Cyberterrorism

Case studies

A city comes under terrorist attack. There are several explosions and people become confused and frightened. Suddenly there is a power blackout. Simultaneously the mobile phone networks stop functioning. Citizens are unable to find out what has happened and cannot contact the emergency services. There is additional loss of life as individuals cannot access medical aid in time. Hackers disrupting the power and communication systems have heightened the fear and confusion arising from a more traditional terror attack.

A young man is unhappy with how a foreign regime is governing his country. Searching online, he discovers that he is not alone. This increases his anger – the fact that there are others who feel the same suggests to him that he is correct to be upset. He finds that he can aid in the fight against this regime by donating funds, providing information or disseminating propaganda. If he wishes, he can even join a terrorist organisation and learn terror-related skills from online videos and websites. He finds that he can contact current members of the organisation via the website, and he feels that finally he has met other people who understand his perspective.

Chapter overview

The two cases above are fictional, and thankfully the world has not yet had to respond to a threat such as the first example. However, the second example is thought to be a common occurrence; the widespread availability of the internet has resulted in considerably easier access to terrorist organisations and information than was previously available. Despite considerable academic and media interest in cyberterrorism, there is relatively little empirical work in this area. There is much disagreement regarding the definition of cyberterrorism and the extent of the danger that it poses, and the online activities of terrorist organisations are inconsistently classified as ‘cyberterrorism’ or not by various authors. The complexity of these arguments is outlined in the section on definitions below. The chapter then goes on to describe the various online activities of terrorists, which include cyberterror attacks but also recruitment, networking, fundraising and gathering and dissemination of information. The distinction between hacktivism and cyberterrorism is also described here. The chapter then goes on to
Consider the process of radicalisation, the motivation for cyberterrorism and the psychology of cyberterrorists, with particular focus on determining whether terrorists have specific personality traits or psychological abnormalities. Finally, the effects on victims are discussed.

**Definitions**

There is some disagreement among writers in the area as to what should and should not be defined as ‘cyberterrorism’, with some authors suggesting that a solid definition of cyberterrorism is elusive (for example, Gordon and Ford, 2003). Many researchers and practitioners do not believe that operational issues and planning online should be classified as cyberterrorism, and some extend this belief to attacks such as website defacements or ‘denial of service’ attacks (where a website or other online presence is rendered non-functional because of a targeted attack). Such authors feel that the term ‘cyberterrorism’ should be reserved for activities that result in death, serious injury or severe disruption.

The complexity in defining cyberterrorism is confounded by problems defining traditional terrorism (Taylor, 2012, p. 208). For the purpose of this chapter, terrorism will be considered to be the use of violence or intimidation to evoke fear in a specific group, in order to achieve a desired goal, which is often political, ideological or religious in nature. Post (1984) distinguished between two main types of terrorist groups – anarchic-ideologue groups and nationalist-separatist groups. Anarchic-ideologue groups are usually smaller, attempting to overthrow a political or social regime, mainly for ideological reasons, and there may be alienation from the terrorist’s family or immediate community. Nationalist-separatist groups are normally larger and do not generally involve estrangement from families or communities.

**Activity 9.1 Defining terrorism**

Consider the definition of terrorism above in light of previous terrorist attacks (with or without an online component). Identify the goal of the terrorist, the targeted group and the mechanism used by the terrorist(s) to evoke fear. Identify whether the terrorist group is anarchic-ideologue or nationalist-separatist in nature. Remember that terror attacks can be conducted by lone terrorists as well as groups.

Due to this disagreement in the perception of cyberterrorism by researchers, there is considerable discrepancy in the definitions that have been proposed to date. Some of these are listed in Table 9.1.

Aside from the specific definitions above, other authors have attempted to differentiate between different types of online terrorist activity. For example, Gordon and Ford (2003) describe ‘pure cyberterrorism’, where activities are carried out primarily online, as distinct from traditional terrorist activities that are carried out in offline
environments, such as recruitment. A similar argument is made by Nelson et al. (1999), who suggest that online activities such as organisation and communication should not be classified as cyberterrorism, but rather ‘cyberterror support’ or ‘terrorist use of the internet’.

Conway (2007) furthers this distinction, using a four-tiered system to classify online terrorist activity. These tiers are:

- use – using the internet to express ideas, which many internet users engage in legally;
- misuse – where the internet is used to disrupt websites or infrastructure, perhaps by hackers or hacktivists;
- offensive use – using the internet to cause damage or to steal;
- cyberterrorism – terrorists using the internet to carry out an attack which would result in violence or severe economic damage.

While it is important to remember the discrepancies in definitions used by authors, for the purpose of clarity this chapter will use the term ‘cyberterrorism’ to define those acts that could result in violence or severe economic harm (in line with the definitions proposed by Denning and Conway). The more inclusive term ‘terrorist activity online’ will also include activities such as fundraising, recruitment, organisation, dissemination and hacktivist activities by terrorist organisations. This chapter now considers several of the main types of terrorist activity online.

\textbf{Table 9.1 Definitions of cyberterrorism}

<table>
<thead>
<tr>
<th>Author</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pollitt</td>
<td>‘the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by subnational groups or clandestine agents’ (1997, as cited in Denning, 2001, p. 281).</td>
</tr>
<tr>
<td>Wilson</td>
<td>‘the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies’ (2005, p. CRS-7).</td>
</tr>
</tbody>
</table>
| Denning  | ‘The convergence of terrorism and cyberspace . . . unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not’ (2007a).
And also . . .
‘politically motivated attacks that cause serious harm, such as severe economic hardship or sustained loss of power or water, might also be characterised as cyberterrorism’ (2001, p. 281). |
Summary box 9.1 Definitions

- There is considerable disagreement as to what does and does not constitute cyberterrorism.
- Some authors, such as Denning and Conway, have suggested that the term ‘cyberterrorism’ should be restricted to attacks which could result in violence or severe economic damage.
- Post (1984) distinguished between two main types of terrorist groups – anarchic-ideologue groups and nationalist-separatist groups.
- Conway (2007) argued for a four-tiered system to classify online terrorist activity, including ‘use’, ‘misuse’, ‘offensive use’ and ‘cyberterrorism’.

Online activities of terrorists

Terrorists use the internet for a wide variety of activities. In some ways, terrorists use the internet for the same reasons as anyone else. For example, Conway (2002) reports that at least nine of the terrorists’ airline tickets used on 11 September 2001 were booked online and emails were used to distribute operational details of the attack. Wilson (2007) indicates that terrorist organisations use websites for recruitment, fundraising and training, while Maghaireh (2008) describes how some websites propagating Islamic rhetoric and ideology have online schools teaching hacking techniques. Conway (2006) describes five main ways that terrorists use the internet – information provision, financing, networking, recruitment and information gathering. Weimann (2004) also suggested that psychological warfare, publicity and propaganda, planning and co-ordination and mobilisation are also engaged in by terrorists online. Although such uses are less likely to draw media attention than pure cyberterrorism, their importance should not be overlooked. Denning (2010) claims that ‘despite the ordinariness of much of this use, the very practice of terrorism – the ways in which terrorists

Illustration 9.1 Cyberterrorism. Terrorists use the internet for a variety of activities, including information provision, financing, networking, recruitment and information gathering (Conway, 2006).
disseminate documents and propaganda, recruit and train new members, and inflict harm on their victims – is being fundamentally transformed and expanded because of the Net’ (p. 194).

This section will consider several of the main activities of terrorists online. It will firstly examine cyberterror attacks, before examining how hacktivist style attacks might be used by cyberterrorists. Following this, other online terrorist activities will be considered, such as recruitment, networking, fundraising and the gathering and dissemination of information.

Cyberterror attacks

Denning (2010) suggests that due to the lack of physical and psychological effects resulting from online terrorist use so far, even denial of service attacks are generally not labelled as acts of cyberterrorism (p. 198). Stohl (2006) argues that terrorists are using the internet and other modern technologies to enhance ease of operations, but not as a form of attack. However, that is not to say that such an event will not occur in the future. There is evidence that some of these attacks could happen. In 2009, the US government admitted that the national power grid had been infiltrated by Chinese and Russian spies, leaving software behind that could shut the grid down (Shiels, 2009).

While many writers do not think that a cyberterror attack is imminent (see, for example, Conway, 2011), there are some who disagree. For example, Leman-Langlois (2008, pp. 2–3) states that:

A ‘cyber Pearl Harbour’ is looming, with attackers targeting essential infrastructures in attempts to cripple economies. They will co-ordinate attacks on . . . targets selected to produce cascading failures along our highly interconnected infrastructures.

Similarly, Whittaker (2004, p. 123) takes a somewhat pessimistic view of what is probably the worst case scenario:

At the throw of a few switches, a saboteur, sitting in relative comfort and with highly technical equipment, can shut down power grids, unravel telephone networks, bring chaos to road and rail transport and air traffic control, and break down the operation of pharmaceutical and food processing plants. A ‘logic bomb’ can be timed to detonate at a certain hour and there will be irreversible damage to software. Computer viruses, if carefully ordered, will completely shut down an entire computer system. A computer can browse through databanks thought to be confidential. Surveillance systems will be entered, examined, and, if necessary, destroyed. Death and destruction can be brought into being at a distance with nobody hostile there to watch.

Denning (2007b) suggests that likely targets for such attacks include water supplies, power supplies (including electricity, oil and gas), communications grids, banks, transportation, essential government services and emergency services. She suggests that there are varying indicators of terrorism, including:

- execution of cyber attacks;
- cyber weapons acquisition, development and training;
- statements about cyberattacks (including declarations of intent and discussions relating to the subject);
Cyberterrorism

- formal education in information technology (particularly network and information security);
- general experience with cyberspace (such as the use of the internet for general communications and propaganda).

On this scale, Denning suggests that a failed attack against a power system is more indicative of a threat than a successful website defacement. She suggests that there is evidence for activity at the second most serious level – cyber weapons acquisition, development and training – and that some terrorist organisations train their members in hacking and engage in ‘cyber reconnaissance’ to gain information about infrastructure. Denning also indicates that some terrorist groups have employed external hackers to aid in gathering information, although it is also possible that terrorist organisations might recruit hackers directly.

Rollins and Wilson (2007) suggest that the tighter security put in place by the US might encourage terrorists to use other forms of attack, including cyberattacks. While so far these attacks have been mostly limited to email bombings and website defacements, Rollins and Wilson indicate that the US Federal Bureau of Investigation (FBI) predicts that future large conventional attacks might be amplified by cyberattacks. For example, cyberterrorists might disable the communication networks of a country while simultaneously detonating explosive devices – the disruption to communications might prevent emergency service calls, leading to a higher death toll. Wilson (2005) provides more detail on this scenario, indicating that there are three possible methods of attack:

- physical attacks – involving the use of conventional weapons directed against a specific computer facility or communication lines;
- electronic attacks – using electromagnetic energy (possibly an Electro-Magnetic Pulse, or EMP) to overload computer circuitry;
- computer network attacks – possibly using malware to infect computers and exploit software weaknesses.

There are several advantages for the terrorist organisation in employing virtual terror attacks, as outlined by Yar (2006). These include:

- allowing the terrorists to act remotely, thus reducing the impact of increased border controls and allowing the terrorist activity to occur within ‘rogue states’ that might protect the perpetrators;
- allowing small terrorist organisations with limited resources to function as more serious threats;
- using the anonymity provided by the internet as a method of reducing the likelihood of apprehension;
- using the security holes caused by lack of regulation of the internet.

It should of course be remembered that such threats do not only originate from cyberterrorists, but could also emerge from foreign governments or criminal gangs, and many countries, including the US, are putting in place greater security measures. For example, on 20 July 2012, a revised version of the Cybersecurity Act was introduced in the US Senate, seeking to make US infrastructure less vulnerable (BBC News Online, 2012).
Summary box 9.2 Cyberterror attacks

- To date, terrorists have mostly used the internet for purposes such as propaganda, recruitment, fundraising, information gathering and dissemination and networking.
- A cyberterror attack involving serious disruption, injury or loss of life has not yet occurred, and some researchers argue that it is unlikely to do so in the near future.
- Denning (2007b) suggests that likely targets for such attacks include water supplies, power supplies (including electricity, oil and gas), communications grids, banks, transportation, essential government services and emergency services.
- Denning (2007b) argues for a five-level categorisation of terror attacks, ranging from general experience of cyberspace to execution of a cyberterror attack.
- Terrorist organisations may hire external hackers, or recruit them to their organisation.
- Rollins and Wilson (2007) suggest that a cyberterror attack may be used to amplify a traditional terror attack.
- Wilson (2005) indicates that there are three possible methods of attack – physical attacks, electronic attacks or computer network attacks.
- There are several advantages for terrorist organisations using cyberterror attacks, particularly anonymity, acting from remote locations, use of security holes and allowing small organisations to function as more serious threats (Yar, 2006).

Hacktivism versus cyberterrorism

There have been several recent cases of hacktivism and hacktivist-style attacks. Campaigns by hacktivist groups have gathered considerable media attention. However, it must be remembered that hacktivists are a very different group to cyberterrorists – hacktivists are generally more interested in disrupting online activity, rather than causing destruction (Conway, 2007). The aim of hacktivist attacks is often to cause frustration and difficulty for administrators holding opposing views to the hacktivist and their group – they do not intend to cause terror as a cyberterrorist would. Because of the lack of fear evoked, Denning (2007b) argues that such activities should not be classified as cyberterrorism. However, that is not to say that terrorist activity online might not employ tactics more commonly associated with hacktivism, such as denial of service attacks.

Recruitment of new members

The widespread adoption of internet technologies allows potential recruits to become members of terrorist organisations in several ways (Conway, 2006). Information gathering is quicker and easier, and the wide variety of available formats, including video, audio and text files, makes content very accessible. For example, McDonald (2009) describes how propaganda videos for the Real IRA and Continuity IRA were easily available on video-sharing websites.
Potential recruits may also feel safer in searching for information and contacting terrorist groups due to the sense of anonymity online. New recruits could also have the option of assisting the terrorist organisation in a wider variety of ways – they may help the organisation through donations of money, software or expertise, rather than formally joining the group (Denning, 2010). Active recruitment online is also possible – the terrorist organisation may scan online chat or bulletin boards, searching for individuals who may be receptive to their cause.

The recruitment process varies from organisation to organisation. Denning (2010) indicates that different types of advice are offered by different websites and organisations. Some of these require the potential recruit to take an oath of loyalty to the organisation’s leaders, while others indicate that all that is required is a wish to join. In some cases online recruitment is targeted to specific age groups – Denning (2010) describes how there is evidence to suggest that recruitment strategies for children include games, music videos and comic-book style readings.

Networking

Many terrorist organisations attempt to work as decentralised networks of cells, thus reducing the impact on the entire organisation should one cell be infiltrated or removed. Denning (2010) describes how the internet further enables this, possibly to the extent that cells may exist that would not be recognised by the terrorist leadership. Nevertheless, the members can still communicate rapidly, cheaply and effectively using online communication (Conway, 2006). Dean et al. (2012) describe how social networking sites, micro-blogging sites and video-sharing sites can all be used by terrorist groups for networking purposes, while Bowman-Grieve and Conway (2012) examine how online discussions support communication for both new and committed dissident Irish Republicans. Use of the internet can assist the terrorist organisation in reducing the need for a single headquarters, and encourages the dissemination of responsibilities to different centres. The reduced need for telephone or face-to-face contact also reduces risks for terrorists.

Summary box 9.3 Hacktivism, recruitment and networking

- Hacktivist attacks are high-profile, but should not be confused with cyberterrorism.
- Hacktivists focus on causing frustration and disruption for specific groups, while cyberterrorists attempt to cause destruction or terror.
- However, cyberterrorists may attempt to employ tactics more commonly associated with hacktivists, such as denial of service attacks.
- The accessibility of online propaganda and terrorist organisation presence enables individuals to join organisations easily.
- A variety of media are created by terrorist organisations, and distributed through social networking sites, video-sharing sites, bulletin boards and other online formats.
- These media are used for recruitment, propaganda and networking.
Online activities of terrorists

- Online communication allows terrorists to interact cheaply, rapidly and effectively, while also disseminating responsibilities away from a central headquarters.

Fundraising

Terrorist organisations can enjoy increased financial donations as a result of an internet presence (Conway, 2006), and these organisations may encourage such donations through direct payment options, either as pure donations, or through the sale of items which may or may not be directly related to the cause. Bowman-Grieve (2011) describes how terrorist groups might also request donations of items, and that an initial donation or purchase might ‘be seen as indicative of a belief that the goals of the movement are legitimate and that their means of achieving these goals, even through the use of violence and terrorism, are acceptable. This may be a first step on the pathway toward involvement’ (p. 78). However, terrorist organisations may also use online fraud to fund their activities, or may use a charity as a fundraising vehicle (Conway, 2006).

Gathering and dissemination of information

Information is an essential part of modern life – our decisions are formed by the information we gather, and we are continuously sharing information with the people around us. Terrorist organisations also gather and disseminate information. The vast quantities of information online can be extremely useful to terrorist organisations – providing knowledge of flight times and routes, floor plans of buildings, street maps of towns and villages, pedestrian-eye views of urban areas and information about upcoming events where large numbers of individuals will be in close proximity at a specific place and time. However, as well as gathering information, terrorist organisations may also disseminate information online, sometimes as a tool for psychological warfare (Conway, 2006). This information may be disseminated on many different online venues, including websites, social networking sites and commercial networks, and using a variety of multimedia and communication tools, such as video files, audio files, boards, blogs and chatrooms (Denning, 2010). Brown and Silke (2011) discuss how dissemination of propaganda through various media outlets, including the internet, is a core activity of modern terrorist organisations.

Terrorist organisations disseminate many kinds of information, including the issuing of threats, releasing videos of terrorist leaders and terrorist activities and spreading false information. This information can reach large numbers of people very quickly, very cheaply and very easily, circumventing established media routes and circulating the information without censorship (Denning, 2010).

Terrorist organisations also disseminate information in the form of training materials, including methods of creating explosive devices and establishing underground organisations (Conway, 2006). Of course, this information might be accessed by individuals other than potential terrorists, who may use these training materials for
other purposes and causes. Some of the instructional materials online describe antiquated technologies (sometimes as much as 100 years old), but other materials describe more modern techniques, including information on computers and the internet (Denning, 2010).

Activity 9.2 Terrorist use of the internet
Using the headings of ‘recruitment’, ‘networking’, ‘fundraising’ and ‘gathering and dissemination of information’, compare how terrorist organisations would have accomplished these tasks before the popularisation of the internet with how they can achieve them now. What effect do you think these changes may have on terrorist organisations?

Summary box 9.4 Fundraising and gathering/dissemination of information
- Terrorist organisations may use an online presence to raise funds through the sale of items or the direct donation of money or goods.
- Terrorist organisations can also gather information online, through publicly available information or hacking techniques.
- Information is also disseminated by terrorist organisations through the use of various online media.
- Information disseminated can include threats, videos of terrorist leaders, videos of terrorist activities, propaganda, training materials and spreading false information.
- Information disseminated online may bypass normal media, thus avoiding censorship.

Radicalisation
There seems to be a consensus that becoming a terrorist is a gradual process, involving several stages (Horgan and Taylor, 2001; Merari, 2007; Taylor, 2012). The process of being exposed to and sympathising with radical ideology is sometimes called ‘radicalisation’, defined by McCauley and Moskalenko (2008) as ‘a dimension of increasing extremity of beliefs, feelings, and behaviours in support of intergroup conflict and violence’ (p. 415). McCauley and Moskalenko (2008) distinguished between twelve mechanisms of radicalisation, and in the majority of these, radicalisation occurs in the context of a perceived threat to an identified in-group, such as the person’s ethnic or religious group. It should be noted that holding radical views does not necessarily mean that these views will be expressed through violence (Taylor, 2012).
Attempts have been made to determine the demographic characteristics that are indicative of potential terrorists, with focus on variables such as specific religious beliefs, education, occupation, relative deprivation and low socioeconomic status. However, these tend not to be useful in predicting future terrorists, as many individuals will share the same background without engaging in terrorism (Sageman, 2004).

It is possible that a more useful method of predicting future terrorist activity involves examining a combination of factors, and it is possible that certain conditions must occur in the right combination for an individual to support or become involved in a terrorist organisation (Kruglanski and Fishman, 2006). These might include wanting to feel a sense of belonging, development of personal identity, social isolation and perception of injustice (Howitt, 2009).

One potential explanation of terrorist activity may include social learning theory (Victoroff, 2005), with the terrorist’s moral imperatives being reconstructed by what they learn from others, rather than any specific characteristics of the individual. It is important to note that this social learning may previously have been restricted to face-to-face interactions, but it may now occur through the dissemination of literature, audio files and video files online. Nevertheless, this still does not sufficiently describe radicalisation, as many individuals are exposed to such avenues for learning, without becoming terrorists.

Terrorists who are recruited online possibly experience similar psychological processes to those recruited using traditional methods. For example, Sageman (2008) suggests that online forums allow the development of a type of social identity required by terrorists. Relationships can be built through forums, and the cognitions of recruits are developed. The interactivity in the forums is important, and considerably more persuasive than passive, non-interactive websites (Sageman, 2008).

Further difficulty exists in attempts to explain why an individual may become a leader in a terrorist organisation. Again, this may be due to a combination of personality attributes. Locicero and Sinclair (2008) suggest that terrorist leaders may demonstrate ‘entrenched cognitive simplicity in one key ideological domain’ (p. 227). This suggests that, in relation to one topic, they hold fast to one way of viewing the world, possibly making diplomacy more difficult to achieve. However, Locicero and Sinclair suggest that in other domains, the terrorist leader shows much greater complexity of cognitive function, allowing for enhanced planning and organisational skills. This combination of factors may result in a highly organised, but highly focused, terrorist leader.

**Activity 9.3 ‘Lone wolf’ terrorists**

Not all terrorists join organisations – there have been many cases of ‘lone wolf’ terrorists. Research some of these cases (see, for example, David Copeland, Anders Behring Breivik, Timothy McVeigh and Theodore Kaczynski), identifying the characteristics of the terrorists, and determining why they engaged in terrorist attacks.
Summary box 9.5 Radicalisation

- Becoming a terrorist is a gradual process, involving several stages.
- The process of being exposed to and sympathising with radical ideology is sometimes called ‘radicalisation’.
- Holding such radical views does not necessarily mean that a person is engaged in violence.
- Holding specific demographic traits is not a useful predictor of terrorist activity, as many others will hold those traits without choosing to engage in terrorism.
- It is possible that a combination of factors is required for a person to be radicalised, including feeling a need to belong and to develop personal identity, social isolation and perception of injustice.
- Social learning theory may explain some cases of terrorism, though not all (Victoroff, 2005).
- Terrorists recruited online may experience similar psychological processes to those recruited offline, and those recruited through interactive forums may develop a social identity associated with terrorism more strongly than those who only passively view non-interactive content.
- Terrorist leaders may experience extreme cognitive simplicity in an ideological domain, while demonstrating enhanced planning and organisational skills (Locicero and Sinclair, 2008).

Motives of terrorism and cyberterrorism

Motives of terrorism vary greatly – some terrorists and terrorist organisations are motivated by ideological reasons (such as prevention of animal cruelty, or anti-abortion groups), while others are motivated by ethnic or religious reasons (such as Al-Qaeda or Hamas). Whatever the ultimate goal of the terrorist organisation, Horgan (2005, pp. 1–2) indicates that:

very often, it seems that the goal of terrorism is simply to create widespread fear, arousal and uncertainty on a wider, more distant scale than that achieved by targeting the victim alone, thereby influencing the political process and how it might normally be expected to function.

Horgan suggests that most terrorist movements seek to overthrow or destabilise a target regime or influence, and that most are relatively small. He indicates that the goal of inducing terror is important – for example, the most important outcome for the terrorists of the attacks on 11 September 2001 was not the deaths of those killed in the attacks, but the 'humiliation of the American government and the subsequent psychological arousal for the greater populace' (Horgan, 2005, p. 2). It should therefore be asked: can a similar reaction be obtained through the use of information technology as a terrorist tool?

Both Veerasamy (2010) and Colarik and Janczewski (2008) suggest that online terrorist activity is best understood by examining the motives of traditional terrorist activity, particularly the generation of fear. Colarik and Janczewski (2008, p. xv)
Psychology of cyberterrorists

specifically refer to the ‘spectacular factor’, potentially resulting in negative publicity or direct losses. A third motive of an attack such as a denial of service might be to emphasise the vulnerability of an organisation, demonstrating weakness in the system. Hacking may also be used to steal information or make political statements about the entity being attacked.

Summary box 9.6 Motives of terrorism and cyberterrorism

- Terrorist organisations have different motives, but the goal of terrorist acts is to create fear and uncertainty among people other than the direct victim of an attack.
- Cyberterrorism is generally motivated by similar goals, but may also hope to demonstrate the vulnerability of an organisation, make political statements, steal information or bring about negative publicity or direct losses.

Psychology of cyberterrorists

There has been very little empirical research examining the psychology of terrorism, with most writings to date being theoretical or based on literature or anecdotal observations (Silke, 2008; Victoroff, 2005). Nevertheless, there has been an increase in terrorism-related research since the attacks on the US on 11 September 2001 (Silke, 2008).

There are several reasons why empirical research on the psychology of terrorists is rare:

- it can be difficult to find terrorists;
- even when terrorists are found, it can be difficult to find those willing to participate in a psychological study;
- studying incarcerated terrorists also holds some difficulty, as it is necessary to get approval from relevant authorities;
- travel expenses could be prohibitive;
- there may be difficulties in gaining approval from ethical boards;
- there could be a language barrier;
- there may be a risk of personal harm to the researcher, through directly contacting terrorists or because of travel to unstable regions.

Nevertheless, there has been some interesting research on the psychology of terrorism. Here, particular focus will be placed on the personality traits of terrorists and the potential for psychological deviance in terrorists. Finally, the possible similarities and differences between traditional and cyberterrorists will be considered.

Personality and profile

Potential demographic characteristics that might lead to radicalisation have already been discussed, but it has also been suggested that engagement in terrorist acts might be associated with some personality traits, such as having a sensation-seeking personality or subjective feelings of humiliation (see, for example, Victoroff, 2005; Zuckerman,
2002). However, empirical evidence has failed to support the existence of specific personality traits in terrorists (Horgan, 2003a, 2008; Howitt, 2009; Silke, 2003; Victoroff, 2005; Wilson, 2010).

Nevertheless, it is possible that even if terrorists do not have unique personality traits, the study of personality may still be important. Kruglanski and Fishman (2006) distinguish between terrorism as a ‘syndrome’ (a ‘psychologically meaningful construct with identifiable characteristics on individual and group levels of analysis’, p. 193) and terrorism as a ‘tool’ (representing ‘a strategic instrument that any party in a conflict with another may use’, p. 193). If terrorism is a syndrome, then it is possible that distinctive personality traits, motivations, and socialisation histories could be associated with terrorists, and that findings about one terrorist group could be generalised to other groups. If, however, terrorism is found to be a ‘tool’, then it provides little psychological insight into the terrorist or organisation – terrorism is just a means to an end, though it may still be of interest to determine why the individual chose terrorism as the means of achieving a goal, over other tools such as diplomacy or peaceful protest.

Kruglanski and Fishman indicate that there is little evidence to support the ‘syndrome’ theory of terrorism, and so the ‘tool’ view is probably more appropriate. This insight is important, as it suggests that the phenomenon can be studied in terms of means–end analysis – if potential terrorists have access to an alternative ‘tool’ of obtaining their goal, which is preferable to terrorist activity, then it is likely that they might choose that ‘means’ instead. It also suggests that if terrorism is not expected to be a successful means of obtaining the goal state, then it will not be utilised. Because of this, the ‘tool’ theory of terrorism is still very important from a psychological perspective, as elements of cognitive psychology, such as decision making and perception, can play an important role in understanding terrorist activity. Some research has determined that the gradual socialisation associated with terrorist groups is often accompanied by an increasing disillusionment with other means of achieving desired goals (Kellen, 1982; Taylor and Quayle, 1994).

Some of this examination of the cognitive psychology of terrorists has been done by Max Taylor and Ethel Quayle (1994), who suggest that terrorists may make fundamental attribution errors regarding their perceived oppressors, increasing their likelihood of becoming actively engaged. Similarly, Victoroff (2005) suggests that rational choice theory might help to explain the behaviour of terrorists, but again this does not explain why the vast majority of people who might have a desired objective do not engage in terrorism, even though it might help to achieve their goal. It may be that cognitive inflexibility or diminished executive functions might also play a part (Victoroff, 2005), and awareness of this might be helpful for negotiators.

Cognitive psychology should not be considered in isolation when discussing terrorist psychology – it is also useful to consider how social psychology can inform our understanding. Group dynamics are a very important aspect of terrorist organisations (Victoroff, 2005). The organisation provides support to the individual from others who have similar goals. They provide the terrorist with a well-defined role and a sense of purpose. The organisation also enables the terrorist to see behaviours that would otherwise go against social norms as acceptable. It is important that the group identity...
is not underestimated: as Post et al. (2003) describe, ‘an overarching sense of the collective consumes the individual. This fusion with the group seems to provide the necessary justification for their actions, with an attendant loss of felt responsibility’ (p. 176).

As with many other types of offenders, terrorism is probably determined by a combination of many factors, including developmental factors, biological factors, cognitive processes, cognitive capabilities, environmental influences, personality and group dynamics (Victoroff, 2005). Without further empirical research, it is unlikely that a full understanding of terrorist psychology can be developed. However, Victoroff (2005) suggests four traits which might characterise ‘typical’ terrorists:

- high affective opinion regarding an issue;
- having a personal stake that separates them from others holding the same opinion (such as a sense of personal oppression, a strong need for vengeance, or a drive to express aggression);
- low cognitive flexibility, with an elevated tendency towards attribution error;
- ability to suppress moral constraints against harming innocent people.

This is an interesting theory, but it requires considerable testing in order to ascertain validity.

Psychological abnormalities

It was once thought that terrorists were likely to hold psychopathic personality traits, but more recent research suggests that this is unlikely to be the case (Horgan, 2003b; Silke, 1998; Victoroff, 2005). Suggestions of any abnormal tendencies seem to be based mainly on anecdotal cases or secondary sources (Silke, 1998). Even suicide terrorists may not be clinically abnormal, although a multidisciplinary approach must be adopted to comprehend such attacks, involving historical, economic, political, psychological and anthropological factors (Post et al., 2009). For example, a person may volunteer for a suicide attack following a lengthy process of disillusionment with an oppressing regime, during which they lost one or more loved ones. Victoroff (2005) concludes that terrorists do not usually exhibit any major psychiatric disorder or personality disorder, although some individuals with antisocial tendencies might use affiliations with terrorist groups to hide their aggressive tendencies.

Activity 9.4 Terrorist psychology

As demonstrated above, it is probably impossible to develop a list of terrorist attributes. However, as with most types of offenders, it is possible to list factors that may contribute to a tendency to choose terrorism over other methods in order to achieve a goal. List some of these factors under the following headings suggested by Post et al. (2009) – i.e. historical, economic, political, psychological and anthropological. Are there any other headings that might also be appropriate?
Comparison to offline terrorists

Understanding the psychology of terrorists in general is difficult, but it is even more problematic to consider the psychology of cyberterrorists. No in-depth psychological studies of this specific group have been completed to date, but some tentative hypotheses can be suggested.

It is possible that cyberterrorists might be very different to those who engage in traditional terrorist activities. Cyberattacks may allow non-violent individuals to support terrorist campaigns, thus expanding the organisation’s potential for harm (Denning, 2010). A person may be attracted to cyberterrorism due to the relative lack of risk when compared to traditional methods of attack (Denning, 2001). As a result of these factors, a cyberterrorist may be a new type of individual in a terrorist organisation, attracting people who would not otherwise have become actively involved.

It is also possible that the possibilities of cyberterrorism may encourage the formation of new terrorist groups (Gordon and Ford, 2003). This could be due to the relatively small amount of finance required, and the fact that such a group could be quickly and easily organised. Gordon and Ford also suggest that the anonymity offered online could be advantageous for terrorist activities.

Summary box 9.7 The psychology of cyberterrorists

- There is relatively little empirical research on the psychology of terrorism, for several practical reasons.
- Empirical evidence has failed to support the existence of specific personality traits in terrorists.
- Kruglanski and Fishman (2006) distinguished between terrorism as a ‘syndrome’ and as a ‘tool’.
  - a syndrome is a ‘psychologically meaningful construct with identifiable characteristics on individual and group levels of analysis’ (p. 193);
  - a ‘tool’ represents ‘a strategic instrument that any party in a conflict with another may use’ (p. 193);
  - there is little evidence for terrorism as a syndrome, but the concept of it as a tool is useful, especially in relation to cognitive factors such as decision making and perception.
- Group dynamics are another very important aspect of terrorist organisations.
- Terrorism is probably determined by a combination of many factors.
- While it was previously thought that terrorists would hold an abnormal psychological profile, this does not generally seem to be the case.
- Cyberterrorists may be very different to those who engage in traditional terrorist activities, due to the different nature of the attack (possibly non-violent and low-risk for the terrorist).
- Cyberterrorism may also encourage the formation of new terrorist groups.
Effects on victims

It is very difficult to predict what the effects of cyberterrorism might be on victims, due to the lack of a successful cyberterrorism attack to date (at least, according to the definition suggested by researchers such as Denning, 2007a). For traditional acts of terrorism, there can be considerable impact on those directly affected, with both DiMaggio and Galea (2006) and Gabriel et al. (2007) finding high rates of mental health problems following high-profile traditional attacks. Such problems can extend not only to those injured or present at the attacks, but also to those in the local area, or those who knew victims of the attacks. While post-traumatic stress disorder (PTSD) was prominent, other psychiatric disorders were also noted in those affected.

It is important to note that the threat, or perceived likelihood, of a cyberterrorist attack can also affect society. Stohl (2006) indicates that there has been a gap between the presumed threat of cyberterrorist attack and known online terrorist activities, but suggests that this may be partially caused by confusion between hacktivism and cyberterrorism and a failure to distinguish between cyberterrorist attacks and online terrorist activity. For this reason, it is important that media reporting relating to such activities is conducted responsibly, to prevent fear of cyberterrorism being unnecessarily raised in the general public (media reporting of criminal events has been shown to impact on public perceptions of crime; see, for example, O’Connell, 2002). More importantly, Brown and Silke (2011) describe how certain types of media reporting might escalate terrorist activity, and it is possible that the same might be true for cyberterrorism.

Summary box 9.8 Effects on victims

- As there has been no successful cyberterrorism attack to date, it is difficult to predict what the effects on victims might be.
- Those affected by traditional terrorist attacks can experience high rates of mental health problems, such as PTSD.
- But the perceived likelihood of a cyberterrorist attack can also affect society, raising fear levels.
- Media reporting of cyberterrorism and cyberterrorist risk should be carefully undertaken to avoid unnecessary fear.

Conclusion

The topic of terrorism, and cyberterrorism in particular, requires considerably more empirical research, but the practical difficulties with carrying out such work continue to impede large-scale studies. It should also be borne in mind that it seems unlikely that cyberterrorism will ever be as significant a risk as more traditional forms of attack, although a hybrid attack may cause considerable panic, disruption and/or loss of life.
It is also important that the role of the internet in terrorist activity generally not be underestimated – its facilitation of recruitment, information gathering and dissemination, networking and fundraising results in easier organisation of terrorist activity in general. As Wykes and Harcus (2010) state, the internet ‘is the public space of the twenty-first century. Its global reach, chaotic structure, ease of access, anonymity and our increasing dependence on it for the information, education, entertainment and communication it offers makes it appear to be both a perfect tool for terrorists and site of terror activity, worldwide’ (p. 216).

**Essay questions**

(1) ‘Cyberterrorism’ should only refer to attacks that are violent or cause economic disruption. Discuss.
(2) Are terrorists psychologically normal?
(3) Are there qualitative differences between traditional terrorists and cyberterrorists?
(4) Compare and contrast online and offline radicalisation techniques.
(5) Does media coverage of cyberterrorism create unwarranted fear?

**Additional reading**

**Books and articles**

Robert Uda’s (2009) book *Cybercrime, Cyberterrorism and Cyberwarfare* examines cyberterrorism from policy, strategy and defence perspectives, but without a primary focus on psychological issues.

Jeff Victoroff and Arie Kruglanski’s (2009) book *Psychology of Terrorism: Classic and Contemporary Insights* compiles many key papers examining key issues in the psychology of terrorism, such as radicalisation, motives and behaviour of terrorists.

Andrew Silke’s (2011) book *The Psychology of Counter-Terrorism* considers several aspects of terrorism and psychology, along with dedicated chapters on the impact of media and the internet on terrorism.

**Websites**


The Federal Bureau of Investigation provides resources on terrorism and counterterrorism: www.fbi.gov/about-us/investigate/terrorism.

The United Nations provides resources on counter terrorism: www.un.org/terrorism.

*The Economist* includes a collection of articles on terrorism: www.economist.com/topics/terrorism.