INTERNET & TERRORISM IN THE AGE OF GLOBAL COMMUNICATION

By S.M. Aamir Ali & Rida Ahmad
From Aligarh Muslim University Murshidabad Centre, Murshidabad, West Bengal

Abstract:
Professor Park stated, "Man is not born human but to be made human", and one of the characteristic of it, is the man's ability to communicate. For the purpose of communicating with each other man have come up with different instruments and mechanism and internet is one of the most recent one. Myriad of websites offering the user the ability to upload videos, record opinions through blogs, wikis, twitter or Facebook and dynamically communicate with individuals have radically changed internet usage. Communicating any piece of information on social networking sites means that information you shared is conceivably available to any user of any degree around the world. The sphere of such users is as wide as the demographics of the globe itself. But at the same time these social networking sites are used by the hate mongers to spread rumors and the same plays a very lethal role in inciting violence in Indian subcontinent. And it is for this reason only that the countries like Bangladesh and Pakistan banned the major social networking sites at one point of time. The terrorists use the internet as an efficient tool for information gathering, propaganda schemes, recruitment and also to terrorize the civilians by posting and uploading videos and photos. They can easily spread powerful words to make an impression in the minds of men and women for joining the terrorist cells and network. Notoriously, the media and its coverage serve as a facilitator for the acts of terrorism. At this juncture when voices are being heard to declare internet as a human right, through the instant academic venture an effort has been made by the author to analyze the critical component of understanding the concept of terrorism and why terrorist draw their attention to media.

Key words:*Human right, Internet, Social media, Terrorism.*

"Terrorists use the Internet just like everybody else"
- Richard Clarke (2004)[1]

INTRODUCTION
In the age of global communication and international media the messengers of hate and terror are no longer impeded by national borders or regions; they can easily spread powerful words and images around the globe and condition impressionable men and women to be recruited into terrorist cells and networks. International and domestic terrorists exploit the traditional and the new

---

[1] As quoted in New 2004. Clarke was the White House cyber security chief during the tenures of both Bill Clinton and George W. Bush. He resigned in January 2003.

communication means to achieve a host of crucial objectives--most of all the media-dependent dissemination of their "propaganda of the deed" among friends and foes. Whether in the United States, Europe, the Middle East, the Far East, or any other region, the architects of terrorism exploit the mass-media— including the Internet for the benefit of their operational efficiency, information gathering, recruitment, fund raising, and propaganda schemes. But governments in countries whose populations are intimidated by terrorist attacks and threats thereof utilize the mass media as well to enlist public support for actual and alleged counterterrorist measures.

The internet has seen blistering development in user interaction in recent decade. Websites offering the users the ability to upload videos, record opinions through blogs, wikis, twitter or Facebook and dynamically communicate with individuals have radically changed internet usage. 'Traditional' internet usage (known as Web 1.0) was based on static websites, which allowed searching different websites for information (with the help of search engines) and downloading required contents. However, the traditional model of static website has been replaced by much more interactive, efficient and dynamic approach (Web 2.0), which allows people to upload, download, chat and blogging and communicates conveniently. Social networking sites and virtual world are at

forefrontof this development as users are no longer simply engaged with the internet in a passive manner, rather through a huge range of media and through a tranche of various inter-faces, including personal computers, mobiles and game consoles.[2]

Communicating any piece of information on social networking sites means that information you shared is conceivably available to any user of any degree around the world. The sphere of such users is as wide as the demographics of the globe itself, with no demarcation in membership as senior and junior, well-off and destitute have to large degree equality of online opportunity.[3] Social networking sites are emerging as a new organizing system as dates, meeting, events, and updates can all be managed through one of these sites.

Various terrorist groups today realize that targeting their enemies through physical violence, while influential, is not solely the best recourse to gaining an overall victory for their cause. Sophisticated terrorists realize that in initiating their terrorist campaign, which does not only need patience, but there is also a piece called propaganda that is heavily involved in the orchestration of activities.

WHY TERRORISTS DRAWN TO INTERNET
Since the 1970s, the degree of global interconnectedness has been demonstrated throughout the world from economies to cultures. New methods of

---

[2]Kevin M Roger, The Internet and the Law, pg-213(Palgrave Macmillan, 1ˢᵗ edition, 2011)

[3]Id at 214.
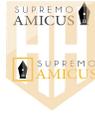
global communication have broaden the possibilities in organizing and mobilizing like-minded individuals and groups throughout the world to include activities of transnational criminal and terrorist networks.[4] "The technological advances associated with globalization have improved the capabilities of terrorist groups to plan and conduct operations with far more devastation and coordination than their predecessors could have imagined. In particular, technologies have improved the capability of groups and cells in the following areas: proselytize coordination, security, mobility and lethality."[5] In the past, States have had the ability to control information flow and use far superior resources to undermine terrorists and their cause while simultaneously winning the hearts and mind of the populace. However, because of globalization, particularly in the area of technology, terrorist groups share in the ability to leverage media technologies to work in their best interest. The increase in internet service providers and the access to more proficient and inexpensive computer, software and wireless technology has empowered terrorist groups with the ability to advertise their causes through the World Wide Web. "Once limited to mimeographed manifestos, some terrorist and their supporters are now capable of building web sites to post any information they choose."[6]

Terrorists use different types of media in a variety of ways, namely as an information instrument, to generate publicity and draw attention to their cause. "Through propaganda, terrorists seek to communicate a particular message to a particular target audience."[7] The purpose and messages behind their communication differs and is dependent on the targeted audience. These messages are designed to be informative, educational, rallying, for soliciting support, and for recruitment. They can also be coercive by being either threatening or winning over its audience through flattery. Through coercion, these groups hope to intimidate and undermine the populace's confidence in the government and leadership, and as a result cripple government and the security forces' ability to prevent, defend and strike back when attacked. This information instrument can also be used by terrorist towards their own members in order to strengthen cohesiveness, boost morale and relieve groups of internal strife. In sum, sympathy and support from the populace for their cause is the ultimate goal.

FIVE TERRORIST USES OF THE INTERNET
   1. **INFORMATION PROVISION**
This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. The

---

[4]Baylis, John; Smtih, Steve, (2006), The Globalization of World Politics: An Introduction to International Relations, p. 20,
[5] Id at p. 489)

[6] Id at p. 489)

[7]Hoffman, Bruce, (2006), Inside Terrorism, p. 199, available at:
http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf

Internet, and the advent of the World Wide Web in particular, have significantly increased the opportunities for terrorists to secure publicity. This can take the form of historical information, profiles of leaders, manifestos, etc. But terrorists can also use the Internet as a tool of psychological warfare through spreading disinformation, delivering threats, and disseminating horrific images, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist Daniel Pearl in Pakistan via their Web sites.[8] These functions are clearly improved by the Web's enhanced volume, increased speed of data transmission, low-cost, relatively uncontrolled nature, and global reach.
As Weimann points out, "these traditional media have 'selection thresholds' (multistage processes of editorial selection) that terrorists often cannot reach"[9] The same criteria do not, of course, apply to the terrorists' own websites. The Internet thus offers terrorist groups an unprecedented level of direct control over the content of their message(s).

2. FINANCING

Money is terrorism's lifeline; it is "the engine of the armed struggle".[10] The immediacy and interactive nature of Internet communication, combined with its high-reach properties, opens up a huge

potential for increased financial donations as has been demonstrated by a host of non-violent political organizations and civil society actors. Terrorists seek financing both via their Web sites and by using the Internet infrastructure to engage in resource mobilization using illegal means.

Numerous terrorist groups request funds directly from Web surfers who visit their sites. Such requests may take the form of general statements underlining the organizations need for money, more often than not however requests are more direct urging supporters to donate immediately and supplying either bank account details or an Internet payment option. Another way in which groups raise funds is through the establishment of online stores and the sale of items such as books, audio and video tapes, flags, t-shirts, etc.

The Internet facilitates terrorist financing in a number of other ways besides direct solicitation via terrorist Web sites. According to Dutch experts, there is strong evidence from international law enforcement agencies such as the FBI that at least some terrorist groups are financing their activities via advanced fee fraud, such as *Nigerian-style scam e-mails*.[11] To date, however, solid evidence for such claims has not entered the public

---

[8] Weimann, Gabriel. 2004a. *WWW.terror.net: How Modern Terrorism Uses the Internet*. Washington DC: United States Institute of Peace. Available at: http://www.usip.org/pubs/specialreports/sr116.pdf
[9] Ibid

[10] Napoleoni, Loretta. 2004. 'Money and Terrorism.' *Strategic Insights* 3(4). Available at: http://www.ciaonet.org/olj/si/si_3_4/si_3_4_nal01.pdf
[11] https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

realm.[12] There is ample evidence, however, to support the contention that terrorist-affiliated entities and individuals have established Internet-related front businesses as a means of raising money to support their activities.

Terrorist organizations have a history of exploiting not just businesses, but also charities as undercover fundraising vehicles. This is particularly popular with Islamist terrorist groups, probably because of the injunction that observant Muslims make regular charitable donations. In some cases, terrorist organizations have actually established charities with allegedly humanitarian purposes.[13]

3. NETWORKING

This refers to groups' efforts to flatten their organizational structures and act in a more decentralized manner through the use of the Internet, which allows dispersed actors to communicate quickly and coordinate effectively at low cost. The Internet allows not only for intra-group communication, but also inter-group connections. The Web enhances terrorists' capacities to transform their structures and build these links because

of the alternative space it provides for communication and discussion and the hypertext nature of the Web, which allows for groups to link to their internal sub-groups and external organizations around the globe from their central Web site.

Many terrorist groups share a common goal with mainstream organizations and institutions: the search for greater efficiency through the internet.[14] As discussed, the new technologies enable quicker, cheaper, and more secure information flows. In addition, the integration of computing with communications has substantially increase the variety and complexity of the information that can be shared.[15]*This led Michele Zanini to hypothesize that "the greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decision making".[16]* Zanini's hypothesis appears to be borne out by recent events. For example, many of the terrorists indicted by the United States government since 9/11 communicated via e-mail.[17]

The Net offers a way for like-minded people located in different communities to interact easily, which is particularly

---

[12] Libbenga, Jan. 2004. 'Terrorists Grow Fat on E-Mail Scams.' *The Register* 28 September. http://www.theregister.co.uk/2004/09/28/terrorist _email_scams/

[13]TERRORIST 'USE' OF THE INTERNET ANDFIGHTING BACK, *Maura Conway,* Available at: https://www.oii.ox.ac.uk/archive/downloads/r esearch/cybersafety/papers/maura_conway. pdf

[14] Margulies, Peter. 2004. 'The Clear and Present Internet: Terrorism, Cyberspace, and the First

Amendment.' *UCLA Journal of Law and Technology* 8(2). http://www.lawtechjournal.com/articles/2004/04 _041207_margulies.pdf

[15] Weimann, Gabriel. 2004a. *WWW.terror.net: How Modern Terrorism Uses the Internet*. Washington DC: United States Institute of Peace. Available at: http://www.usip.org/pubs/specialreports/sr116.p df

[16] Ibid.

important when operatives may be isolated and having to 'lie low.' Denied a physical place to meet and organize, many terrorist groups are alleged to have created virtual communities through chat rooms and Web sites in order to continue spreading their propaganda, teaching, and training. Clearly, "information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility."[18] It "puts distance between those planning the attack and their targets and provides terrorists a place to plan without the risks normally associated with cell or satellite phones."[19]

4. RECRUITMENT

This refers to groups' efforts to recruit and mobilize sympathizers to more actively support terrorist causes or activities. The Web offers a number of ways for achieving this: it makes information gathering easier for potential recruits by offering more information, more quickly, and in multimedia format; the global reach of the Web allows groups to publicize events to more people; and by increasing the possibilities for interactive communication, new opportunities for assisting groups are offered, along with more chances for contacting the group directly. Finally, through the use of discussion forums, it is also possible for members of the public-- whether supporters or detractors of a group--to engage in debate with one another. This may assist the terrorist group in adjusting their position and tactics and, potentially, increasing their levels of support and general appeal.[20]

Online recruitment by terrorist organizations is said to be widespread. **Harris et al provide t**he example of an Iranian site that boasts an application for suicide bombers guaranteeing that the new 'martyr' will take seventy relatives with him into heaven. If the recruit is unsure about joining, or if the group is unsure about the recruit, he is directed to a chat room where he is 'virtually' vetted. If he passes muster, he will be directed to another chat room for further vetting, and finally contacted personally by a group member. This process is said to be aimed at weeding out 'undesirables' and potential infiltrators.[21] It is more typical, however, for terrorist groups to actively solicit for recruits rather than waiting for them to simply present themselves. Weimann suggests that terrorist recruiters may use interactive Internet technology to roam online chat rooms looking for

---

[18] Tibbetts, Patrick S. 2002. *Terrorist Use of the Internet and Related Information Technologies*. [Unpublished Paper]. Fort Leavenworth, Kansas: United States Army Command and General Staff College. http://stinet.dtic.mil/cgi-
[19] Thomas, Timothy L. 2003. 'Al Qaeda and the Internet: The Danger of "Cyberplanning."' *Parameters* Spring. http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm

[20] Gibson & Ward 2000, 305-306; Soo Hoo, Goodman & Greenberg 1997, 140; Weimann 2004a.
[21] Margulies, Peter. 2004. 'The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment.' *UCLA Journal of Law and Technology* 8(2). http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf

receptive members of the public, particularly young people. Electronic bulletin boards could also serve as vehicles for reaching out to potential recruits.[22]

5. INFORMATION GATHERING

This refers to the capacity of Internet users to access huge volumes of information, which was previously extremely difficult to retrieve as a result of its being stored in widely differing formats and locations. Today, there are literally hundreds of Internet tools that aid in information gathering; these include a range of search engines, millions of subject-specific email distribution lists, and an almost limitless selection of esoteric chat and discussion groups. One of the major uses of the Internet by terrorist organizations is thought to be information gathering. Unlike the other uses mentioned above, terrorists' information gathering activities rely not on the operation of their own Web sites, but on the information contributed by others to "the vast digital library" that is the Internet.[23] There are two major issues to be addressed here. The first may be termed 'data mining' and refers to terrorists using the Internet to collect and assemble information about specific targeting opportunities. The second issue is 'information sharing,'

which refers to more general online information collection by terrorists.

Terrorists can also use the Internet to learn about antiterrorism measures. Even a simple strategy like conducting word searches of online newspapers and journals could allow a terrorist to study the means designed to counter attacks, or the vulnerabilities of these measures.

As an example, Jessica Stern points to *Bacteriological Warfare: A Major Threat to North America (1995)*, which is described on the Internet as a book for helping readers survive a biological weapon attack and is subtitled 'What Your Family Can Do Before and After.' However, it also describes the reproduction and growth of biological agents and includes a chapter entitled *'Bacteria Likely to Be Used by the Terrorist.'* The text is available for download, in various edited and condensed formats, from a number of sites while hard copies of the book are available for purchase over the Internet from sites such as Barnesandnoble.com for as little as $13.[24]

This kind of information is sought out not just by sophisticated terrorist organizations but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas.

---

[22] Weimann, Gabriel. 2004a. *WWW.terror.net: How Modern Terrorism Uses the Internet*. Washington DC: United States Institute of Peace. Available at: http://www.usip.org/pubs/specialreports/sr116.pdf

[23] (Weimann 2004a, 6)

[24] Stern, Jessica. 1999. *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press, p. 51.
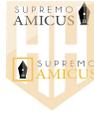
The threat posed by the easy availability of bomb-making and other 'dangerous information' is a source of heated debate. We must not underestimate the feasibility of such threats. As a result, many have called for laws restricting the publication of bomb-making instructions on the Internet, while others have pointed out that this material is already easily accessible in bookstores and libraries[25] (ADL 1998). In fact, much of this information has been available in print media since at least the late 1960s, with the publication of William Powell's The Anarchist Cookbook and other, similar titles. Finally, it is important to keep in mind that removal of technical information from public Web sites is no guarantee of safeguarding it. In essence, this effort is akin to 'closing the barn door after the horse has bolted.'

THE MEDIA AND COUNTERTERRORISM

Use of the Internet is a double-edged sword for terrorists. They are not the only groups 'operating' the Net (Rogers 2002, 191), which can act as a valuable instrumental power source for anti-terrorist forces also. The more terrorist groups use the Internet to move information, money, and recruits around the globe, the more data that is available with which to trail them. Since 9/11 a number of groups have undertaken initiatives to disrupt terrorist use of the Internet, although a small number of such

efforts were also undertaken previous to the attacks. Law enforcement agencies have been the chief instigators of such initiatives, but they have been joined in their endeavors by other government agencies as well as concerned individuals and various groups of hacktivists.

Just as terrorists utilize and exploit the domestic and international triangles of political communication, government officials as well take advantage of this form of mass communication while displaying less expertise than terrorist groups in using the Internet for their purpose. Indeed, whereas terrorists must resort to violence or make credible threats to be admitted to the triangle of political communication by the gatekeepers of the traditional media, highly placed public officials do not have to unleash violence to gain such access because they form one corner of the domestic communication triangle and are part of the international triangular communication linkages as well. From this position of strength governmental sources tend to dominate reporting on foreign and security policy—especially when this involves military conflict or the likelihood of military deployment.

Freedom of the press is a fundamental right in liberal democracies because only a media free from governmental control can function as a check on governments in the interest of citizens. However, just

---

[25] Anti-Defamation League (ADL). 1998. 'Terrorist Activities on the Internet.' *Terrorism Update* Winter.http://www.adl.org/Terror/focus/16_focu

s_a.asp, Associated Press. 2002. 'Man Hijacks Al-Qaeda Site for FBI Use.' *USA Today* 30 July. http://www.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm
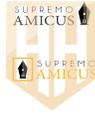
as during war time and other serious international crises the press may be caught up in a public outburst of patriotism in reaction to terrorism at the expense of its watchdog responsibilities. Whether this change from watchdog to lapdog is the result of self-censorship or of intimidation by governments and their supporters, or both, the result is the same: Domicile media organizations allow presidents and other governmental leaders far more latitude to enact emergency policies and enlist support for extreme military actions in response to terrorist strikes and threats than they would in times of normalcy. Thus, when societies suffer major terrorist blows, citizens tend to rally around their government leaders and thereby strengthen their presidents' or prime ministers' hands to effectively respond to such attacks.

CONCLUSION

Researchers are still unclear whether the ability to communicate online worldwide has resulted in an increase or a decrease in terrorist acts. It is agreed, however, that online activities substantially improve the ability of such terrorist groups to raise funds, lure new faithful, and reach a mass audience.[26] The most popular terrorist sites draw tens of thousands of visitors each month. Obviously, the Internet is not the only tool that a terrorist group needs to 'succeed.' However, the internet has added new dimensions to existing assets that groups can utilize to achieve their

goals as well as providing new and innovative avenues for expression, fundraising, recruitment, etc. At the same time, there are also tradeoffs to be made. High levels of visibility increase levels of vulnerability, both to scrutiny and security breaches. The proliferation of official terrorist sites appears to indicate that the payoffs, in terms of publicity and propaganda value, are understood by many groups to be worth the risks.

Freedom of the press and speech is another challenge faced. Some argue that limiting access to the press to obtain information is wrong and that the public deserves to know what is taking place throughout the world. Sadly they fail to understand the impact of unlimited dissemination of information when arguing limitations. Appeals to patriotism to "muzzle independent media;" legal and legislative measure in place; self-censorship; and steps taken to restrict privacy on the internet and encryption software to protect email traffic are just some of the tools that some argue should not be used against the media. The one thing that is indisputable is that the media feeds on violence; and whoever can tell the most violent story wins the audience. This is not really about freedom of speech, but rather who will get the biggest audience and thus reap the capitol benefits.

Google has taken a step in the right direction. In order to avoid legal liability,

---

[26]Arquilla, John & David Ronfeldt. 2001a. 'Emergence and Influence of the Zapatista Social Netwar.' In John Arquilla & David Ronfeldt

(Eds.), *Networks and Netwars*. California: Rand. http://www.rand.org/publications/MR/MR1382/MR1382.ch6.pdf

Google's French and German no longer offer anti-Semitic and pro-Nazi websites to surf; however these sites still remain on Google's main U.S. based site. German law considers the publication of Holocaust denials and similar material as an incitement of racial and ethnic hatred, and therefore illegal. France has similar laws that allowed a students' antiracism group to successfully sue Yahoo in a Paris court for allowing Third Reich memorabilia and Adolf Hitler's "Mein Kampf" to be sold on the company's auction sites." However, in November 2001, a U.S. judge ruled that Yahoo was free from liability because of the First Amendment's guarantee of free speech.[27]

*****

---
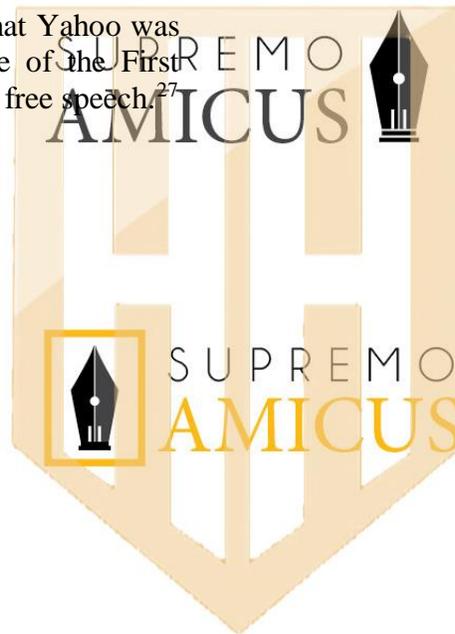
[27] McCullagh, Declan. 2003. 'Military Worried About Web Leaks.' *C/Net News* 16 January. http://news.com.com/2100-1023-981057.html