate their own narratives and ideology, and to create virtual imagined communities. Attack planning is cheaper and carries less risk. There is greater potential for outsourcing and it is easier to co-ordinate multiple operations at once. The threat of cyberterrorist attacks has not yet materialized, but terrorists have engaged in psychological warfare by releasing videos of acts of brutality and inflaming ongoing disputes. There are new opportunities for fund-raising, plus it is now easier for sympathisers to make contact with terrorist groups directly to donate funds or join operations. And it is far more difficult to remove online publications from circulation and to identify those who exploit the capacity for online anonymity.

Further primary source research is required to more thoroughly understand the trends that have been outlined in this chapter. This is important in order to evaluate existing counterterrorism strategies and assess the extent to which they reflect the differences between offline and online dynamics. It will also inform the development of preventative work, including policing methods, deradicalisation and the construction of counter-narratives. Terrorists' activities in this new environment present new challenges which require new forms of response.

References

9/11 Commission. (2004). The 9/11 commission report. *Retrieved 07/04/2014*.

Abrahms, M. (2006) Why Terrorism Does Not Work. In Brown, M. E., Coté Jr, O. R., & Lynn-Jones, S. M. (Eds.). (2010). *Contending with terrorism: roots, strategies, and responses*. MIT Press.

Ackerman, S. (2013a) 'There's No Turning Back.' My Interview With a Hunted American Jihadist. Retrieved September 2013. Available at: http://www.wired.com/2013/04/omar-hammami/all/ (last visited 07 April 2014)

Ackerman, S (2013b) 'Cyber-attacks eclipsing terrorism as gravest domestic threat – FBI'. *The Guardian*, 14 November 2013. Available at: http://www.theguardian.com/world/2013/nov/14/cyber-attacks-terrorism-domestic-threat-fbi (last visited 19 March 2014).

Al Arabiya News (2014) 'Al-Qaeda women use websites to entice youth' 20 March 2014. Available at: http://english.alarabiya.net/en/News/middle-east/2014/03/20/Al-Qaeda-women-use-websites-to-entice-youth.html (last visited 20 March 2014).

Altheide, D. L. (2006) *Terrorism and the Politics of Fear.* Lanham: AltaMira Press.

Anderson, B. (1983) *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Thetford: Thetford Press.

Atran, S. (2006). The moral logic and growth of suicide terrorism. *Washington Quarterly*, **29(2)**, 127-147.

Azriel, J. (2005). The Internet and Hate Speech: An Examination of the Nuremberg Files Case. *Communication Law and Policy*, **10(4)**, 477-497.

Baldwin, T., Ramaprasad, A. and Samsa, M. (2008) Understanding Public Confidence in Government to Prevent Terrorist Attacks. *Journal of Homeland Security and Emergency Management*, **5(1)**, 1547-1577

Bayshore Networks. (2010). 'Stuxnet took $3m to write ...', 14 October 2010, available at http://www.bayshorenetworks.com/blog/?p=476 (last visited 20 March 2014).

BBC News (2003) 'Terror Link Pair Jailed' 1 April 2003 available at:

http://news.bbc.co.uk/1/hi/england/2907427.stm (last visited 17 March 2014)

BBC News (2009) 'Jail for 'suicide vest' student' 17 July 2009 available at: http://news.bbc.co.uk/1/hi/uk/8155978.stm (last visited 03/04/2014).

BBC News (2011) 'Islamic terrorist propaganda student Mohammed Gul jailed' 25 February 2011 available at: http://www.bbc.co.uk/news/uk-england-london-12576973 (last visited 20 March 2014).

BBC News (2013) 'Student accused of Harvard bomb hoax' 18 December 2013 available at: http://www.bbc.co.uk/news/world-us-canada-25425504 (last visited 10 May 2014).

Benjamin, D & Simon, S. (2003) *The Age of Sacred Terror: Radical Islam's War Against America*. New York: Random House.

Berger, J. (2012) 'Is Al-Qaeda coming back to NY?' 3 April 2012 available at: http://news.intelwire.com/2012/04/is-Al-Qaeda-coming-back-to-ny.html (last visited 06/04/2014)

Best, C. (2008). 'Open Source Intelligence' in F. Fogelman-Souie, D. Perrotta, J. Piskorski & R. Steinberger (Eds.), *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining and their Applications for Security*. 331-344. Netherlands: IOS Press.

Bobbitt, P. (2008) *Terror and Consent: The Wars for the Twenty-First Century*. London: Allen Lane.

Bosco, F. (2013). Terrorist Use of the Internet. *Capacity Building in the Fight Against Terrorism*, **112**, 39.

Brunst, P.W. (2008). 'Use of the Internet by Terrorists – A Threat Analysis'. In Centre of Excellence – Defence Against Terrorism (Ed.), *Responses to Cyber Terrorism*. 34-60. Amsterdam: IOS Press.

Brunst, P. W. (2010). 'Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet'. In M. Wade & A. Maljevic (Eds.), *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications*. 51-78. New York: Springer.

Burnett, J. & Whyte, D (2005) 'Embedded Expertise and the New Terrorism'. *Journal for Crime, Conflict and the Media*. **1(4)**: 1-18.

Cabinet Office (2013) Tackling extremism in the UK. Cabinet Office: London

Chen, H. & Larson, C. (2007). Dark Web Terrorism Research, available at: http://ai.arizona.edu/research/terror/ (last visited 04 April 2014)

Clapper, J. R. (2014) *Worldwide Threat Assessment of the US Intelligence Community*. Available at: http://www.intelligence.senate.gov/140129/clapper.pdf (last visited 19 March 2014).

Clutterbuck, R. L. (1981). *The Media and Political Violence*. London: Macmillan.

Coaffee, J., O'Hare, P., & Hawkesworth, M. (2009). The visibility of (in) security: the aesthetics of planning urban defences against terrorism. *Security Dialogue*, **40(4-5)**, 489-511.
Coll, S. & Glasser, S. B. (2005). 'Terrorists Turn to the Web as Base of Operations'. *Washington Post*. 7 August 2005.

Conway, M. (2002). 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet'. *First Monday*, **7(11)**: 4 November 2002.

Conway, M. (2006). Terrorism and the Internet: New Media—New Threat?. *Parliamentary Affairs*, **59(2)**, 283-298.

Conway, M. (2014). 'Reality Check: Assessing the (Un)Likelihood of Cyberterrorism' in T. Chen, L. Jarvis & S. Macdonald (eds) *Cyberterrorism: Understanding, Assessment and Response*. New York: Springer.

Conway, M., & McInerney, L. (2008). 'Jihadi Video and Auto-radicalisation: Evidence from an Exploratory YouTube Study'. In D. Ortiz-Arroyo et al. (Eds.) *Intelligence and Security Informatics*. Berlin: Springer

Coshall, J. T. (2003). The threat of terrorism as an intervention on international travel flows. *Journal of Travel Research*, **42(1)**, 4-12.

Crenshaw, M. (2008) 'The Debate over "New" vs. "Old" Terrorism'. In I. A. Karawan, W. McCormack & S. E. Reynolds (eds) *Values and Violence: Intangible Aspects of Terrorism*. Dordrecht: Springer.

Davis, S. (2006) Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the rule of law and Improved Tools for Cybergovernance. *Commlaw Conspectus*, **15**, 119-135.

Denning, D. (2010). 'Terror's web: how the Internet is transforming terrorism'. In Y. Jewkes & M. Yar (Eds.) *Handbook of Internet Crime*. Devon: Willan Publishing. 194-213.

Dutton, W.H. and Blank, G. (2013) *Cultures of the Internet: The Internet in Britain*. Oxford Internet Survey 2013. Oxford Internet Institute, University of Oxford

Duyvesteyn, I. (2004) 'How new is the new terrorism?' *Studies in Conflict & Terrorism*, **27(5)**, 439-454.

Enders, W., & Sandler, T. (2012). *The political economy of terrorism, second edition*. Cambridge University Press.

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission.

Farwell, J. P. & Rohozinski, R. (2011). 'Stuxnet and the Future of Cyber War'. *Survival*. **53(1)**: 23-40.

Felter, J., & Fishman, B. (2007). *Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records*. Military Academy West Point New York Combating Terrorism Center

Financial Action Task Force (2008) *Terrorist Financing*. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf> (last visited 17 March 2014).

Fletcher, G (2006) ;The Indefinable Concept of Terrorism' *Journal of International Criminal Justice*. **4**, 894-911.

Fox, S. and Madden, M. (2006) Generations Online (Demographic Report). *Pew Internet & American Life Project*

Frieburger, T. & Crane, S. (2008). 'A systematic explanation of terrorist use of the Internet'. *International Journal of Cybercriminality*. **2(1)**, 309-319.

Furnish, T. R. (2005). Beheading in the Name of Islam. *Middle East Quarterly*.

Gerges, F. A. (2009). *The far enemy: why Jihad went global*. Cambridge University Press.

Giacomello, G. (2004). 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism'. *Studies in Conflict & Terrorism*, **27(5)**: 387-408.

Goodman, S., Kirk, J. & Kirk, M. (2007). 'Cyberspace as a medium for terrorists'. *Technological Forecasting and Social Change*. **74(2)**, 193-210.

Goolsby, R. (2013). On cybersecurity, crowdsourcing, and social cyber-attack. *Commons Lab Policy Memo Series*, **1**, 9.Gorman, S. (2012). 'US Team and Israel Developed Iran Worm'. *Wall Street Journal*, 1 June 2012.

Grand Jury Indictment (1995) Timothy James McVeigh and Terry Lynn Nichols, No CR-95-110, available from: http://law2.umkc.edu/faculty/projects/ftrials/mcveigh/mcveighindictment.html (last visited 20 May 2014)

Grindstaff, D. A. & DeLuca, K. M. (2004). 'The Corpus of Daniel Pearl'. *Critical Studies in Media Communication*. **21(4)**, 305-324.

The Guardian (2006) 'Web of Hate' 4 October 2006 available from: http://www.theguardian.com/technology/2006/oct/04/news.g2 (last visited 04 April 2014)

Gundecha, P., Feng, Z., & Liu, H. (2013). Seeking provenance of information using social media. In *Proceedings of the 22nd ACM international conference on Conference on information & knowledge management*, (pp. 1691-1696).

Gunning, J., & Jackson, R. (2011). What's so 'religious' about 'religious terrorism'?. *Critical Studies on Terrorism*, **4(3)**, 369-388.

Hardy, K. (2011) Hijacking Public Discourse: Religious Motive in the Australian Definition of a Terrorist Act. *University of New South Wales Law Journal*. **34(1)**, 333-350

Hegghammer, T. (2014) Interpersonal Trust on Jihadi Internet Forums. In: Diego, G. (ed) Fight, Flight Mimic: Identity Signalling in Armed Conflicts, forthcoming.

HM Treasury (2014) Consolidated list of financial sanctions targets in the UK. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/278046/Liberia_consolidated_list.pdf (last visited 24 February 2014)

Hinnen, T. M. (2004). The cyber-front in the war on terrorism: Curbing terrorist use of the Internet. *The Columbia Science and Technology Law Review*, **5(5)**, 1-42.

Hoffman, B. (1998) *Inside Terrorism*. New York: Columbia University Press.

Home Affairs Select Committee, Roots of Violent Extremism, HC 2010-12, 1446

Home Affairs Select Committee, Counter-terrorism, HC 2013-14, 231-v

Homeland Security News Wire (2013) 'Cyberattacks more serious domestic threat to US than terrorism: FBI'. Homeland Security News Wire, 20 November 2013. Available at: http://www.homelandsecuritynewswire.com/dr20131120-cyberattacks-more-serious-domestic-threat-to-u-s-than-terrorism-fbi (last visited 19 March 2014).

Horgan, J. and Gill, P. (2013) Who Were the Volunteers? 1 The Shifting Sociological and Operational Profile of 1240 Provisional Irish Republican Army Members. *Terrorism and Political Violence*, **25(3)**, 435-456

Horgan, J., & Taylor, M. (1997). The provisional Irish Republican army: Command and functional structure. *Terrorism and Political Violence*, **9(3)**, 1-32.

Hudson, R. (1999) The Sociology and Psychology of Terrorism. Who becomes a terrorist and why? Washington DC: The Library of Congress.

Independent (2013) ''White Widow' Samantha Lewthwaite pens poem celebrating late Osama Bin Laden' 22 October 2013 available at: http://www.independent.co.uk/news/uk/crime/white-widow-samantha-lewthwaite-pens-poem-celebrating-late-osama-bin-laden-8895285.html (last visited 03 April 2014)

Intelligence and Security Committee of Parliament (2013) *Annual Report 2012-2013*. HC 547. London: The Stationery Office.

Jacobson, M. (2010). 'Terrorist Financing and the Internet'. *Studies in Conflict and Terrorism*. **33(4)**, 353-363.

Janis, I. L. (1983). *Groupthink* (pp. 2-13). Boston: Houghton Mifflin.

Jarvis, L., Macdonald, S. & Nouri, L. (2014) 'The Cyberterrorism Threat: Findings from a Survey of Researchers'. *Studies in Conflict & Terrorism*. **37(1)**: 68-90.

Jenkins, B (1975) 'International Terrorism: A New Mode of Conflict?' in D. Carlton & C. Schaerf (eds) *International Terrorism and World Security*. New York: Wiley.

Juergensmeyer, M. (2003). *Terror in the Mind of God: The Global Rise of Religious Violence* (Vol. 13). 3rd edn. Berkeley: University of California Press.

Keller, J., DeSouza, K. & Lin, Y. (2010). 'Dismantling terrorist networks: evaluating strategic options using agent-based modelling'. *Technological Forecasting and Social Change*. **77(7)**: 1014-1036.

Kennedy, H. (2006) 'Beyond anonymity, or future directions of for Internet identity research'. New Media & Society, **8(6)**, 859-876

Kenney, M. (2010). 'Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists'. *Terrorism and Political Violence*. **22(2)**: 177-197.

Kohlman, E. (2006) *The Real Online Terrorist Threat*. Foreign Affairs, **85**, 115-123

Krebs, B. (2007) 'Terrorism's hook into your inbox'. *Washington Post*. 5 July 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html (last visited 17 March 2014).

Lacqueur, W. (1999). *The New Terrorism: Fanatics and the Arms of Mass Destruction*. New York: OUP.

Langner, R. (2013) *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington: The Langner Group.

Leader, S. and Probst, P. (2003) The Earth Liberation Front and Environmental Terrorism. *Terrorism and Political Violence*, **15(4)**, 37-58

Legrand, T. (2014) 'The Citadel and its Sentinels: State Strategies for Contesting Cyberterrorism in the UK' in T. Chen, L. Jarvis & S. Macdonald (eds) *Cyberterrorism: Understanding, Assessment and Response*. New York: Springer.

Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D. & Zanini, M. (1999) *Countering the New Terrorism*. California: RAND, Project Airforce.

Mcgarry, R. (2014). Dismantling Woolwich: terrorism 'pure and simple'? Ross McGarry asks about the relationship between the 'victim', the 'criminal'and the state. *Criminal Justice Matters*, **95(1)**, 28-29.

Michel, L., Herbeck, D., & Telles, G. (2001). *American Terrorist: Timothy McVeigh & the Oklahoma City Bombing*. New York: Regan Books.

Minton, A. and Aked, D. (2013) Prevention Working Paper: 'Fortress Britian'

Morgan, M. (2004). The origins of the new terrorism. *Parameters*, **34(1)**, 29-43.

Nesser, P. (2014). Towards an increasingly heterogeneous threat: A chronology of jihadist terrorism in Europe 2008-2013. *Studies in Conflict & Terrorism*, (just-accepted), 00-00.
Neumann, P. (2009). *Old and New Terrorism*. Cambridge: Polity Press.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, **31(4)**, 418-436.

NY Times (2004) 'Madrid suspects tied to e-mail ruse' 27 April 2006 available from: http://www.nytimes.com/2006/04/27/world/europe/27iht-spain.html?_r=1& (last visited 04 April 2014)

ONS (2012) *Internet Access 2012: Households and individuals.* UK: Office for National Statistics. Retrieved September 2013. Available at: http://www.ons.gov.uk/ons/rel/rdit2/Internet-access---households-andindividuals/ 2012/stb-Internet-access--households-and-individuals--2012.html.(last visited 27 September 2013)

Paz, R. (2005). Global Jihad and WMD: Between martyrdom and mass destruction. *Current trends in Islamist ideology*, **2**, 74-86

Piper, P. (2008). 'Nets of Terror: Terrorist activity on the Internet'. *Searcher*. **16(10)**: 28-38.

Post, J. M. (1984). Notes on a psychodynamic theory of terrorist behavior.

Ramsay, G. (2009). 'Relocating the Virtual War'. *Defence against Terrorism Review*. **2(1)**: 31-50.

Rapoport, D. C. (2012) 'The Four Waves of Modern Terrorism'. In J. Horgan & K. Braddock (eds.) *Terrorism Studies: A Reader*. Abingdon: Routledge, 41–62.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
Rogan, H. (2006). *JIHADISM ONLINE - A study of how Al-Qaeda and radical Islamist groups use the Internet for terrorist purposes.* Norwegian Defence Research Establishment.

Roger, N. (2013). *Image Warfare in the War on Terror*. Basingstoke: Palgrave Macmillan.

Sageman, M. (2004) *Understanding terror networks*. Univ of Pennsylvania Press. As cited in, Horgan, J. and Gill, P. (2013) Who Were the Volunteers? 1 The Shifting Sociological and Operational Profile of 1240 Provisional Irish Republican Army Members. *Terrorism and Political Violence*, **25(3)**, 435-456

Sageman, M. (2011). *Leaderless Jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.

Schmitt, M (ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.

Spencer, A. (2006). Questioning the concept of 'New Terrorism'. *Peace, Conflict and Development*, 1-33.

Stenersen, A. (2008). 'The Internet: A Virtual Training Camp?' *Terrorism and Political Violence*. **20(2)**: 215-233.

Stenersen, A. (2013). 'Bomb-Making for Beginners': Inside al Al-Qaeda E-Learning Course. *Perspectives on Terrorism*, ***7*(1).**

Stern, J. (1999) *The Ultimate Terrorists*. Cambridge: Harvard University Press.

Sunstein, C. R. (2003) 'Terrorism and Probability Neglect' *Journal of Risk and Uncertainty* **26**: 121

Sunstein, C. R. (2005) *Laws of Fear: Beyond the Precautionary Principle*. New York: Cambridge University Press.

The Telegraph (2007a) 'Terrorists 'use Google Maps to hit UK Troops'' 13 January 2007 available at: http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html (last accessed 10 May 2014)

The Telegraph (2007b) 'Terrorist jailed over failed July 21 bomb plot.'6 November 2007 available at: http://www.telegraph.co.uk/news/uknews/1568502/Terrorist-jailed-over-failed-July-21-bomb-plot.html (last accessed 20 May 2014)

The Telegraph (2011) 'MI6 attacks Al-Qaeda in Operation Cupcake' 2 June 2011 available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/MI6-attacks-Al-Qaeda-in-Operation-Cupcake.html (last accessed 04 April 2014)

The Telegraph (2013) 'What every jihadi in Syria needs: hair gel, an iPad and KitKats' 26 Noevember 2013 available at: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/10476333/What-every-jihadi-in-Syria-needs-hair-gel-an-iPad-and-Kit-Kats.html (last accessed 10 May 2014)

The Telegraph (2014a) '700 Britons fighting in Syria terror groups, warns Hollande' 31 January 2014, available at: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/10611286/700-Britons-fighting-in-Syria-terror-groups-warns-Hollande.html (last visited 12 March 2014)
The Telegraph (2014b) 'Device exploded in bombers face after he 'forgot about clocks changing'' 2 April 2014 available at: http://www.telegraph.co.uk/news/worldnews/europe/ireland/10739277/Device-exploded-in-bombers-face-after-he-forgot-about-clocks-changing.html (last accessed 07 April 2014)

Theohary, C. A. & Rollins, J. (2011). *Terrorist Use of the Internet: Information Operations in Cyberspace*. Congressional Research Service Report for Congress 7-5700.

Thomson, I. (2014) 'Japanese cops arrest man with five 3D printed guns at home' *The Register* 8 May 2014 <http://www.theregister.co.uk/2014/05/08/japanese_cops_arrest_man_with_five_3d_printed_guns_at_home/ > accessed 22 May 2014

Tsfati, Y. & Weimann, G. (2002). 'www.Terrorism.com: Terror on the Internet'. *Studies in Conflict and Terrorism*. **25(5)**, 317-332.

Tucker, D. (2001). What is new about the new terrorism and how dangerous is it? *Terrorism and Political Violence*, **13(3)**, 1-14.

United Kingdom Government. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Cm 7953. Norwich: The Stationery Office.

United Nations Office on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes*. New York: United Nations.

United States Joint Forces Command (2010). *The Joint Operating Environment 2010*. Suffolk, VA: United States Joint Forces Command.

von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the digital era. The use of the internet in 15 cases of terrorism and extremism. London: RAND

Weber, M. (1949) '"Objectivity" in Social Science and Social Policy' in E. A. Shils & H. A. Finch (trans. and eds.) *The Methodology of the Social Sciences*. New York: The Free Press.

Weimann, G. (2004). *How Modern Terrorism Uses the Internet*. United States Institute of Peace Special Report 116.

Wilson, C. (2014) 'Cyber Threats to Critical Information Infrastructure' in T. Chen, L. Jarvis & S. Macdonald (eds) *Cyberterrorism: Understanding, Assessment and Response*. New York: Springer.

Zhang, J., Carpenter, D., & Ko, M. (2013). Online Astroturfing: A Theoretical Perspective.