Internet, Social Media and Terrorism

Lieutenant Colonel Sushil Pradhan*

"The hand-held video camera has become as important a tool of insurgency as the AK-47"1

Introduction

Terrorist campaigns have shifted from military campaigns supported by information operations, to strategic communications campaigns supported by guerrilla and terrorist operations. Managing perceptions is seen by these groups as a vital effort. The great virtues of the Internet like ease of access, lack of regulation, vast potential audiences, and fast flow of information, have been turned to the advantage of groups committed to terrorising societies to achieve their goals. Terrorist groups like Al Qaeda, Hezbollah and Hamas use a vast and anonymous terrorist web network as another front in their war against their enemies.

Virtually every terrorist group in the world today has its own Internet website and, in many instances, multiple sites in different languages with different messages tailored to specific audiences2. Web sites are only one of the Internet's services used by modern terrorism. There are other facilities on the Internet; e-mail, chat rooms, e-groups, forums, virtual message boards, social media networks and blogs that are increasingly used by terrorists as virtual training camps, providing an online forum for indoctrination as well as the distribution of terrorist manuals, instructions, and data.

While terrorist organisations still invest in the weapons of kinetic warfare, they are also investing heavily in laptops, generators, and video editing software, and making effective use of high-speed Internet connections available at Internet cafés in towns and cities throughout the world. The emergence of new means of communication and new styles of virtual social interaction has transformed the context for mass persuasion and has expanded opportunities for extremists to disseminate their message.3

Terrorism and the Internet

Terrorist websites target three different audiences; current and potential supporters, international public opinion, and enemy publics (i.e. citizens of the states against which the terrorists are fighting). Contemporary terrorists can use the Internet in eight different ways.4

(a) Psychological Warfare. Terrorists can use the Internet to spread disinformation, to deliver threats intended to distil fear and helplessness, and to disseminate horrific images of recent actions, such as the videotape of the brutal murder of the American journalist Daniel Pearl by his captors.

(b) Publicity and Propaganda. The Internet has significantly expanded the opportunities for terrorists to secure publicity. They can shape how they are perceived by different target audiences and to manipulate their own image and the image of their enemies.

(c) Data Mining. Terrorists can learn from the Internet a wide variety of details about targets such as transportation facilities, nuclear power plants, public buildings, airports and ports; and even about counterterrorism measures.

(d) Fund raising. Like many other political organisations, terrorist groups use the Internet to raise funds. Al Qaeda, for instance, has always depended heavily on donations, and its global fund raising network is built upon a foundation of charities, NGOs, and other financial institutions that use websites and Internet-based chat rooms and forums.

(e) Recruitment and Training. In addition to seeking active recruits, terrorist organisations capture information about the users who browse their websites. Users who seem most interested in the organisation's cause or well suited to carrying out its work are then contacted. The Internet also serves as a 'virtual sanctuary' and training ground where training manuals and videos can be posted.5

(f) Networking. Most terrorist groups have undergone a transformation from strictly hierarchical organisations with designated leaders to affiliations of semi-independent cells that have no single commanding hierarchy. Through the use of the Internet, these loosely interconnected groups are able to maintain contact with one another; and with members of other terrorist groups.

(g) Sharing Information. The World Wide Web is home to dozens of sites that provide information on how to build chemical and explosive weapons. Many of these sites post well-known manuals like The Terrorist's Handbook, *The Anarchist Cookbook, The Mujahadeen Poisons Handbook, The Encyclopedia of Jihad* (prepared by Al Qaeda) and *How to Make Bombs* that offer detailed instructions on how to unleash terror attacks.

(h) Planning and Coordination. Terrorists use the Internet to plan and coordinate specific attacks, like Al Qaeda operatives did for the September 11 attacks. Hamas activists in the Middle East use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel; like the Lashkar-e-Taiba did in the case of the 26/11 Mumbai attack. Instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of *steganography,* which involves hiding messages inside graphic files. They can use publicly accessible tools like Google Earth, Google Latitude and encrypted messaging to plan and execute their attacks.6

The Technology Advantage

The ease with which individuals can create and disseminate content has been radically enhanced through a variety of technological developments. Some of the technological developments that have given rise to present day application

include increased bandwidth, speed of Internet connections, improved tools for posting content, digitalisation of technology using high-quality, user-friendly cameras and video editing tools, Internet penetration, advances in social networking, and capitalisation of the Internet (people are making money by posting content and generating traffic).7

A key defining characteristic of what is called 'Web 2.0' is actually the separation of form and content.8 Users are now able to "mash" content (through what are known as "mash-ups") with little effort. The new language XML enables automated data exchange, free of formatting constraints. This allows users to both upload and export data with ease, facilitating collaboration, information sharing, and network formation.

At the core of new Internet is a significant shift in the way messages and images are shared and, as a result, the way perceptions are formed. One of the central concepts is that of 'user-generated content.' User-generated content refers to the material created and posted by the end user, whether it is newlyweds posting their wedding photos on Flickr, or an aspiring terrorist posting his ruminations on his personal blog or uploading a graphic video to YouTube.9 The phenomenon represents a broad change in the way in which the Internet is being used by individuals, a change that cuts across diverse societal groups and demographics.

Viral marketing include effortless transfers between individuals, exploiting common behaviours, and utilising existing communication networks. Many of the aspects of this strategy have significant parallels with the ways in which militants have sought to disseminate their messages and use this new environment to their strategic advantage.

The fastest growing websites today are sites that are built around social interaction. Video and photo sharing, as well as networking sites like MySpace and Facebook, derive their purpose from a social basis; from people uploading information about themselves and their beliefs, tastes and activities, with the goal of broadcasting this content to a wide audience and creating a social connection. Much of this technology has been fused and integrated. For instance, once you upload videos to YouTube, the comment forums on YouTube function just like the feedback available on blogs.

Another important function included in many web applications is language translation. With the integration of this capability, the audiences for particular messages are dramatically expanded instantly, through the click of a mouse.

Cyberterrorism and Cyber attacks

Cyber-crime has now surpassed international drug trafficking as a terrorist financing enterprise10. Terrorist organisations seek the ability to use the Internet itself as a weapon in an attack against critical infrastructures. The effects of a widespread computer network attack would be unpredictable and might cause massive economic disruption, fear, and civilian deaths. Thus, cyber-terrorism in the form of unlawful, politically motivated computer attacks can intimidate or coerce a government or population to further a political objective, or to cause grave harm or severe economic damage.

Cyber-attacks attributed to terrorists have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial of service attacks, or defacing of websites. However, their increasing technical competency is resulting in an emerging capability for network-based attacks.12 The objectives of a cyber-attack may include loss of integrity (information could be tampered with), loss of availability (information systems are rendered unavailable to users), loss of confidentiality (critical information is disclosed to unauthorised users), and physical destruction (where information systems create actual physical harm through commands that cause deliberate malfunctions). Publicity would potentially be one of the primary objectives for a terrorist cyber-attack. Communication networks are likely to become the target of terrorist cyber attacks seeking to paralyse our societies and economies.

User Generated Content:The Power of Video and Blogs

The use of videos by radical groups for the purpose of incitement and radicalisation is not a new tactic in itself. But the recent emergence of various video-swapping websites, which facilitate easy upload, enjoy a vast viewership and provide an accompanying forum for commentary have enhanced the strategic value of such images and helped guarantee their ubiquity.

The most popular of such sites, YouTube, has proven to be an extremely useful tool for posting videos depicting insurgent attacks on American soldiers in Iraq or Afghanistan; or even of Western strikes killing innocent civilians.13 Improvements in digital video technology have allowed these productions to be easily paired with music and captions, with the end products attaining a high level of slick professionalism. Taliban fighters equipped with video cameras send visual images which are broadcast often only hours later. In Chechnya, mujahideen created videos and posted them on the Internet to disseminate their messages, to raise much needed funds and to demoralise Russian citizens.

Another realm of user generated content that has been harnessed effectively to propagate radical ideologies is the world of blogs. Blogs (or web logs, as they were originally named) tend to be written in the format of personal journals or diaries that use web publishing technology which facilitate quick and easy updates and displays postings in reverse chronological order. Blogs usually have lots of links to other related web based content like articles, web-sites, videos, or anything of interest to the blog writer.

One of the key distinguishing features of a blog is the forum it provides for reader's comments. The power (and potential danger) of the blog is that it offers users an opportunity to bypass traditional media outlets to publish their views and frame current affairs according to their own particular ideologies. This offers the opportunity for average people, or even terrorists, to emerge as key influencers or ideologues on a given issue, despite having no real credentials or authority.

Social Networking

Militants and terrorists have become extremely web-savvy and have recognised the value of social network sites like

Friendster, Facebook, Orkut and MySpace in reaching out to prospective followers. Of late, Al Qaeda and Taliban have started using Twitter to spread their propaganda.14 The Islamist extremists sent out their first tweet in English on May 12, 2011 claiming 'enemy attacked in Khak-e-Safid', with a link to their website for more details.

Britain's MI5 warned troops returning from service in Iraq and Afghanistan not to publicly post their personal information and details about their military tours due to the risk of possible terrorist activities being carried out against them.15 The soldier's identities were uncovered by militants after they posted information about their tours on Facebook.

It is easy to create extremist communities within an existing social network because the nature of these sites is highly decentralised and the massive membership makes surveillance nearly impossible. Young people tend to be idealistic, are often drawn to charismatic leaders, and many are seeking a cause to believe in, even if that cause promotes violence, hatred, and destruction.16 Online social network communities are a great way for militants to garner support and create a community of believers, where aberrant attitudes and beliefs may be exchanged, reinforced, hardened and validated.

Virtual Worlds and Video Games

Video games are valuable tools for shaping perceptions and for portraying a particular world view. They are a powerful media, because while they typically cast the user in the role of the hero, the opponent is often effectively demonised through its visual depiction and through other elements of the game's context. Embedded messages and images can have an insidious impact on the user, as the exposure to these subtle elements may ultimately shape ideas, values and attitudes. Video games are played primarily by children and teens, thus they present a valuable medium for the transmission of messages to an impressionable audience.

The Lebanese Hezbollah has been using video games as a central aspect of their information campaign for many years, in an effort to influence youth perceptions.17 At the beginning of the second Palestinian *Intifada,* the Hezbollah Internet Bureau created a video game called *Special Force,* in which the user tries to kill former Prime Minister of Israel Ariel Sharon and other Israeli dignitaries. The success of the first version of Special Force prompted Hezbollah to create *Special Force 2* in the aftermath of the Israeli-Hezbollah war, to give Lebanese children a chance to virtually experience attacking Israeli soldiers, launching Katyusha rockets at Israeli towns and ultimately claiming victory against Israel.

The Web 2.0 offers a new and different generation of online games which are more technologically sophisticated, and incorporate a dimension of social interactivity that blurs the line between virtual and real. These massive multiplayer online role playing games (MMORPGs) are fundamentally different from conventional video games as they dynamically connect real users (in their online avatars), from geographically disparate physical locations in real time through the virtual game environment. The vast social network of games like *Second Life* and its many counterpart games clearly offer unique opportunities for like-minded players from all over the world to connect, interact and communicate.

Meeting the Challenge

How should we respond to this challenge? Given the inter-connectedness of national networks into a single worldwide web, international cooperation is an imperative to counter the use of the Internet for terrorist purposes.18 First, we must become better informed about the uses to which terrorists put the Internet and be able to monitor their activities. Second, while we must better defend our society against terrorism, we must not provide governments (especially authoritarian governments and agencies with little public accountability), tools with which to violate civil liberties. India needs to have adequate preparations in terms of appropriate backup strategies; and plans on how to deal with the consequences of terrorist exploitation of the Internet. An effective strategy should limit and discredit the terrorist message, deny safe haven to terrorists on the internet, thwart their ability to obtain support from a vulnerable online population, and continue to monitor their communications on web forums. The private sector and the government also have a role in information campaigns aimed at discrediting terrorists by widely publicising their atrocities on the internet. Media entrepreneurs can follow the lead of Google, which has removed numerous violent Al Qaeda videos from YouTube. Internet providers that repeatedly aid terrorist entities by hosting their websites should be fined to the full extent of the law. The various aspects involved in combating terrorist activity promoted by the Internet are a vast and discursive subject, which needs to be explored in greater detail separately.

Endnotes

1. 'A World Wide Web of Terror', *Economist,* July 14, 2007, p. 28-30.

2. Bruce Hoffman, '*The Use of the Internet by Islamic Extremists*'. Testimony presented to the US House Permanent Select Committee on Intelligence (May 4, 2006), p. 18, available at http://rand.org/pubs.

3. Raphael Perl, '*Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation*', Report of the Organisation for Security and Cooperation in Europe (OSCE), April 2008.

4. Gabriel Weiman, '*How Modern Terrorism Uses the Internet*', US Institute of Peace, March 2004, available at www.usip.org.

5. Robert Dover and Michael Goodman (Eds), Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence, Columbia University Press, 2009, p.61.

6. Philip Seib and Dana Janbeck, Global Terrorism and New Media, Routledge, 2011.

7. Aidan Kirby Winn and Vera L Zakern, *'Terrorism and Strategic Influence:Jihad.com 2.0',* in Influence War: How Terrorists and Governments Fight and Shape Perception in a War of Ideas (Ed James Forest), Pentagon Press, 2010.

8. See Tim O'Reilly, *'What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software',* September 30, 2005, available at http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

9. *'Participative Web: User-Created Content',* Report of the Committee for Information, Computer and Communications Policy, OECD, on 12 April 2007, http://www.oecd.org/dataoecd/57/14/38393115.pdf.

10. John Rollins and Clay Wilson, 'Terrorist Capabilities for Cyber-attack: Overview and Policy Issues', US Congressional Research Service Report RL33123, 22 January 2007.

11. The Information Technology (Amendment) Act, 2008, declared cyberterrorism as a heinous cyber crime. Available at the web-site of the Department of Information Technology, Ministry of Communication and Information Technology, at http://www.mit.gov.in.

12. Catherine Theohary and John Rollins, 'Terrorist Uses of the Internet: Information Operations in Cyberspace', US Congressional Research Service Report R41674, 08 March 2011.

13. Edward Watt, 'Anti-US Attack Videos Spread on the Web,' *New York Times,* October 6, 2006, http://www.nytimes.com/2006/10/06/technology/06tube.html.

14. 'Taliban on Twitter as Afghan rebels enter Internet age', *Hindustan Times,* New Delhi, 15 May 2011.

15. Sean Rayment, 'Troops Warned Off Facebook Over Terror Fears,' *Telegraph Daily,* 12 November 2007, www.telegraph.co.uk.

16. Perry Aftab, 'Using the Web as a Weapon: the Internet as a Tool for Violent Radicalization and Home-grown Terrorism,' US House Committee on Homeland Security, 6 November 2007, available at http://homeland.house.gov/hearings/index.asp71D=102.

17. Toby Harden, 'Video Games Attract Young to Hezbollah,' *Telegraph Daily,* 21 February 2004, available at www.telegraph.co.uk.

18. the UN Working Group on Countering the Use of the Internet for Terrorist Purposes organised a meeting with Microsoft and Google in Feb 2011 in Seattle. Details available at http://www.un.org/terrorism/workgroup6.shtml.

***Lieutenant Colonel Sushil Pradhan** was commissioned into the 5th Battalion, the Mechansied Infantry Regiment (14 Kumaon) in 1990. Presently, he is Colonel Administration at the Mechanised Infantry Regimental Centre, Ahmednagar. He won the Second Prize in the COAS Essay Competition 2010 and is a regular contributor to professional journals.

Journal of the United Service Institution of India, Vol. CXLI, No. 585, July-September 2011.