Cyber Terrorism:
A New Dimension in Battlespace

Major J P I A G CHARVAT
SO2 Course Director
Centre of Excellence Defence Against Terrorism

Abstract. This paper discusses the concept of terrorism, who the terrorists are and develops an understanding of why they conduct the activities they do. Understanding the *mens rea* of the attacker will allow consideration of the type of attack they may plan and the effect they are likely to try and achieve. It looks at the main motivations of terrorist groups and discusses their use of the Internet for various aspects of a terrorist campaign such as propaganda and recruitment. It will consider the various tactics that have been used and how the Internet has provided a new opportunity for terrorists to conduct their campaigns and how it has been adapted by them for their purposes. It examines the potential threat of a cyber attack by terrorist organizations and how they can use the Internet and Cyber Space to attack a target with similar results to a conventional physical attack. The paper will briefly discuss some of the possible defences against this form of terrorism.

Keywords. Terrorism, Terrorist motivation, Cyber attack, Terrorist use of the Internet

Introduction

Since the 2001 attacks on the United States there has been a significant effort from NATO and its partners to address the issue of International Terrorism. Terrorism has many different types and there is no profile that consistently fits either a terrorist organization or an individual terrorist. Terrorism is an adaptive threat and will constantly look for weak points in the state or organization it is attacking. Cyber Space and the Internet are providing an emerging battleground that many terrorist organizations are trying to exploit as a means of furthering their campaigns or actual attacks using an electronic medium. As developed societies become increasingly reliant on electronic communications, control systems and commerce the potential for a terrorist to hit the target becomes a more realistic possibility. As with a conventional attack or command and control medium, the Internet now offers genuine targets that will become attractive to certain terrorist organizations for certain acts. Just as when defending against conventional terrorism, cyber systems can be secured and any potential threat investigated using electronic evidence to catch the instigators.

1. Defining Terrorism

Most people would say they know what terrorism is, but surprisingly there is no internationally agreed definition. There are literally hundreds of different definitions in current use with the use of violence or threat of violence being the only general common theme [1]. The only other elements to appear in more than 50% of definitions are "Political" and "fear, terror emphasized" [2]. This is a hamper on international cooperation as some terrorist organizations are seen as legitimate fighters by some countries. Terrorism does differ from other crimes in its *mens rea*; it is done with a purpose and a specific strategic outcome in mind.

If there has been significant international and intellectual disagreement about a definition for terrorism itself, the disagreement as to what, if anything, constitutes Cyber Terrorism is even more diverse. This paper will consider the battle against terrorism in Cyberspace, Cyber Terrorism as a form of attack and the terrorist use of the Internet as a tool for physical action. It will also consider areas of both anti and counter terrorism within a cyber environment.

It is important that we consider who the terrorists are. There are literally hundreds of groups of varying size and ability, which, to some extent, warrant the label of terrorists. Terrorism has 4 classic motivations [3]. Firstly there are single-issue terrorists, those who believe in a particular cause and are prepared to use violence to protest their message in the hope of ending the issue, which sparks their grievance. Animal Rights and Anti-Choice over abortion are the two most prevalent of such issues. Vivisection researchers or family planning workers have been the targets of sustained campaigns and assassinations in protest over these issues. Although generally small and with a low lethality rate, these groups could find the cyber world particularly to their liking as in the cyber environment they can effectively punch above their weight. Ideological Terrorists are those who use violence to promote their political ideology, usually from the far left or right. While these groups were most active in the Cold War, there are still several of such groups still active[1] and other active groups that have evolved from their beginnings as an Ideological Terrorist group.[2]

Nationalist terrorists have been the most lethal of all terrorist groups over the last 40 years[3] [4] and are still active in several major campaigns worldwide. These are terrorist groups who seek independence from a state or to cede from one state to another because of ethnic or geographic grievances. Very few modern nations are made up of just one ethnic group and in many areas of the world this has led to ethnic tensions that have spilled over into terrorism. The LTTE in Sri Lanka and the PKK Kongra/Gel[4] terrorist organization in Turkey are the most active of such groups.

Religio-Political terrorist groups tend to be more lethal as they believe they are acting for God or on a divine order and that those not of their belief are against God [3]. There are extremist groups spanning all major religions and some minor cults who have resorted to

1 FARC (Revolutionary Armed Forces of Columbia) are probably the most active today.
2 The PKK Kongra/Gel terrorist organisation, active in Turkey, began seeking a socialist revolution in that country.
3 Religio-Political groups have been more lethal over the last 5 years.
4 The EU lists LTTE and PKK as terrorist organizations.

terrorism. These terrorists have abused their religion and act outside it, they must not be confused with the religion they misrepresent in their claims. Although many religions do accept that there are circumstances for justifiable violence or warfare, none, with the exception of a doomsday cult such as Aum Shinrikyo, would apply this to the indiscriminate targeting of civilians or security forces outside the legal conventions of legitimate warfare.

As with any definition labelling model, there can be hybrid terrorist groups that either evolve their motivations or have multiple aims. The Provisional IRA are an example, they were a Nationalist group as they wanted Northern Ireland to cede from the United Kingdom to the Irish Republic but were also an Ideological group as they wanted Ireland to become a Socialist state.

The terrorists themselves must be considered, understanding their psychology is important in understanding how to defeat them. There is no clear profile of a terrorist, they come from all walks of life and have varying levels of education, employment and wealth. One common factor is that they are not mentally unstable, terrorist organizations want activists with the ability to think and be reliable. The level of intelligence may decide the role of the terrorist, as will any specialist skills such as chemistry or IT, and the organization will require College level members as well as those with more basic standards of education. We must accept that most terrorist groups are made of skilled and intelligent people who are acting out of genuine belief (self-formed or indoctrinated) and not a group of clueless idiots. This must be considered in the cyber defence plan against terrorism, they will study, take time, plan and employ experts of the highest calibre to achieve their aim.

2. Terrorist use of the Internet

Terrorists use the Internet for a variety of reasons that although nothing new *per* se make their business far simpler and have a far wider reach than through non-electronic means. Cyber Space offers many areas of potential exploitation to terrorist organizations. It is a tool for recruitment, radicalization, propaganda and fund raising as well as offering quick and simple command and control. Undoubtedly the Internet and electronic mediums offer many advantages to terrorists, given the ease of use and the increased reliance of developed societies on the Internet the potential for terrorist exploitation is expanding daily.

The first area of concern is the terrorist use of the Internet. By this I mean a medium for many aspects of terrorism other than as an attack tool, which will be discussed later. There are many features of terrorism that can be conducted through the Internet, although this is primarily an information and communication medium it does allow a greatly extended reach and far quicker communication. Terrorism is a politically motivated act and therefore requires publicity and a forum of communication. The key areas of exploitation in modern terrorist use are propaganda, recruitment, radicalization, communication and research. The Internet allows small groups or individual terrorists the opportunity to reach literally millions of people very easily. “Perhaps one of the most promising features of the Internet is that it gives voice to many who have been unable to buy or generate media attention” [5].

Propaganda is essential to terrorism, these are rational people who carry out their campaigns for a political or social end state, they must have a medium to explain their message and 'justify' their actions. Before the Internet this was relatively difficult to achieve for a mass audience. Television and print media would run stories on terrorists but these would be subject to editorial control and sometimes to legal restrictions. Books, magazines and pamphlets would only hit a small audience and would only really be read by those with an interest in the terrorist's cause. The World Wide Web is unregulated and accessible to almost everyone. Internet Cafes are increasingly popular and allow access to the public without the need for the ownership of a computer or subscription to an Internet Service Provider. Simply by adding the correct key words or links via a seemingly mainstream site, the terrorist organization can easily display its message without regulation. It can allow the key grievances, which motivate the terrorists, to be publicly aired, and as they control the content, these can be backed up with 'proof' manufactured and edited by the organization. These sites look official and will use multimedia to attract attention and create an air of legitimacy for the site visitor. They also have the advantage that their Information Operations are not bound by truth or conventions, which allows, with appropriate editing, a seemingly convincing piece of propaganda without any real basis. By May 2005, using only the US State Department's list of terrorist organizations, there were over 4500 terrorist supporting websites [5], rising to 5500 in 2007 [6].

An example of how easily websites can be used for misinformation is the German *Bund Deutscher Juristen*[7]. This website for the German Lawyers' Association ran an article about their Chairman, Dr Claus Grötz, quoting that he said the possible use of testimony gained after light torture could be used in German courts. There was public outcry and headline news calling for his resignation. The site had only been set up 2 days before the 'story' broke and neither the Association nor Dr Grötz actually existed. Although this is not a terrorist example, it highlights the possibilities that a terrorist organization could exploit. Lazy journalism meant that the story was not corroborated and given to the German public as authentic by the mainstream media. To have this about a State's action relating to a terrorist situation could be used by the terrorist organization to gain public sympathy and international condemnation of the victim state.

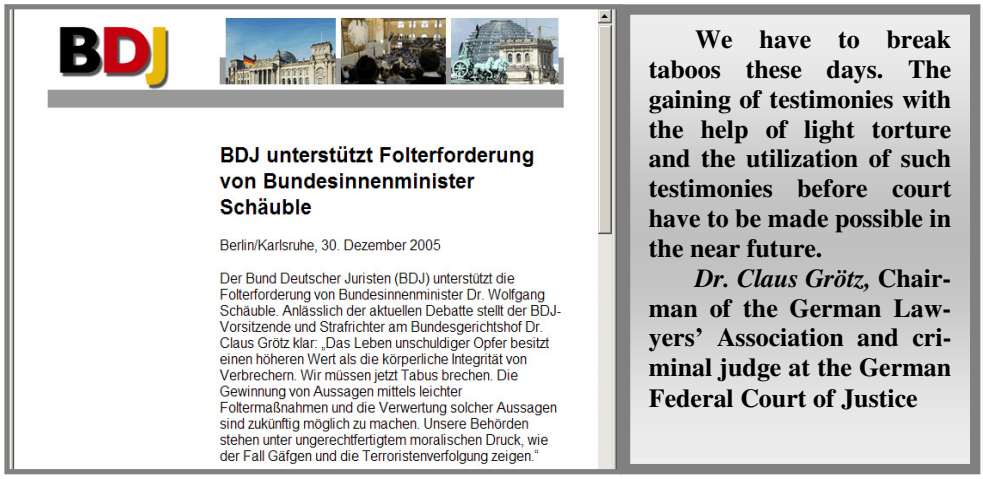

Figure 1. Screenshot of BDJ website and translation

Recruitment and Radicalization are an essential element for a terrorist organization. The Internet provides a greatly enhanced forum for this. The ability for terrorists to find and groom young people is demonstrated in Forum and Chat Room websites. This provides a largely unregulated medium for terrorists to meet and groom potential recruits. Often they will monitor those Forums and Chat Rooms that may have a relevance to their motivation, grievance or cause. This could be an animal rights Chat Room where extremists Single Issue terrorists may use the opportunity to engage anyone who shows thoughts or emotions along the same lines. This form of contact can be well orchestrated and involve several people, effectively keeping the potential recruit in an air lock away from the terrorist proper until they are deemed ready. Initially a pro-terrorist 'chatter' will engage the potential recruit in fairly mainstream conversation and ask a few probing but seemingly innocent questions over a period of time. They will use this time to pass on pro-terrorist messages and try to affirm the potential recruit's feelings to that particular cause. The will also post messages against the terrorist's targets in an attempt to convince the potential recruit that the terrorist message is accurate.

Once regular contact is made, the initial contact will assess the potential recruit and pass them on to a groomer. Those selected for such grooming have already displayed some form of agreement with the terrorist cause and also the personality traits that suggest they may be willing to take an active part in any struggle. Still at this point the potential recruit is unlikely to know she or he is in contact with anyone other than a fellow chatter of a like mind and engaging in serious conversation. The groomer is likely to be very knowledgeable about the cause and will start to feed strong propaganda about the terrorist's motivation. This is again a filtering process to find out those who would continue towards direct action from those who have strong views but would never cross from political protest. Those who are regarded as strong believers in the terrorist cause, and displayed the correct personality traits to suggest they would join are then passed on to their first proper contact with the terrorist organization itself. This process can take a long time, as the groomer has to be certain they have the right people and the potential recruit is not going to be made aware that he or she is in contact with a terrorist until they are ready.

The groomer will pass the potential recruit onto a recruiter who, at that stage will, for the first time, make indications that they are from a terrorist organization. From this point the skill set of the potential recruit will be examined and their commitment finally checked before they are in a position to ever actually meet or know the identity of anyone they have been engaged with.

An example of this, in its early stage was monitored on a mainstream Muslim Youth website in the United Kingdom.[5] Hussain was a 15-year-old schoolboy who posted a school project for comment from other members of the forum site. In his post he expressed mixed feelings and uncertainty about how the West saw Islam and the true nature of the Jihad. Hussain stated that he believed Jihad was a personal struggle and it was against Islam to kill. He also expressed that he felt as though the West regarded him as a terrorist because he was Muslim and that there was significant anti-Muslim sentiment in Western Society. The

[5] This case was monitored by the author, the website name is withheld as it has no association with terrorism and quickly banned OBL4caliph from the site. There is no evidence OBL4Caliph directly represented or was a member of any terrorist organization.

first two replies agreed with Hussain that in Islam it is forbidden to kill innocents. OBL4Caliph entered the debate and began saying that he was an authority on Islam and that Jihad was a duty for all Muslims and that it was a requirement to kill those who opposed the religion. During the ensuing posts it was clear that most forum members said OBL4Caliph was wrong. However his language and argument were more structured to a youth's mind and he began to try and convince Hussain. While clearly Hussain had used the Internet for a sensible and reasonable purpose, canvassing views of like-minded people about his thoughts as a confused teenager, he had inadvertently shown a little potential in his thought, which led to a potential terrorist grooming.

Terrorism has evolved and in the beginning of the 21st Century we are dealing with a new type of terrorist organization as well as the classical groups. Traditionally terrorist organizations have been just that, an organization with a leadership and strict control. Attacks and campaigns would be planned and authorized by the leadership as part of a coordinated approach to their policy. The emergence of more 'networked' organizations with a horizontal leadership has made the Internet a breakthrough in Command and Communication. Obviously e-mail is an instant form of communication and can easily be encoded. Seemingly innocent messages can be sent that only the recipient would understand, although a coded message is as old as terrorism itself, email allows much greater speed in delivery and an almost guaranteed receipt. An example was a mail sent by the 9/11 hijacker Mohammed Atta:

> "*The semester begins in only three more weeks. We've obtained 19 confirmations for students in the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering.*
>
> *Best wishes from the Professor to all of you!*
>
> *Mohammad*" [7]

Clearly this message seems innocent, but knowing the events of 9/11 and who wrote it, we know this set the attack dates (it was written 3 weeks before the attacks), the 19 confirmations were the 19 terrorists who were carrying out the atrocities, the 'faculties' were codes for the targets and this confirmed which ones, and of course the 'professor' is Osama Bin Laden.

The Internet also offers a unique opportunity for people to meet likeminded others despite geographical separation. Via forums, chat or other emerging methods such as Twitter or Facebook, unconnected and uncommon 'radicals' could easily contact other uncommon radicals and find a common virtual space online.

Messages can be hidden in pictures or a made to look like Spam mail so not to attract attention. Terrorists have also been known to set up an email account and change the password daily, the cells and terrorists will know the username and daily password. Messages can be written, saved as a draft and then accessed by the whole network without being sent. This greatly reduces the possibility of interception or an evidence trail before or after an attack.

Simple symbolism is also a known method of terrorist communication. Many terrorist organizations have websites or will publish video clips on video sharing sites. These can

contain a hidden code; simple graphics such as a terrorist holding his or her AK47 in the left hand will be displayed. Having the same graphic with the rifle in the right hand can be a signal for a terrorist cell and be almost undetectable to the intelligence services monitoring it.

Training and Research & Development are essential elements for a terrorist attack. The Internet provides easy and immediate information sharing and research capabilities to a Terrorist organization. There have been numerous examples of terrorists posting training manuals on the Internet, which explain how to conduct attacks and make explosives using readily available high-street ingredients. This has a greater appeal to network organizations with horizontal hierarchies, such as al-Qaeda. These organizations would be content for cells, even with no formal contact with the organization proper, to conduct attacks in their name. Their philosophy is espoused on-line and those who are radicalized to support it could become competent terrorist without physically going to a training camp. Publications such as the Terrorist Cookbook provide the know-how that a budding terrorist would need.

Fund raising for or by a terrorist organization is another area where the Internet provides a quick and simple medium for the organizations. In the modern world of electronic banking this can be achieved directly or indirectly, both via legitimate transitions and illegal means. The Internet offers many opportunities for front business and pseudo-charities to raise monies. It also allows easy transfer, internationally, to make the tracking and freezing of suspect terror funds very difficult. In some examples, charities have been set up for disaster relief, such as the devastating earthquake in Pakistan in 2005. While these charities have done some relief projects, some of the funds were siphoned off to terrorist organizations. If $100,000 is set aside to build a school, the actual relief could be $800,000 with 20% going to terrorism. These 'charities' can be easily set up by terrorist supporters and be indistinguishable from genuine relief work. The Internet allows a wide target audience for donation requests and easy transfer to the 'relief' fund. At a time of such disaster considerable amounts of money can be stolen in this way.

3. Terrorist Cyber Attack

There are many who argue that there is no such thing as Cyber Terrorism proper. Terrorists can use the Internet as discussed above, but Terrorism needs to be a tangible physical attack. I would disagree, there are many features of modern life that are reliant on Cyber Space and present a new opportunity for terrorist direct action, and these opportunities are increasing as we become reliant on computers. There are the possibilities of attacking electronic means such as web-defacement, malware, data mining, training and Denial of Service. As SCADA becomes more widely used and controls important key infrastructure, an attack on these could be as physical as a bomb.

Web-defacement is an easy way to annoy a target or gain propaganda. Unlike a spurious site, such as the BDJ, these attacks alter the data and information on an official site. The ISP and web domain name would prove to be official if they were checked.

While simple altering of an official website gains little more than small scale propaganda, there is a potential to cause real panic. The often given scenario is a terrorist

defacing the Homeland Security website and advising people to leave a major city due to a chemical leak. If picked up by the press or enough people, this false message could gain legitimacy and cause panic, with untold casualties in the ensuing rush to leave and the obvious financial implications that would cause. This sort of attack is relatively unlikely to succeed as other forms of warning would not back it up, but if a TV network accidentally picked it up it could be damaging. The increase in popularity of 'New Media' does allow a greater potential for this type of scenario as it as unregulated and can lack the responsibility of confirming a source that traditional media would have. Social contact media such as Twitter could inadvertently spread false information and be taken as genuine. Although most users are responsible and corrective information will quickly appear a botnet giving mass 'tweets' may give legitimacy through weight of numbers [8]. This is a very simple action for a skilled hacker Cyber Terrorist with very little risk or cost.

Malware is an obvious weapon that a cyber expert terrorist could unleash. Viruses and works can bring down systems and networks and cause great disruption to the target. These could render an important operating system temporarily useless or make it malfunction. The potential loss of data through such a virus or work could have a huge implication if targeted correctly.

Data mining is an appealing prospect for a terrorist organization and an area where INFOSEC becomes a priority for governments and security services. Increasingly personal and financial details are held on record in electronic files. Often, for ease of use and legitimate information sharing, these are held on networked systems. Terrorist organizations could attempt to hack in to these systems to gather information about potential targets, financial details or indeed information altering to damage the victim organization. This could be used to identify key individuals to target for assassination or kidnap. It could also find details, which it used to discredit or blackmail key personnel to help with a terrorist activity. Identity theft could allow a terrorist access to bank, identity documents or access control passes which could be severely damaging and greatly assist in an attack. Given the ease and size of modern data transportation mediums, such as flash USB sticks, the loss of this information must be guarded against in all electronic forms. In the United Kingdom the membership list for the right wing British Nationalist Party was made available on the Internet, much to the embarrassment of several high profile members whose membership of this party was proscribed by their employers[6]. There are many such types of information, which could be of use to a terrorist organization. They can also learn about the schedules and locations of targets. According to an al-Qaeda training manual captured in Afghanistan "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy"[6].

Seemingly innocent programmes and tools on the Internet can provide valuable information to a terrorist planning a physical attack. These are in everyday use by millions of Internet users for wholly legitimate purposes. Programmes are easily available that offer satellite imagery of the world. These offer exact details of often-sensitive areas and can allow accurate target selection and area knowledge without the risk of reconnaissance. Indeed the al-Qaeda computer expert Muhammed Naeem Noor Kahn was captured in

[6] Clearly this is a non-terrorist related example and no inference relating the BNP to terrorism is drawn in any way.

Pakistan in July 2004 with a computer filled with photographs and floor diagrams of buildings in the US [8].

If the Internet is brought down in a country or region it will do immense damage to the population, infrastructure and financial sectors of that society. The Internet relies on bandwidth and if targeted with a Distributed Denial of Service, DDoS, this can block the selected servers and effectively jam the Internet. This is relatively simple to do. If enough emails are sent in a short enough time, or enough hits are made simultaneously on a selected website, the bandwidth will fail to cope with the amount of data it is being requested to move and simply clog up, rather like a main street in rush-hour. One method of doing this is through a Botnet. A Botnet is a network of computers that have been taken over as slaves by one master computer. From the master computer a terrorist could direct all the Bots in the Botnet to email or log onto a website simultaneously. A Botnet can be millions of computers all over the world with the slaves showing no apparent symptoms. Botnets are relatively easy to set up for an experienced hacker and are available for purchase. Although not a terrorist attack, Estonia was the victim of a sustained DDoS attack in 2007. As Estonia prefers to operate as paperless as possible, effectively closing the Internet had a huge effect in that country.[7] This was combined with some civil disturbance relating to the moving of a Soviet war memorial in Tallinn city centre. This could be used by a terrorist organization to bring down a major banking system, Bishop's Gate and the Baltic Exchange bombs in the early 1990's in London highlight the attraction of a purely economic target to a terrorist organization. What the Provisional IRA achieved with a bomb could now be done to a much larger target area with only a laptop.

Supervisory Control And Data Acquisition (SCADA) systems control many major infrastructure systems and are increasingly being relied upon. These provide one of the greatest vulnerabilities to a purely Cyber Terrorism attack with potentially massive physical effect. SCADA systems are used to run power plants, control dams and even city traffic flow by controlling the traffic light system. If these can be accessed by a terrorist organization they can effectively take control of that facility. One of the main vulnerabilities for this is through a mole employee or a disgruntled worker. If a terrorist organization placed members as regular employees of a facility it is possible that they could, given the patient nature of sleeper cells, gain a position of trust in the facility and gain access to the SCADA computer system. From there they could initiate an attack to break a key facility or cause other forms of damage. An example of the potential this has happened in Queensland in Australia. Although not a terrorist attack a hacker got into the Sewerage SCADA in Maroochy Shire Council on Australia's Sunshine Coast. Vitek Boden put in glitches and deliberately released millions of liters of raw sewerage into the water system and sparked an investigation. He was a former employee who had access to the required passwords and knew the system. After his dismissal the council had failed to change the passwords and effectively allowed Boden access to the system [8]. His motives were personal but this shows what a terrorist could do.

4. Conclusions

The face of modern terrorism is ever changing and it seeks new methods of carrying out attacks, propaganda campaigns and recruitment. Cyber Space in certainly a new area of a battlefield and one that terrorist organizations are striving to exploit. There are many advantages to the terrorist to use the Internet for a myriad of essential threads to maintain a terrorist campaign. This threat must not be overlooked, as many societies move more areas of life and infrastructure to computer control and networked systems, the reliance on then is ever increasing. Unfortunately this reliance creates a fairly soft target. The terrorist no longer needs to physically be in the same country, let alone the site of an attack if it is conducted through cyber space. Information is far more accessible and available instantly, something a terrorist could exploit. Taking a photograph of a military instillation will raise suspicion and risk alerting the authorities to the terrorist or that an attack is being planned. Looking at the same site on a computer would leave the terrorist completely anonymous and undetected.

Terrorists such as Younis Tsouli, the infamous Terrorist 007, have become vital to terrorist organizations. Tsouli was not a fighter that offered much ability to conduct a physical attack, but he was committed to the al-Qaeda cause. He set up countless websites and video sharing forums to promote a pro-al-Qaeda message and demonize the US and UK. He operated from a London flat and was financed by another terrorist, interestingly who he never actually met. Tsouli was arrested with millions of files and videos with terrorist propaganda and training aids, which he was the central hub in distributing and putting on line. It was assessed that his arrest as a major blow for al-Qaeda, as much as any active field commander.

It is not all bad news though, by using electronic means, the terrorists can leave a signature and be monitored or arrested based on electronic evidence. It can also be used to monitor terrorist ‘noise’ [9] as an intelligence-gathering tool. Like any form of attack, a cyber attack is likely to leave some form of signature or evidence that if properly monitored or collected can be used as a counter terrorist tool. There is also some potential to use cyber means to attack the terrorists back, however this has some ethical dilemmas and is not within the scope of this paper.

Defence Against Cyber Terrorism will differ little form solid cyber defence and security. It is however important to understand the terrorist mindset and how they are likely to use the medium for their purpose. It must be conducted as part of the wider force protection and be conscious of the massive potential for compromise. It is highly unlikely anyone would take a large paper file, with highly sensitive information useful to a terrorist, outside a secure office, but this seems to be ignored when that information and a thousand times more is held on a 5cm USB stick. It is not only the system that requires improved security if the defence against Cyber Terrorism is to be successful. The often used comment, TPIBKAC, The Problem Is Between Keyboard and Chair and that there is no patch for stupidity hold true.

Having attended several workshops on Cyber Defence, one area of concern is that many ‘experts’ believe Cyber Terrorism simply won’t happen. It is foolish to write it off, at best it may currently be more ‘potential than problem’, but it is short sighted to exclude it

from risk assessment. Firstly, it may have already, we don't know who may be in place ready to attack a SCADA system, secondly we are increasing our reliance on these systems and their attractiveness as a target grows. Without doubt, the modern terrorist needs the Internet as much as the AK47 and it is a factor we would ignore at our peril.

All views expressed in this article are the authors and do not necessarily reflect or represent the views of COE DAT, CCD COE, NATO or the UK MOD or Government.**References**

[1] Record, Jeffery: Bounding the Global War on Terrorism, Strategic Studies Institute, US Army War College, Leavenworth, 2003
[2] Schmid, Alex and Jongmans, Albert et al: Political Terrorism: A new guide to Action, Authors, Concepts, Data Bases, Theories and Literature, Transaction Books, New Brunswick, 1988
[3] CSTPV St Andrew's University Certificate in Terrorism Studies
[4] COE DAT Information Collation Managemant Cell database
[5] Weimann, Gabriel: Terror on the Internet, USIP, Washington DC, 2006
[6] Weimann, Gabriel: WWW.AL-QAEDA: The reliance of Al-Qaeda on the Internet7
[7] COE DAT Cyber Terrorism Couse IV Mar 09
[8] COE DAT Strategic Communications Workshop May 09
[9] Huizing, Harry: Cyber Terrorism Briefing Note, COE DAT, Ankara, 2008
[10] Krone, Troy: Gaps in cyberspace can leave us vulnerable, Platypus Magazine (edition 90, Mar 2006)
[11] COE DAT Cyber Terrorism Workshop Oct 07
[12] Bunker, Robert J: Networks, Terrorism and Global Insurgency, Routledge, Abingdon, 2005
[13] Hennessy, Joh L and others: Information Technology for Counterterrorism, National Academies Press, Washington DC, 2003
[14] Hoffman, Bruce: Inside Terrorism, Columbia University Press, New York, 2006
[15] Huntington, Samuel: The Clash of Civilizations, Free Press, London, 2002
[16] Laqueur, Walter: The New Terrorism: Fanaticism and the Arms of Mass Destruction, Oxford University Press, New York, 1999
[17] Sageman, Marc: Understanding Terror Networks, Penn, Philadelphia, 2004
[18] Stern, Jessica: The Ultimate Terrorist, Harvard University Press, Cambridge MA, 1999
[19] Tuman, Joseph S: Communicating Terror, Sage, Thousand Oaks, 2003
[20] Whittaker, David (ed): The Terrorism Reader 3rd Ed, Routledge, London, 2007
[21] Wilkinson, Paul: Terrorism Versus Democracy, Routledge, London, 2006

[7] Thanks to Prof Weimann for his kind permission to use this article.