What is the terrorist threat in cyber-space?

https://www.e-ir.info/2011/07/26/what-is-the-terrorist-threat-in-cyber-space/

ROSS HALL, JUL 26 2011

What is the terrorist threat in cyber-space? Is this threat likely to grow in the coming decades?

The typical approaches to warfare, force, offence, defence and deterrence, do not necessarily cross over into cyber conflicts, be they for cyber warfare or countering cyber-terrorism. The world of network interactions changes the rules of the game, where the attackers can more easily remain anonymous, and the targets can be anything that is on an open network. This presents an immediate issue; so long as nations, businesses and civilians rely on computer networks as a basis for modern life, and these computer networks are connected to the outside world, they will be at permanent risk of attack. Those that choose to attack their targets through networks do so through the exploitation of system vulnerabilities (Libicki 2009: xiii-xiv). These attackers exploit human fallibility in the manufacture of machines and system, discovering loop holes and errors in programming that allow them access to their desired destination. Due to this, cyber-terrorism and cyber warfare should not be seen in the same light as traditional warfare as they are not made of and cannot be tackled by the use of physical force in the cyber realm. Physical force can only be brought to bear if the source of the attack can be identified, and even then it could possibly have comparably little effect compared to traditional warfare due to the difference between the two mediums.

These anxieties have promoted a view on the internet and open networks as potentially dangerous places. Even as early as 1990, there were claims that the use of computers could possibly be damaging. In this year the National Academy of Sciences issued a report that claimed, “We are at risk. Increasingly, America depends on computers…. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb (Wiemann 2006: 2). While there is undoubtedly a great deal of potential for almost any venture in the internet, these claims could be suggesting too much. This could be a result of the intentions of those that research the issue; those that sell internet security companies chase sales, academics follow grants and politicians budgets. All of these actors have a common interest in that it benefits them to overstate the risks that the internet can pose to the government, businesses or the population as a whole (Economist 2002).

When analysing the terrorist threat in cyberspace, there are some immediate issues which need to be assessed, namely the problems of defining a terrorist, and then further defining a cyber-terrorist. There is a constant debate as to what constitutes a terrorist or a terrorist act, which simply serves in the meantime to aid the terrorist as without a clear, universal definition, it is not possible to construct a uniform approach to tackling acting and would-be terrorists. This is due to the multiplicity of terrorist aims, motives and ways in which they are viewed by the public, such as the “one man’s terrorist is another man’s freedom fighter” issue. Such as it is the confusion that revolves around the competing definitions of terrorism has amounted to a hindrance in tackling the act itself (English 2009: 21). Due to these complications, it is necessary to give a workable definition for what a terrorist is before any discussion of their nature is possible.

‘Terrorist’ is a very pejorative term, which can be loaded with whatever meaning the user wishes it to hold in the context that it is used. It is used as a tool to delegitimise enemies, and as such, groups that are deemed terrorists do not usually seem themselves as such. Instead, they describe themselves with terms such as guerrillas, revolutionaries or mujahedeen, as they are seen as being more positive in their description of the group (Lia 2005: 9). This only serves to further complicate the problem of defining who is, and isn’t, a terrorist as each actor has his own set of principles that dictate a terrorist. Some states may wish to define a terrorist very specifically so as to list the

'others' as merely being criminals, therefore restricting their activities to mainly police responsibilities. However, Enders and Sandler (1999: 147-148) offer a useful definition as claim that terrorism is the 'premeditated use, or threat of use, of extra-normal violence or brutality to obtain a political objective through intimidation or fear directed at a large audience'. The presence of a political objective is a necessary addition as without one, the use of violent acts as a means to end simply constitutes criminal activity. With the use of an overall political objective, a criminal becomes a terrorist. In the case of terrorism, the political objective in question can include the promotion of religious equality, income redistribution, nationalism, separatism, ideology (such as Marxism), nihilism, racism, and issue-specific causes (ibid). Also, in this definition, the inclusion of 'extra-normal violence' is necessary as it determines the way in which terrorists act. Extra-normal violence, such as acts that are designed to generate a large media response, is used to promote disproportionate levels of fear in a population that is used to being subjected to normal levels of violence in the media. This definition does, however, lack the inclusion of the involvement of non-combatants as the target of the terrorist acts as many believe should accompany the definition of a terrorist (Victoroff 2005: 4). This is an important aspect in the definition of terrorism as it prevents any violent act against military personnel from being label as an act of terrorism. Instead, for the use of violence to be classed as terrorism, it must be targeted at those who are not members of the military or are not actively involved in military hostilities (Ruby 2002: 10). A terrorist act is directed towards a civilian population because they are not at the same level of readiness to deal with it as the military. Due to this, a greater deal of panic can be caused through the use of media reports than would be possible if a group attacked a military target. By defining terrorism with these three important criteria, the requirement of a political objective, the use of extra-normal violence and a non-combatant target, certain groups or persons can be excluded and others included so as to focus the debate and anti-terrorist attempts.

The constant debate that surrounds terrorism is further exacerbated when it is expanded into the field of cyber-terrorism. When classical definitions of terrorism are applied to the mediums of cyber-terrorism they can lose some of their effectiveness. One of the main issues is the inclusion of 'violence' as a central tenet of the definitions. The choice in the definition of what violence means can change an entire argument of who constitutes a cyber-terrorist completely. If Galtung's concept of violence is used, it can be characterised as 'avoidable insults to basic human needs, and more generally to life, lowering the real level of needs satisfaction below what is potentially possible', which can also include threats of violence (1990: 292). This concept of violence can include almost any action of one party towards another as long as it prevents the other from achieving its full potential. This definition can be expanded further by using Pontara's clarifications (1978: 22-23), where it is claimed that an act of violence must be unauthorised. In this sense, an act is unauthorised if it is not sanctioned by a legitimate authority, which in international relations is typically seen to be either the state or an international organisation such as NATO or the UN. Pontara also claims that violence does not necessarily need to involve or cause physical harm as, for instance denying aid to a state can result in the deaths of many people through starvation. While this is not comparable to traditional conceptions of terrorist violence, such as bombings and shootings, they reach the same ends. This definition presents further issues as there is no single international framework that is designed to define and counter terrorists, and even less so cyber-terrorists. These definitions can therefore include the recently publicised distributed denial of services (DDoS) attacks which have targeted various sites that have withdrawn their services for the whistle blowing site, WikiLeaks (BBC 2010a). If the original definition of what constitutes a terrorist attack is applied to this instance then it is possible to deem the perpetrators as terrorists. As was stated above, to be a terrorist, an individual or a group must fulfil four definite criteria; the act must be premeditated, use violence, target non-combatants and attempt to achieve a political objective. Firstly, DDoS attacks are designed to prevent a given site from operating either within its normal parameters or even being able to operate at all. These attacks therefore prevent the sites, the individuals who operate them and those that use them from achieving their full potential, and can as a result be classed as a violent act. By attacking privately owned sites that are used by the public, the groups that are conducting these DDoS attacks are targeting non-combatants, therefore satisfying another criterion for being labelled as a terrorist. Thirdly, as the attacks are the product of an international group of individuals that share a common goal, they must be considered as premeditated as they would have required organisation prior to the actual attack. Finally, the group, which is now known as 'Anonymous' has a political objective, in that it wishes to influence government foreign policy with concern to WikiLeaks by expanding its DDoS attack campaign to anyone that has an 'anti-WikiLeaks agenda' (Guardian 2010). With this final criterion fulfilled, Anonymous, with this definition, can be seen as a terrorist group that is operating within cyberspace, therefore making them cyber-terrorists.

These DDoS attacks represent a different attack approach for cyber-terrorists, if they are to be deemed as such. These attacks allow those who are not necessarily as apt with computer systems to join groups or individuals who wish to achieve a certain objective through the use of cyber-space. They are, however, not a new phenomenon, it was claimed in 2001 that an 'Iraq Net' had existed since the mid-nineties, comprised of over one hundred websites that were used to mount DDoS attacks against US companies. Yonah Alexander, the terrorism researcher from the Potomac Institute who announced this, claimed that "Saddam Hussein would not hesitate to use the cyber tool he has…. It is not a question of if but when. The entire United States is the front line" (Wiemann 2006: 3). These attacks are designed to bombard websites with such vast amounts of information that their bandwidth is exceeded and they either crash or a forced offline while they are repaired. To maximise their effectiveness, DDoS attacks are conducted with the use of botnets. A botnet is a group of computers that are all link by a certain piece of software that allows them all to synchronise on a common task. This software is often downloaded onto a computer as part of a virus or it can be voluntarily downloaded so as to deliberately take part in a botnet. The way in which these attacks tend to be used is through a blunt force attack where the botnet instructs all of the constituent computers to log onto a website, send mass emails to a site filling its bandwidth or sending other forms of information. The scale of these botnets has grown considerably in recent years, to a state where the 'Iraq Net' botnet of over one hundred websites has been considerably dwarfed. This has also been coupled by the massive expansion of the numbers in ownership and the power of computers that are held by the public. For example, it was recently found that more than 2.2m US computers were part of botnets in just the first six months of 2010 (BBC 2010b). These botnets are notoriously difficult to trace due to the nature of their work, they are designed to attack all at once, therefore making it near impossible to locate the progenitor of the attack or of the software itself. Also, due to the fact that a person can either take part willingly through downloading the software or without knowing causes issues for proving guilt if any attempt is made at tackling these botnets. These kinds of attacks are classified by some as acts of cyber-terrorism as they are seen to be distinct from 'traditional' terrorism due to that fact that 'physical terror does not occur', and instead efforts are focuses on attacking information systems and resources (Furnell and Warren 1999: 30).

These DDoS attacks are, however, a very basic tool that is often used by members of the public in attempt to achieve their goals through the use of cyberspace. This is not the extent of cyber-terrorism and is very simplistic when compared to the recent Stuxnet Worm, which was first discovered in June 2010. This worm appears to have been created by a state as its complexity and specific target place it out of the general realm of public concern. The target appears to be Siemens' 'supervisory control and data acquisition' (SCADA) system, which control valves, pipelines and industrial equipment as the worm specifically targets a piece of software that the SCADA systems use, called WinCC. This worm operates by seeking out the WinCC software, and if it finds it, the worm will install a program that allows it to connect to the internet for further instructions. The fact that the worm looks for a specific piece of software in a specific system implies that it is looking for a certain plant or process (Economist 2010a). This is because in order to implement an attack of this kind, a great deal of very detailed knowledge about the target plant and its systems would be needed. This is due to the very nature of computer attacks, if an would-be attacker wishes to attempt to even access a system, they must be using the right form of code, with the right constitution and aim, resulting from very detailed knowledge of the systems that are used, it is not as simple as the use of a bomb. The main target of the attack would appear to have been the centrifuges at the Iranian Natanz nuclear refinery as it uses the systems and software that the Stuxnet worm was designed to complicate. This is timed with a drop in the number of working centrifuges at Natanz during 2009, though it is unclear whether this was due to Stuxnet. If this was the intended target, then the originator would appear to be a state as only states are likely to have such detailed knowledge of the software that is used to operate very specific centrifuges in an Iranian nuclear facility (Economist 2010b). While this kind of attack could delay the use of the centrifuges in the Natanz facility, it would not be able to shut them down permanently. A physical military attack would be able to destroy the centrifuges, giving a definite outcome to an operation, but would incur great repercussions on the state that initiated the attack. This kind of cyber-attack, however, is extremely difficult to link to the source and therefore could be more useful to a state that wishes to use a less traceable method so as to avoid blame and condemnation, but achieve at least a small aspect of the overall goal.

If this attack was indeed the result of a state using cyberspace to achieve its military goals, then it marks the first, documented, use of this form of attack by a state. Under the above concepts of what constitutes a terrorist, this act would appear to be one of terrorism on the part of a state as it could fulfil all of the four criteria that are necessary.

The worm has been used to target what could be a civilian nuclear facility, it has a political objective in halting or preventing Iranian nuclear development, it has caused violence in preventing the plant from operating correctly and was definitely premeditated. This attack could still be claimed by a state, if it was the creator of the worm, to be information warfare rather than cyber-terrorism as information warfare has a longer grounding in international relations and the conduct of states. This is because information warfare can be defined as a 'planned attack by nations or their against information or computer systems, computer programs and data that result in enemy losses' (Colarik and Janczewski 2008: xiv). With this definition, the Stuxnet worm could be classified as information warfare is it was proven to be released by a state as the worm was designed to attack the systems and programs of a very specific plant. While the definition does not clarify what it means to be enemy losses, it would be generally understandable to include the loss of productive capabilities in this definition.

The attacks that have already been described may not, however, be regarded as terrorist acts if a cyber-terrorist is defined in another way. In an attempt to demystify this issue, Arquilla and Ronfeldt (2001: 241) offer a different conceptualisation. They classify three different categories in the use of networks for activity, namely activism, hacktivism and cyber terrorism. Activism is defined as 'normal, non-disruptive use of the internet in support of an agenda or cause'. This can include distributing political messages and information through the internet and other such networked mediums. Hacktivism is defined as 'the use of techniques against a target's internet site with the intent of disrupting normal operations but not causing major damage'. Under this definition, hacktivism would include any DDoS attacks as these are designed exactly to disrupt normal operations, therefore limiting these attacks to criminality, rather than terrorism. Finally, cyber-terrorism encompasses 'politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage'. With this definition the Stuxnet attack that would appear to have been targeted at Iran could be described as a terrorist act as the shutting down of nuclear centrifuges could result in severe economic damage if the attack is made correctly. What is clear in these definitions is that there is a general progression towards a greater level of damage and disruption through the categories from the first to the third, resulting in terrorism definitely including actual harm to people or economies. This definition allows for the classification of terrorism to only be applied to the most extreme of cyber-attacks, therefor eliminating many others and leaving them as merely criminal acts that are more easily dealt with, especially as in the UK DDoS attacks are illegal.

So far this essay has looked at deeming a cyber-terrorist as a person who seeks to use violence, in different capacities, as a tool actually in cyberspace in order to achieve their political goal. There is however a contending opinion that believes a person is a cyber-terrorist if he simply uses an aspect of the globalising media to aid his campaign. This can include spreading a press release on their websites after an attack to claim responsibility or communicating and organising an attack through cyberspace (Arquilla and Ronfeldt 2001: 42). Whittaker (2007: 277) defined cyber terrorism as 'an attack on information systems rather than on people'. With this definition it is possible to include many more groups and people into the definition of who is, and who is not a cyber terrorist.

The world has witnessed the more widespread use of information technology, from the internet to easier access to media outlets, by terrorist groups as they look for ways to increase the impact that their message has upon the general population. In recent years, terrorist organisations have been harnessing the power of networked, mass media. This has led to a new class of threat in the form of cyber terrorism. This includes groups such as Anonymous whose aim is to attack systems that are widely used in order to further their cause. However, arguably the first group to successfully harness the power of the internet for their cause was the Zapatista National Liberation Army (EZLN). While this organisation is more of an insurgency than a terrorist organisation, they illustrated how the efficient use of communications technologies can be used to inspire further demonstrations and protests from those who reside outside of the group (Hoffman 2006: 202-204).

The recent Strategic Defence and Security Review (2010) defined terrorism as the highest security concern to the UK. Cyber terrorism was ranked third of all tier one threats, placing it high on the UK agenda for defence and security needs. This highlights the belief, at least in high government, that there is a constant fear of attack, with a growing concern of the risk of cyber terrorism. When defining cyber terrorism in a loose way as outlined above, it is easy to see how it has expanded in recent years. The internet has enabled the rapid, universal and inexpensive exchange of information. It provides the opportunity to develop groups all over the world to attempt to influence foreign policy. This

kind of reach has only been possible since the internet's inception. Through using the internet, a group is able to portray themselves in any light they wish. This is known as 'perception management' and can be used to recruit large numbers of followers in the face of damning media reports (Hoffman 2006: 201-202).This expansion in the use of the internet by terrorists has been coupled by the rise of globalisation. This globalisation in areas such as transportation, communication and finance has benefitting both business can terrorists. The development of affordable and powerful communication technologies has allowed terrorists to organise in growing global networks. These technologies allow for more fluid structures than the rigid hierarchies of states. This creates opportunities for greater adaptability, resilience, innovation, learning and recruitment (Eilstrup-Sangiovani and Jones 2008: 7-8). These network-centred terrorist groups can be difficult for states to tackle as they are not designed to do so. This is why there has been such a growth in the numbers of groups that use the internet to further their cause. Inn 1998, fewer than half of the thirty groups that the US State Department describes as Foreign Terrorist Organisations (FTOs) had websites. This had changed by 1999 to such an extent that nearly all of the groups on the FTO list had websites (Hoffman 2006: 206). This expansion is due to the fact that a personal website can allow the publishing of personal material that other, mass media outlets would not release, enabling the group to reach a wider audience, including worldwide sympathisers and possible recruits. The use of networks can also promote the efficient use and development of communication technologies and methods of information processing. In a horizontal terrorist group that does not revolve around a strict hierarchy and as such is not constrained by the rigid decision making structures, networks can allow information and communications to flow unhindered from one actor to another. This in turn enables actors to receive and process information faster than those that reside in a strict hierarchy, such as those who work for state organisations (Eilstrup-Sangiovani and Jones 2008: 13-14). This can be seen as an inherent advantage over states as it is possible for these groups to develop even further horizontally, adding new members and groups, thus creating greater recruitment opportunities.

So far cyber terrorism has yet to yield the kind of attacks that cause actual harm to people in the same way as traditional terrorism has done. This is because, as Dorothy Denning puts it, terrorists "still prefer bombs to bytes" (Cronin 2003: 46). Cyber terrorism has instead been limited to the spreading of information and the denial of certain services. This is due to the inherent difficulties of reaching beyond the computer with a cyber attack such as the doomsday scenarios that are so often used in movies. For example, the U.S., the water supply infrastructure is controlled by 54,064 separate water systems. Of these systems, 3,769 of these systems serve eighty one per cent of the population and 353 serve forty-four per cent (Lewis 2002: 4). Due to the makeup of this infrastructure, it can prove to be a very difficult target to successfully attack. This is because not all of these systems use the same programs or hardware, making it necessary for the cyber terrorists to be fluent in many different programming languages. Also, many of these systems are not connected to the internet for just such an eventuality (ibid). These issues mean that it is very unlikely that a successful cyber-attack will be waged on this infrastructure. To do so would need colossal organisation, expertise and most certainly expense, which are not typically available beyond the few experts that work for government bodies and utility companies. To make any kind of headway on this structure, it would be necessary to mount a prolonged attack on all aspects at one time, which would create a logistical nightmare for those that wish to use this as a method of terrorist activity. This is why both activists and terrorists have instead increasingly tuned to the use of hacktivism to attack internet sites with web defacements, hijackings, sit ins, DDoS attacks and automated email spamming as they provide a means for operating anonymously, and are easily organised internationally (Cronin 2003: 46-47). This is shown by the growth of in the numbers of malicious software applications that have been discovered in recent years. In 2009 alone, fifty-one per cent of all malicious software ever created, were detected (Strategic Defence and Security Review (2010). Ian Lobban, director of the Government Communications Headquarters (GCHQ), recently claimed that there are over 20,000 malicious emails circulating on government networks each month, of which, 1,000 are deliberately targeting them government systems (Lobban 2010: 6). While this form of terrorism is not currently at the same stage as traditional terrorism in terms of the amount of physical destruction that it can cause, with this quantity of malicious software circulating, it is easy to see why it has been seen as an escalating threat to governments and civilians.

While it is difficult to predict what is going to happen in future situations, it is likely that the trend towards the use of the internet and other mass networks by terrorists is likely to continue and grow. The rapid expansion of the internet and the capabilities that are available for use is progressively lowering the bar of entry for those who wish to join the 'espionage game' (Ibid: 7). In order to tackle this growing threat, it is necessary to treat cyberspace as its own,

separate medium, and not like a typical threat. This is because cyberspace is a medium that presents a whole new set of principles that need to be contended with. Cyber-attacks are conducted through the generation of force in the same way as other forms of warfare; instead they are done so through the exploitation of the enemy's weaknesses. This is further complicated by the level of ambiguity that accompanies cyber space, resulting in confusion over who attacked who and whether they have the capabilities to do so again. Any attempts to transfer similar policies from other forms of warfare and policing will not only fail to succeed in their primary aims, but they will also hinder further policy and planning (Libicki 2009: 5). These groups are likely to grow in numbers and their capabilities and capacity to cause damage and terror will become increasingly sophisticated. By examining current trends, it is possible to see that with the constant growth and spread in ownership of new communications technologies, the growth of cyber terrorist groups, or the adoption of cyber methods by traditional terrorists, will be accelerated (Hoffman 2006: 228). While the threat of cyber terrorism has been overstated by the media and governments alike, there is still a significant threat that can be posed. Texan congressman, Lamar Smith, claimed that "Until we secure our cyber-infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy and endanger lives". He also ended his speech by stating that "A mouse can be just as dangerous as a bullet or a bomb" (Economist 2002). While terrorism does pose a threat to the security of the state and civilians, it is not a threat of quite this magnitude. For example, a simulation was carried out by the United States Naval War College and a Gartner, a consultancy firm found that an attack on this scale, which has been termed an 'electronic Pearl Harbour', would first need five years of preparation and $200m of funding (Ibid). This kind of funding and expertise is for now beyond the scope of individuals or groups that wish to take part in cyber terrorism. This issue could well have already been highlighted by the Anonymous group itself. This has been shown by at least one faction of Anonymous instructed followers and supporters to take to the streets on December 18th to distribute paper copies of the WikiLeaks cables to people in the streets (BBC 2010c). Even when examining state use of cyber acts against an enemy, as the Stuxnet example shows, there are still great difficulties that need to be overcome before an attack anywhere near that of an 'electronic Pearl Harbour' can be mounted.

Bibliography

Arquilla, J. and Ronfeldt, D. (2001) 'Networks and Netwars' RAND, Santa Monica

The BBC (2010a) http://www.bbc.co.uk/news/technology-11980125 13th December 2010

The BBC (2010b) http://www.bbc.co.uk/news/technology-11531657 13th October 2010

The BBC (2010c) http://www.bbc.co.uk/news/technology-12008565 16th December 2010

Colarik, A. and Janczewski, L. (2008) 'Cyber Warfare and Cyber Terrorism' Information Science Reference, London

Cronin, A. (2003) 'Behind the Curve: Globalization and International Terrorism' International Security, Vol. 27, No. 3, pp. 30-58

Economist (2002) 'The Mouse that Might Roar' Economist October 24th 2002

Economist (2010a) 'The Stuxnet Outbreak: A Worm in the Centrifuge' September 30th 2010 the Economist

Edwards, L. (2010) 'The Anonymous group is taking aim at the wrong target' The Guardian 10th December – http://www.guardian.co.uk/technology/blog/2010/dec/10/internet-wikileaks-anonymous

Eilstrup-Sangiovani, M. and Jones, C. (2008) 'Assessing the Dangers of Illicit Networks' International Security, Vol. 33, No. 2, pp. 7–44

Enders, W. and Sandler, T. (1999) 'Transnational Terrorism in the Post-Cold War Era' International Studies Quarterly, Vol. 43, No. 1, pp. 145-167

English, R. (2009) 'Terrorism: How to Respond' Oxford University Press, Oxford

Furnell, S. and Warren, M. (1999) 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?' Computers & Security, 18, 28-34

Galtung, J. (1990) 'Cultural Violence' Journal of Peace Research, Vol. 27, No. 3, pp. 291-305

HM Government (2010) 'Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review' Her Majesty's Stationery Office

Hoffman, B. (2006) 'Inside Terrorism' Columbia University Press, New York

Lewis, J. (2002) 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' Centre for Strategic and International Studies

Lia, B. (2005) 'Globalisation and the Future of Terrorism: Patterns and Predictions' Routledge, Oxon

Libicki, M. (2009) 'Cyberdeterrence and Cyberwar' RAND Corporation, Santa Monica

Lobban, I. (2010) 'Speech for International Institute for Strategic Studies' GCHQ

Pontara, G. (1978) 'The Concept of Violence' Journal of Peace Research, Vol. 15, No. 1 (1978), pp. 19-32

Ruby, C. (2002) 'The Definition of Terrorism' Analyses of Social Issues and Public Policy, pp. 9–14

Sinclair, A. (2003) 'An Anatomy of Terror: A History of Terrorism' Macmillan, Basingstoke

The Economist (2010b) 'The Meaning of Stuxnet' September 30th 2010 The Economist

The Guardian (2010) 'Theresa May warns of growing threat of cyber warfare' 18th October 2010 http://www.guardian.co.uk/politics/2010/oct/18/theresa-may-threat-cyber-warfare – accessed November 20th 2010

Victoroff, J. (2005) 'The Mind of the Terrorist' The Journal of Conflict Resolution, Vol. 49, No. 1, pp. 3-42

Whittaker, D. (2007) 'Terrorism: Understanding the Global Threat' Pearson, Edinburgh

Wiemann, G. (2006) 'Cyberterrorism: How Real Is the Threat?' United States Institute of Peace, Washington DC

—

Written by: Ross Hall
Written at: Plymouth University
Written for: Dr. Fotios Moustakis
Date: December 2011

About the author:

Ross is currently studying for an MA Applied Strategy and Security Studies with the Britannia Royal Naval College at Plymouth University. His main interests are the contemporary application of force, military strategy and British defensive capabilities.