Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

Global Reach: Terrorists and the Internet

Simon O'Rourke
Edith Cowan University

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/15

Global Reach: Terrorists and the Internet

Simon O'Rourke
Edith Cowan University
E-mail: sorourke@student.ecu.edu.au

Abstract

The use of the Internet by terrorists appears to diverge into two distinct modes neither of which is mutually exclusive. The first aligns to the view that terrorists will use the Internet as a platform to launch cyber attacks against critical infrastructure nodes as well as key government and private sector networks. This paper discusses the alternate mode that being the primary use of the Internet by terrorists will be to recruit, train, communicate and gain information about potential targets by conducting virtual reconnaissance. It will examine the nexus between the virtual world and the physical threat that is manifested as a result of the ideology being promoted. The requirement for law enforcement agencies to develop capabilities to track the activities of terrorists in cyberspace presents technological and human resource challenges.. Whilst the Far Right and Islamic Fundamentalist groups have seized upon the opportunity to network and promote their particular ideologies, they have until recently done so in relative isolation. This scenario is now in transition as Far Right groups are providing links and information on their websites about Islamic Fundamentalism.

Keywords

Terrorism, Internet, Training, Planning, Police, Intelligence, Attacks, Logistics, Recruitment, Media, Al-Manar, Aryan Nations, Stormfront, Far Right, Jihad, Iraq, Afghanistan.

INTRODUCTION

The use of the Internet by terrorists appears to diverge into two distinct modes neither of which is mutually exclusive. The first aligns to the view that terrorists will use the Internet as a platform to launch cyber attacks against critical infrastructure nodes as well as key government and private sector networks. This paper discusses the alternate mode that being the primary use of the Internet by terrorists will be to recruit, train, communicate and gain information about potential targets by conducting virtual reconnaissance. The very success of the Internet in facilitating these endeavours may provide some degree of protection from direct attack, however it may still be utilised as a platform from which to carry out virtual attacks against physical infrastructure.

VIRTUAL COMMUNICATION: REAL TIME THREAT

The increasing availability of comparatively cheap, reliable and high bandwidth communications have aided the increasing globalisation of businesses and commercial services. Many of these same inputs can be seen as aiding the globalisation of terror networks. The trend that was clearly seen for the first time in the 1970's when organisations such as the Popular Front for the Liberation of Palestine (PFLP) began to use the global media network in order to publicise their agenda has continued. In the specific case of what is known as Islamic fundamentalist terrorism, the dispersed nature of recruiting and communications has caused a fundamental shift in how to define and approach the threat posed by this utilisation of leading-edge communications technology.

The Metropolitan Police Service (MPS) Deputy Commissioner Peter Clarke when asked if the experience with the Irish Republican Army (IRA) had prepared the police for the new threat posed by Islamist terrorism stated, "What we see is global in origin, global in ambition, global in reach. The networks are loose, they are fluid and they are incredibly resilient" (Clarke cited in *The Weekend Australian* 23 September 2006).

This 'global reach' is aided by recent advances in communications technology, which provide a medium that allows terrorist groups and their political supporters to promote their ideology and activities on the world stage

with minimal infrastructure and costs. Digital video cameras, laptops and editing software can all be utilised to advocate the cause of the particular terrorist group involved. It has being said that, "The media are the terrorist's best friend. The terrorist's act by itself is nothing, publicity is all", .

The availability of modern digital technologies and the ubiquity of communications channels such as the Internet can be seen as making these groups their own media entity. They no longer need to rely on the presence of third party media organisations to record and distribute their message, at least to a sympathetic audience.

Once the video and accompanying imagery are prepared they can then be uploaded onto the Internet and accessed from almost anywhere, providing the contemporary terrorist with the ability to potentially influence activities at the national and international level . This ability to deliver a different viewpoint counteracts the framing of events by the mainstream media organisations allowing for terrorist groups to reach a global audience. It also provides for anonymity when accessing and viewing the material for those who may share the same ideological views as the terrorist organisation . Like-minded individuals can find each other in cyberspace via online blogs and chat-rooms. "The arrival of the Internet has provided the first forum in history for all the disaffected to gather in one place to exchange views and reinforce prejudices", . Against this background of widely available communications and digital media technology it is hardly surprising that terrorist groups are utilising it to maximum effect.

TERRORISTS ON THE INTERNET

Whilst there has being much discussion regarding the possibility of a cyber attack against critical infrastructure nodes, it would appear that the primary uses of the internet by terrorist groups are currently, "propaganda, secure communications, intelligence gathering, and funds management" . This stance is supported by Weimann who is of the opinion that the Internet was used for, "coordinating attacks, and planning actions including the attacks of September 11, 2001, as well as those of March 11, 2004, in Madrid and of July 2005 in London".

In Australia the Commonwealth Director of Public Prosecutions (DPP) in the material facts regarding R v Lodhi alleges that the accused used the Internet to access and download photographs of selected establishments that he wished to attack. The Commonwealth DPP also alleges in the material facts regarding R v Khazall that the accused in this case compiled and partly authored an electronic document titled, "Provision in the Rules of Jihad – Short Wise Rules and Organisational Structures that Concern every Fighter and Mujahid Fighting against the Infidels". It is further alleged that this document was then uploaded onto a website with unrestricted access where it remained for a period of 8 months . These cases demonstrate the use of various modern communications technologies, most notably the Internet, as an aid to planning and intelligence gathering rather than as a mode of attack. In this case the Internet can be seen as an enabler to assist in achieving the desired outcome.

It is also plausible that the invasion of Afghanistan and the destruction of many terrorist training camps have forced the leaders of these groups to put material on the Internet in order to survive and maintain their ability to instruct recruits. This has made the information more readily available to a wider audience. It has, however made the information more vulnerable to interception by police and intelligence agencies who will study it in order to discern the 'modus operandi' of the groups involved .

The Internet combines global reach with the capability to store and disseminate extremist materials. It is also a conduit by which to instruct and indoctrinate potential members via email or provision of access to restricted websites. Digital communications also provide opportunities for police and intelligence agencies to intercept, track and decrypt if resources and legislation permit.

TRACKING TERRORISTS IN CYBERSPACE

The manner in which terrorist cells communicate, distribute propaganda and training materials and other pertinent information via the Internet makes it difficult for state and nation based law enforcement agencies to track and curtail their activities. The ability to log on anonymously in Internet cafes around the globe makes it problematic for conventional law enforcement strategies to be effective. In place of a centralised command and control structure, there exists a flatter more diversified loose cluster of senior cells offering spiritual and

operational guidance via the Web .

This diversified structure provides for 'tactical independence' whilst ensuring that the individual cells still adhere to an overarching strategic effort. This view is supported by Whine who also identifies the resilient nature of such a structure due to the increased stability provided by, "geographical dispersion both physical and in cyberspace" .

Terrorist cells are communicating covertly via the Internet thereby minimising discernable links to known parent terrorist organisations. Many of those involved will not even have travelled to countries of interest to participate in training. This presents a challenge to law enforcement and intelligence agencies as to how they identify these cells prior to an event occurring. "The radicalisation process is occurring more quickly, more widely, and more anonymously in the Internet age" .

The openness of the Internet presents challenges for police and intelligence agencies to track seemingly innocuous message traffic between cell members, unless they have already being identified as being of interest. The nature of the challenge posed by attempting to track down and identify 'amorphous' terrorist networks can be resource intensive . However, whilst Clarke & Newman advocate that these resources may be better utilised in preventative actions they acknowledge the use of the Internet by terrorist groups for recruitment and the transmission of messages from charismatic leaders.

According to Melman the following communication was the last message sent by Mohammed Atta, to the other members of the 9/11 terrorist cell, "we've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering".

This message would clearly have not triggered any warnings on monitoring or 'sniffing' technologies hardwired into Internet Service Providers like the FBI's Carnivore system otherwise known as 'DCS100' . The message referred to the targets to be attacked by the hijacked aircraft as well as the number of terrorists who would be taking part. Some Internet messages or strategic documents compiled by known terrorist entities can provide insight into future activities. These are the documents, which need to be identified and analysed as a priority.

Once such document was posted online in December 2003 and identified by Brynjar Lia from the Norwegian Defence Research Establishment (FFI). His view was that the document was of strategic value to the ongoing insurgency in Iraq and it was only reviewed after the March 11, 2004 attacks in Madrid . The FFI analysis of the document clearly identifies economic cost as a key weakness in the sustainability of the U.S. led operation in Iraq. Should coalition partners be forced to withdraw from Iraq, then the U.S. could not fund the operation either economically or politically on its own. Spain was discerned as the most vulnerable because of the public opposition to the war, which could prove pivotal if harnessed .

In addition to using the Internet for coordination and exchange of information prior to an attack, terrorists can also conduct research on potential targets and obtain detailed photos and plans electronically, thereby minimising the actual time they are exposing themselves during a physical reconnaissance of a target . The recent attacks on mass transit systems have highlighted the volume of publicly available information regarding schedules, routes and timetable changes that is available for download from various government and private web sites. This can be combined with imagery from sites like 'Google Earth' when planning a terrorist attack as it provides additional detail about the potential target and its surroundings.

GLOBAL IDEOLOGY – LOCAL INTERPRETATION

The nature of the personnel who may become involved in Islamic terrorism is changing. The source of recruits now extends from not only those who have fought in traditional Jihad overseas, in conflicts like Bosnia, Chechnya and Afghanistan but also encompasses those who are second and third generation born in countries not directly involved in such conflicts and who may never have travelled outside their country of birth. These home grown extremists know little of the homeland of their parents or grandparents, yet they feel aggrieved by the foreign policies of their country of birth or by the perceived injustice being experienced by groups overseas .

This emotional attachment to a group with whom they share little in common other than a religious belief is being fed by images of Jihad warriors fighting in conflicts in places like Afghanistan and Iraq. The importance of propaganda is clearly understood by terrorist groups who video their attacks and then upload them onto the Internet for editing and hosting by various websites. These videos serve as a powerful tool for recruitment . In addition to being shown on the Internet the videos cause controversy when they are shown on mainstream western media like CNN (CNN, 2006).

In a speech at Queen Mary's College in London on the 9th of November 2006 the Director General of the UK Security Service better known as MI5 spoke of the ideology developed and marketed by groups like Al-Qaida via the Internet which links the approach taken by Western countries to regional issues in the Muslim world. This can be interpreted by extremists, "as evidence of an across-the-board determination to undermine and humiliate Islam worldwide" .

Dame Manningham-Buller also highlighted the difficulties facing the Security Service and police given the sheer numbers involved and volume of information requiring analysis. Figures provided included in excess of 1600 individuals who formed part of 200 known networks. Some of these individuals were undergoing radicalisation, "through chat rooms and websites on the Internet" .

Therefore the possibility exists for an individual or group to become completely radicalised via the Internet thereby remaining virtually unknown to police and intelligence agencies. This can be achieved through virtual training camps like, "Al Qaeda's *Al Battar Training Camp*" .

A recently declassified report from the Canadian Security Intelligence Service (CSIS), details the threat posed by Islamic extremists of Canadian birth and nationality due to their ability to avoid detection as they appear no different to any other Canadian citizen. Islamist groups recognise the value of genuine travel documents and the potential to access countries with strict boarder controls they represent .

This trend has also being identified by the Dutch Intelligence Service (AVID). Terrorist activity by nationals was graphically demonstrated by the suicide bombings in London in which those involved were able to become radicalised whilst outwardly maintaining the veneer of being part of the UK culture.

Recent arrests in Australia as a result of Operation Pendennis demonstrate the wide spread nature of the threat of 'home grown' extremism for many nations This threat has been recognised by the Australian Government, "the terrorist threat to Australia does not only come from external sources. It can also come from people living and working in Australia" .

The lessons learnt from the London bombings on July 7th 2005 clearly show that the timeframe in which to identify a person in the process of becoming radicalised is extremely short . Potential terrorists in this country may be second or third generation Australians, and may not have travelled to countries of interest or conducted themselves in such a manner as to draw attention from the Australian Security Intelligence Organisation (ASIO), or other national agencies like the Australian Federal Police (AFP). "It is terrorism of a previously unknown scale. It is a different kind of conflict, perpetrated in the name of a Muslim extremist cause. We must understand it if we are to defeat it" .

CHALLENGING THE MAINSTREAM WESTERN MEDIA

Islamist groups target particular nationalities in order to obtain the necessary media coverage to potentially generate community demands for change to a nation's foreign or domestic policy. One such incident was the attack on the rail infrastructure at peak hour in Madrid just prior to the last Spanish general elections. The resultant loss of office by the reigning political party and the subsequent withdrawal of Spanish troops from Iraq could be interpreted as a significant victory for the Islamists and a vindication for their use of force to achieve a political objective .

A prime example of a media organisation that is highly supportive of terrorist acts is the Al-Manar Satellite Television network. This network shows the understanding that groups like Hezbollah regarding the impact and

reach of mass media. The ability for subscribers across the globe to access the network provides a medium, which can be used to communicate and influence a wide audience. The potential exists for some subscribers to use this as a primary source of news and information, instead of commercial networks in countries where they now reside. This could influence their judgement on key issues and alter their opinions regarding foreign policies of the governments in their new homes. It can also limit assimilation and lead to a sense of self imposed isolation, from the remainder of the community.

Clearly, the challenge is how to present an alternative viewpoint. The U.S. has invested heavily into an its own Arabic language satellite network, which is not being well received by its intended audience in the Middle East who have clearly recognised it as a propaganda tool . It is however a step in the right direction and acknowledges the need to communicate a different viewpoint in a foreign language, to an audience who if receptive could alter the perception of the U.S. in that region.

Traditional values and outlooks are undergoing change in most Australian communities regardless of their ethnicity or geographical location. Drug use is penetrating all levels of social, economic and ethnic strata and its effects are challenging the traditional authority of community leaders and policing agencies. There clearly exists the potential for homogenous groups to withdraw from active participation in the wider Australian community, this could leave them highly susceptible to influences from sources like Al-Manar.

The linkage between Al-Manar and Hizballah is such that cameramen are often in position to get footage that no other new agency has access to. This level of cooperation clearly indicates a high degree of trust with the inference that Al-Manar journalists and camera crews may have prior knowledge of Hizballa and Palestinian operations .

The ability to disseminate material favourable for their cause has enhanced Hizballa's standing and esteem in the Arab world. The medium by which to exert influence is normally accompanied by the responsibility that it entails. These guiding ethics of journalism have led to it being cited as the fourth estate where truth and integrity in reporting pertinent and newsworthy information are seen as key principles. Al-Manar has by definition always admitted its journalistic bias in reporting and it was one of the first Arabic media outlets to perpetrate the conspiracy theory regarding the events on 9/11 . This has resulted in many in the Arab world believing that the attacks were carried out by Mossad with some U.S. assistance thereby removing any sympathy that would be normally generated by such a large loss of civilian life.

However, one program regularly broadcast on Al-Manar presents a chilling insight into the mindset of a suicide bomber when his family stated, "our youths do not dream of luxury and comfort; they dream of life after death" . In Tunis, 2005 key industry and government leaders met at the, World Summit on the Information Society (WSIS). One of the keynote speakers at the event was Israeli Foreign Minister Silvan Shalom who on 16 November delivered an address clearly identifying the dangers posed by Hamas and its use of the Internet stating that it, "is one of the most active terrorist groups on the Net. It runs no less than eight Internet sites in seven languages" .

One way in which governments have reacted to the identified threat posed by AL-Manar is to legislate and prevent its provider service from broadcasting it in their respective countries. However the current broadcast technology makes it difficult to actually achieve this without the cooperation of the service provider. In France this was achieved by political pressure on Eutelsat, which is a French owned company that was carrying the Al-Manar signal. However, Nilesat, which is Egyptian owned and Arabsat, which is Saudi, owned, are still capable of broadcasting to an audience in France .

Whilst not in the same ideological frame as Al-Manar the Doha based Arabic news network Al-Jazeera has frequently being the first media organization to air controversial videos from conflicts in places like Iraq. Whilst the ability of this network to reach Arabic speaking viewers globally is understood there is some debate regarding its new English language news channel and the manner in which it will frame issues like "terrorism and resistance", (http://news.bbc.co.uk/2/hi/middle_east/6105952.stm). This is pertinent when consideration is given to the dramatic expansion in viewer audience that is likely.

TERRORIST WEB SITES

Whine identifies two extremist groups as being pivotal in the use of the Internet by terrorists these being the Islamic Extremists and members of the Far Right or White Supremacist Movement. Whilst the Islamists seek a return to the Caliphate, the Far Right seek a utopia where they can live untroubled by other races, politicians or the rule of law . Given the very nature of the ideology of these groups it is of concern that they appear to be forming virtual alliances against what they perceive as a common enemy, even if it is an alliance of convenience. This common enemy is seen as the state of Israel and the disproportionate influence on global activities they perceive exerted by members of the Jewish faith .

One of the better known Far Right websites is 'Aryan Nations' . On this site are links to Mujahideen and Islam, which take the enquirer to forums regarding Islamic related topics posted next to Nazi SS symbols. Another Far Right site is Stormfront 'White Pride World Wide' and whilst this site as yet has no links to Islamic websites it shares many of the characteristics of other extremist sites. These include multimedia, ideology, training, physical fitness and merchandise to promote the group.

The Islamist websites act as a conduit for information to those who are ideologically close but geographically distant. These sites provide material with a narrow puritanical interpretation of Islam from well known extremist authors, thereby creating the opportunity for someone to become 'virtually radicalised' without ever having contact with a member of a terrorist group in person. These sites are also useful in recruiting new members . The former leader of the Finsbury Park Mosque Abu Hamza used to promote his sermons and worldview by recording them on cassette tapes for sale across the UK . Amongst those attracted to Hamza's particular interpretation of Islam were university educated young men who understood the potential of the Internet. They began converting the sermons and writings of Hamza into digital format and uploaded them onto various websites where they freely accessible to anyone. Since the arrest of Hamza on terrorism related offences in the UK some of these sites have being shut down and others continue to relocate .

CONCLUSION

The phrase, "the Internet interprets censorship as damage and routes around it" is attributed to John Gilmore one of the co-founders of the Electronic Frontier Foundation . It clearly identifies the potential challenges of attempting to prevent the use of cyberspace by terrorist entities. Whilst there are technical means to attack such websites the legal challenges posed by the transnational nature of these activities place them beyond the legislative capabilities of nation states . Clearly more work is required at the international level to enact legislation that can successfully meet the challenges posed, by the exploitation of the Internet by terrorist entities. There needs to be an enforceable legal framework that limits the illegal activities conducted in cyberspace. The challenge here is to ensure cooperation between the governments and law enforcement agencies of those nation states involved. Existing information sharing infrastructure and procedures could be enhanced so organisations like INTERPOL can take a lead role in prosecuting offenders regardless of where they reside.

It is not only police and intelligence agencies that are seeking to learn from the Internet, the terrorists are also watching and learning. They review failed operations to see what prompted intervention by the police, they also look at material presented in open court which reveals capabilities and they also examine media reports particularly those that might include leaks regarding sensitive investigations .

It is intriguing that terrorist groups with such a puritanical worldview would avail themselves of one of the freedoms to which they are so vehemently opposed, when communicating or spreading their ideology . The use of the Internet by terrorists will need to be continually monitored and the material they circulate examined in an effort to both understand their motivations and prevent further attacks.

REFERENCES

COPYRIGHT

Simon O'Rourke ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission

of the authors.