

FROM INTERNET TO ISLAMNET: NET-CENTRIC COUNTER-TERRORISM

By B. Raman

22 October 2005

(Paper presented at a conference jointly organised by the State Islamic University (UIN) of Jakarta and the Institute for Defence Analyses (IDA) of Washington DC at Bali, Indonesia, from October 19 to 21,2005)

INTRODUCTION

The Internet enables every jihadi to feel part of a larger whole. It enables every angry Muslim to give vent to his or her anger in myriad ways. It enables every Muslim to become a participant in the jihad in his or her own way, with or without a leader. It has strengthened Islamic solidarity. Cyber space has become the spawning ground of jihadi warriors. The use of the Internet by the jihadi terrorists illustrates the folly of dismissing them as irrationals or as persons with a medieval mind. An irrational person or one with a medieval mind cannot use the Internet as effectively as the jihadi terrorists have been doing. In this paper, the increasing use of the Internet by international jihadi terrorist organisations would be discussed under six heads: Propagation; Communication; data mining; cyber warfare; other aspects; and Net-centric counter-terrorism.

PROPAGATION

2. All political dissident and other minority groups who in the past lacked access to the conventional media---print or electronic--- have found in the Internet an easily available means of propagating their cause, creating an awareness of their ideology, winning adherents and promoting a feeling of solidarity and unity of action for achieving their objective. Web activism is not a recent phenomenon and not confined to Islamic groups---moderate or extremist.

3. Terrorist organisations of different hues ---ethnic, ideological or religious--- too have found in the Internet an ideal tool for facilitating the pursuit of their objectives. The international jihadi terrorist organisations were not the first to turn to the Internet. Ethnic terrorist organisations like the Liberation Tigers of Tamil Eelam (LTTE), ideological terrorist organisations such as the Maoist groups of India and Nepal and religious terrorist organisations such as those of the Punjab in India and the Irish Republican Army (IRA) in the UK were amongst the earliest to have realised the utility of the Internet as an operational tool in their attempts to achieve their objective.

4. Amongst the indigenous jihadi terrorist organisations, those of the Palestinians and pro-Palestinian groups, the Chechens and the Kashmiris were the first to start using the Internet for propagating their cause. These were followed by organisations in Indonesia. Jihadi terrorist organisations with pan-Islamic objectives and trans-national networking started using the Internet in a big way only in 2000 and, since then, have replaced the indigenous jihadi terrorist organisations as the most extensive and innovative users of the Internet.

5. The initial use of the Internet---whether by the indigenous jihadi organisations or by the pan-Islamic ones--- was confined to the creation and the use of web sites for propagating their cause, for enrolling members and collecting funds. The web sites were also used for a psychological warfare (PSYWAR) against their State adversaries through the dissemination of details of their alleged suppression of the Muslims.

6. Well-known and well-identified jihadi organisations restricted their use of the web sites for purposes, which would not bring them into conflict with the law. They refrained from using their web sites for purposes such as giving instructions on how to wage a jihad through means such as the fabrication of an improvised explosive device (IED), publicising their claims relating to the successful commission of acts of terrorism etc.

7. Amongst the ostensibly legitimate purposes for which they used their web sites were proclaiming their objectives and policies, disseminating statements of their leaders, carrying articles on different aspects of Islam, and making appeals for volunteers and funds. The web sites took care not to let themselves be seen as indulging in and justifying acts of terrorism.

8. However, this cautious policy did not prevent them from indirect facilitation of acts of terrorism through means such as dissemination of articles carried by the professional journals and web sites of governmental institutions like the Armed Forces and the police on matters such as the low-intensity conflict, which indicated the various ways in which terrorist and insurgent organisations functioned. Their purpose in carrying such articles was to facilitate copy cat terrorism, without falling foul of the law. In their perception----which was valid---since they were mostly reproducing articles on the modus operandi of other terrorist organisations written by governmental experts, they were not committing any breach of the law.

9. The period before 2000 also saw the emergence of a number of web sites created by either Muslim individuals or by organisations not identified with indigenous or pan-Islamic terrorist organisations. They sought to encourage feelings of Islamic solidarity and made Muslims aware of the writings and teachings of well-known jihadi leaders associated with organisations such as the Muslim Brotherhood. An important example is the writings and statements of the late Abdullah Azzam, considered one of the mentors of Osama bin Laden, which started appearing in these web sites. The purpose of these web sites was to provide a religious and ethical justification for jihad.

POST-1998 MUSHROOMING

10. Statements condemning the US and Israel and projecting them as the enemies of Islam and the Muslims started appearing with increasing frequency in all the web sites of the pan-Islamic jihadi terrorist organisations after the formation of the International Islamic Front (IIF) for Jihad Against the Crusaders and the Jewish People by Osama bin Laden from his hide-out in Kandahar in February, 1998. The IIF sought to bring together in a trans-national network bin Laden's Al Qaeda, an exclusively Arab terrorist organisation, and a number of non-Arab jihadi terrorist organisations operating from countries such as Pakistan, the Central Asian Republics, Egypt, the Philippines, Bangladesh etc. The frequency and virulence of the anti-US

statements carried by these organisations increased after the US Cruise missile attacks on alleged training camps of the Al Qaeda in Afghanistan and the Sudan in August, 1998.

11. The projection of the US as the principal enemy of Islam became the defining characteristic of all pan-Islamic jihadi extremist or terrorist organisations after the Cruise missile attack. However, the indigenous jihadi terrorist organisations such as those of the State of Jammu & Kashmir (J&K) in India and Chechnya in Russia refrained from adopting any anti-US propaganda line in their web sites.

12. In February 2000, a search of the World Wide Web (WWW) by this writer, even if not very exhaustive, led to about 1,500 sites of Islamic organisations. Most of them had the benign objective of helping in a better understanding of Islam among Muslims and non-Muslims alike. They contained interpretations of the holy Koran, explanations of Islamic religious traditions and practices and articles on the contribution of Islam to science and fine arts etc. They also provided a useful database of the Muslim scientists, thinkers and women engineers of the world, the Muslim media and so on.

13. The following conclusions emerged from their study undertaken by this writer at that time:

* A large majority of them was Sunni and Wahabi sites, with very few Shia or Iran-based ones. Some were anti-Ahmadiya.

* The preponderance of sites run by members of the Muslim community of the US. The next in number were those of Western Europe, Malaysia, Indonesia and Pakistan.

* There was a large network of Muslim Students' Associations in US universities. All of them had their sites.

* The US also had some sites meant for Muslim members of the US armed forces. There was one site, called Muslim Military Members (MMM), which enrolled adherents from the Muslims serving in the armed forces of different countries all over the world. It described its aim as follows: " The MMM is an information source for brothers and sisters serving in the armed forces. We are a gathering point. A place where information is disseminated. A means to keep people informed. Through MMM, you will stay informed of different events, resources and news items to help you survive as a Muslim in the armed forces. The MMM is not an official organisation, but rather a loose association of military personnel and those in the service of military personnel. The cost of the web site is provided freely as a service by the Islamic Information Office, paid by Muntadanet.Inc."

* The comparatively fewer sites from West Asia and North Africa, which was explained by the restrictions there on non-government organisations (NGOs) and also possibly by local curbs on access to the Internet.

* Surprisingly, while there were about 50 sites focusing on the problems and history of the Muslims of Jammu & Kashmir, one noticed only three sites relating to the Muslims in the rest of India-- those of the Aligarh Muslim University Alumni, the

Indian Muslim Relief Committee and the "Islamic Voice", a journal published from Bangalore. It was possible there were many more sites, but the search engines did not pick these up.

* While there were many sites to discuss the relations of Islam with Christianity and Judaism, one did not come across any on relations with Hinduism.

14. Of the 1,500 sites studied by this writer, only about 150 contained extremist material relating to the so-called jihad. The rest of them appeared to be benign in their objectives. The majority of the jihadi sites was run by Muslim extremist organisations in different parts of the world which had taken to violence to achieve their political and/ or religious objectives. Individual Muslims also kept some with assumed names such as Abu Mansoor, Abu Mujahid, Abu Jindal etc.

15. Some of these jihadi sites performed the following services:

* Dissemination of information regarding the jihad in different countries.

* Instructions on how to become a Mujahideen, how to manufacture explosives etc.

* Database on the availability of arms and ammunition for purchase, including the prices. The sites providing Muslims in apparently ran this information the US, because the arms sellers recommended by them were all based in the US.

* A bibliography of articles on urban warfare and low-intensity conflicts, which had appeared in the military and strategic journals of the US. A list of 266 such articles was available. Many of them had been collated from the US Marine Corps Doctrine Publications, the Marine Corps War fighting Publications, the Marine Corps Reference Publications and the US Army Field Manuals. One can directly access many of these articles at the Army Doctrine and Training Digital Library sites, by just clicking on the relevant titles.

* Examples of articles collated by these jihadi sites: Operations in a Low Intensity Conflict; Physical Security; Intelligence Preparation of the Battlefield; Intelligence Officers' Handbook; Military Operations in Built-up Areas; Urban Warfare Communications; Air Operations in Low Intensity Conflicts; Bomb Protection Handbook; Chemical/Biological/Radiological Incident Handbook, purported to have been prepared by the CIA; Chemical Warfare Handbook of the Marine Corps Institute; Chemical Warfare Agents; Military Intelligence--Using Organic Assets; Psychological Operations in Guerilla Warfare, purported to have been prepared by the CIA's Psywar Division for use in Nicaragua; Dealing With Vehicle Hijacking Situations; Emergency Response to Terrorism; Media Facilitation; Public Affairs Operations; Media Relations; Building a Newspaper--Tactics, Techniques and Procedures; Combat Neurosis etc

16. While most of these articles and papers made available by the jihadi web sites were apparently procured from open sources, the origin of some such as the documents purportedly of the CIA was not clear. Were the pro-jihadi Muslim members of the US Armed Forces and security agencies providing some of this

material to the jihadi web sites? One had a strong suspicion, which could be neither proved nor disproved.

17. Nearly one-third of the 150 jihadi websites related to Kashmir. These were run by indigenous Kashmiri organisations such as the Jammu & Kashmir Liberation Front (JKLF), Pakistan-based terrorist organisations such as the Markaz Dawa Al Irshad and its militant wing, the Lashkar-e-Toiba (LET), the Harkat-ul-Mujahideen etc, Western-based Kashmiri organisations such as the Kashmir American Council, the Kashmir Canadian Council etc, Kashmiri activists based abroad such as Ajaz Siraj, moderator of the Kashnet, Dr.Ayub Thakur of the World Kashmir Freedom Movement, Azmat A.Khan, Secretary-General, JKLF,UK/Europe, Bashir Siraj of the Kashmir Forum etc Some Western personalities taking interest in the Kashmir issue such as Lord Avebury of the UK and Ms. Karen Parker of the US had their own sites. Some of the Kashmiri sites seemed to have been constructed and run by a Colorado-based Internet Service Provider with the typical Hindu name of Indra's Net.

18. Amongst other jihadi organisations active in the WWW were those of Chechnya, which maintained their sites in eight different languages, with video/audio coverage of the fighting, scenes from the training camps, interviews with the Mujahideen etc, Kosovo, Indonesia and the Xinjiang province of China. One did not come across any sites of the jihadi organisations of the Central Asian Republics. Interestingly, the Uighur jihadi organisations of Xinjiang seemed to operate as lone wolves, with no links to other jihadi groups. No satisfactory explanation for this was available.

19. The Taliban Government of Afghanistan used to have its own site maintained apparently from Islamabad. After the enforcement of the UN sanctions against the Taliban in November 1999, this disappeared. The site carried a message that due to difficulties in loading and maintaining the site directly from Afghanistan, it had been discontinued. The visitors were advised to read the "Dharb-e-M'umin", an online electronic monthly, for news about Afghanistan, Kashmir and Chechnya.

20. Amongst organisations of West Asia and North Africa having their own sites were the Hamas, the Hizbollah, the Islamic Salvation Front of Algeria etc.

21. Some of the jihadi sites were in the Malaysian language. Surprisingly, one came across very few references to Osama bin Laden in the 150 jihadi websites. There were far more references to the late Abdullah Azzam, a Palestinian who, along with bin Laden, was quite active during the Afghan war and who was mysteriously killed in an explosion in Peshawar in the late 1980s. The complete text of a book on jihad by Azzam was available on the web even in 2000.

22. In a note prepared by me giving my assessment of the sites on February 23, 2000, I had stated as follows: "It would be difficult to estimate the impact of these jihadi web sites on the ground situation in terrorism-affected areas. In regions such as Chechnya, where the Russians don't allow foreign journalists, the web sites definitely become reference points for outside people wanting to have a version different from that of the Russians. One does not know in how many instances, the terrorists were established to have learnt their tradecraft from the web sites. However, it is important for the security agencies to closely monitor the jihadi sites."

23. The period between 9/11 and the US-led invasion and occupation of Iraq in March-April, 2003, saw a mushrooming of jihadi web sites, with organisations suspected or identified as facades for the Al Qaeda and pro-Al Qaeda individuals starting a plethora of them. Since the organisations and individuals behind these web sites had no reasons to take care not to come into conflict with the law, they made no secret of their desire to use their web presence not only to propagate their cause and carry on a campaign against the US and other countries perceived as supporting the US, but also to spread the jihad across national borders by paying homage to suicide terrorists, and by converting the Internet into a virtual madrasa and jihadi training centre. The number has further grown up after the US-led occupation of Iraq. The number of jihadi web sites is estimated to have increased from about 150 in February 2000, to about 4,000 today.

24. The military operations by the US-led coalition in Afghanistan after 9/11 not only deprived the Al Qaeda and other jihadi organisations associated with it of their training infrastructure, but it also damaged the ability of their leadership to personally interact with their cadres and motivate them. The scattered remnants of the Al Qaeda and other jihadi organisations found themselves forced to split into small groups and take shelter in different places in Pakistan as well as in other countries such as Iran, Bangladesh, Yemen etc. The post-9/11 security measures made travel to other countries difficult, thereby drastically reducing the possibility of personal meetings. This period also saw the emergence of the phenomenon of free-lance jihadis----- individual Muslims angered by the actions of the US and other Western countries in Afghanistan and Iraq waging an individual jihad, either alone or in association with like-minded co-religionists, without necessarily belonging to the Al Qaeda and other members-organisations of the IIF. The free-lance jihadis also made their presence felt in the WWW.

25. As these scattered small groups, at their initiative without necessarily any directions or guidance from a central leadership, planned and executed jihadi terrorist strikes in different parts of the world, they started depending on the Internet more and more for keeping up the motivation of their cadres and for sharing their knowledge and expertise in matters such as fabricating explosives from commonly available materials, assembling an IED, use of modern innovations in science and technology for the commission of acts of terrorism etc.

26. The web sites consequently became the main tool not only for the propagation of their cause, Psywar against their adversaries, the collection of funds and the motivation of their supporters, but also for the dissemination of knowledge and instructions on the techniques of reprisal against their adversaries. A telling example of such dissemination of knowledge is about the use of mobile telephones for triggering IEDs. It was through the Internet that lessons on this subject were spread across the world so that today one finds widely scattered jihadi terrorist groups, which had not come into contact with each other post-9/11 and which did not have the benefit of any formal training, successfully using the mobile phones as a trigger in different areas such as Casablanca, Madrid, southern Thailand and so on.

27. While there has thus been a remarkable growth in the number of web sites operated by pan-Islamic jihadi terrorist organisations, a similar growth has not been witnessed in the web presence of indigenous terrorist organisations--- whether they

are ethnic, ideological or religious. The WWW is today largely dominated by pan-Islamic jihadi terrorist organisations, which have pushed other terrorist organisations to the background. Moreover, since the leaders of the indigenous jihadi terrorist organisations do not face difficulty in traveling clandestinely within the territory of the country in which they are operating to brief and motivate their cadres through personal meetings, they do not have the same operational dependence on their web presence as the pan-Islamic, trans-national jihadi terrorist organisations.

28. The pan-Islamic jihadi terrorist organisations are aware that the Internet is a double-edged weapon. While it facilitates their trans-national networking and operations, the Internet also makes them vulnerable to detection by the intelligence and counter-terrorism agencies. They, therefore, avoid the use of their web sites for the dissemination of any knowledge regarding their future operational plans and any information, which might enable the agencies to determine the identities of their followers and their whereabouts. Their net-centric warfare is more strategic than tactical, more general objectives oriented than specific operations oriented.

29. Those operating these web sites are also increasingly adept in Internet-specific evasive techniques such as frequently changing their location in order to add to the difficulties of the agencies in monitoring them, exploiting other legitimate web sites as safe haven for concealing their web presence etc..

30. What has been the impact of the growing web presence of the international jihadi terrorist organisations on their operations? Firstly, they have been able to add to the anger against the US, Israel and other countries supporting the US through the skillful use of video and audio clips of atrocities allegedly committed against the Muslims in Afghanistan and Iraq. This anger has strengthened the motivation of their own cadres and motivated many other Muslims in different parts of the world to take to free-lance jihadi terrorism.

31. Secondly, they have been able to create or aggravate feelings of alienation amongst the Muslims of countries, which have been supporting the US. Thirdly, they have been trying to intimidate some States and individuals presently co-operating with the US to stop doing so through methods such as the kidnapping and murder of their nationals and publicising their acts through the Internet. .

32. Fourthly, they have been able to propagate their cause in the Islamic Ummah and in the Muslim Diaspora in Western countries and widen the base of support for their jihad against the US. Fifthly, they have been able to disseminate knowledge and expertise in the techniques of carrying out acts of jihadi terrorism.

33. And sixthly, they have been able to bring about an apparently inexhaustible flow of volunteers for suicide missions in Iraq through their skillful motivational techniques using video and audio clips of the atrocities allegedly inflicted on the Sunni Muslims.

34. However, there is so far no evidence to show that their web presence has contributed to the success of any specific operation. It is difficult to assess and quantify the extent of fund flows to them through the Internet.

COMMUNICATION

35. Till the early 1990s, couriers and landline telephones were the preferred means of communication of all terrorist organisations---ethnic, ideological or religious. They then started using mobile and satellite telephones. They have been increasingly using the Internet for their communications since 1995. Their use of the Internet is through the E-mail, Messenger Services, Message Boards and Chat Rooms.

36. Personal couriers were the safest means of communications unless the couriers were intercepted and interrogated by the security agencies. Telephones are quite vulnerable and communications through them could be easily intercepted unless the terrorists use scramblers. The success of the Indian counter-terrorism agencies against the Sikh terrorist organisations in the Punjab in the 1990s was made possible by the frequent use of the landline telephone by the terrorists.

37. Different terrorist organisations started using satellite and mobile telephones from the early 1990s. The mobile telephone calls posed some difficulty for the technical intelligence agencies, particularly in determining where the persons making and receiving the calls were located. This was particularly so if the terrorists used stolen mobiles or used the mobiles while moving around and not from a stationary position. The widespread use of the mobiles by the terrorists in Karachi in 1995 forced the Government of Mrs. Benazir Bhutto, the then Prime Minister of Pakistan, to ban the use of mobiles. This forced the terrorists to go back to the use of landline telephones. This enabled the agencies to capture or kill a number of terrorists by intercepting their telephone calls and pinpointing their location. A way out of the difficulties posed by frequency hopping and mobile telephones has since been found by the security agencies. It is understood that the arrest of a number of operatives of the Al Qaeda in Pakistan after 9/11 was made possible by their unwise use of satellite or mobile phones and the success of the US intelligence agencies in intercepting their conversations and in pinpointing their location.

38. E-mails are a safer means of communications than telephones and the terrorists have become adept in frustrating the efforts of the intelligence agencies to intercept the E-mail and identify the sender and receiver through evasive techniques such as one-time E-mail address, one-time Internet cafes etc. Different E-Mail addresses and different Internet cafes are used for each operational message.

39. Interception of E-mails poses certain special problems. Whereas a telephone conversation can be intercepted even while the conversation is in progress and the location of the terrorist making the call determined with a fair measure of accuracy. E-mails can be intercepted only after the terrorist has typed the message and sent it. Instantaneous interception of a suspect E-mail and successful follow-up action on it is more an exception than the rule. By the time an intelligence agency intercepts an E-mail, analyses it and determines from which Internet cafe it was sent, it would have become too late and successful identification and arrest of the suspect becomes very difficult.

40. To ensure that even a single interception does not damage their operations, the terrorists have been using encryption techniques. The most primitive, but the

most effective encryption technique is the use of domestic codes in messages. A domestic code is a set of pre-determined meanings for certain words and phrases used in a message. The message, when intercepted, appears enclair, but the words and phrases used have a meaning different from what they seem to be. It is virtually impossible to break a domestic code unless one has a human source in the targeted terrorist organisation who knows what the key words and phrases in the message actually mean.

41. It is believed that Mohammad Atta and his associates, who carried out the 9/11 terrorist strikes in the US, often, if not always, used domestic codes for their communications among themselves and with Khalid Sheikh Mohammad (KSM) in Karachi and with Osama bin Laden in Kandahar. Unless one knows the identity of the sender as a terrorist, one would not suspect the messages sent by him as having anything to do with a terrorist operation. To be able to use domestic codes effectively, periodic personal meetings are necessary. The post-9/11 security measures by making travels for terrorists difficult have reduced the chances of personal meetings and thereby affected to some extent their ability to use domestic codes.

42. However, after 9/11, barring Iraq, there has hardly been any jihadi terrorist strike in which the perpetrators came from outside. Many, if not most, of those, who participated in the jihadi terrorist strikes at Bali, Mombassa, Casablanca, Istanbul, Madrid and London were locals, who would have been able to communicate among themselves in domestic codes without any major difficulty.

43. In other cases, to overcome the difficulties and to protect themselves against interception of their messages, the jihadi terrorists have been increasingly using commercially available encryption keys. To be able to break them, the intelligence agencies would need a large number of sample messages originated by the same organisation or individual using the same keys. This is quite difficult and this should explain why intelligence agencies fail to detect preparations for specific terrorist strikes.

44. In the case of the international jihadi terrorists, inadequate knowledge of their language and inadequate understanding of the allusions to the Holy Koran made by them in their messages add to the difficulties faced by the intelligence agencies in making effective use of the intercepts of their E-Mails. Intelligence professionals would know how difficult it is to pinpoint suspect telephone conversations in the English language and examine those intercepted by them. To make their task manageable, they use special software containing key words and phrases through which one could technically separate suspect messages from innocent ones. Even then, there is often a time-gap between the interception of a message and its examination and follow-up action.

45. Such difficulties are considerably magnified in the case of E-mail messages, which are in millions, if not billions, and particularly when a foreign language is used. Not infrequently, the foreign language itself becomes a kind of a domestic code.

46. The case relating to the kidnapping and murder of Daniel Pearl, the US journalist based in Mumbai (Bombay), India, by jihadi terrorists based in Karachi, Pakistan, in

the beginning of 2002 provides an interesting example of the use of the E-mail services by the terrorists for their operations and the difficulties faced by the intelligence agencies in tracking them. Pearl had heard that the final instruction to Richard Reid, the shoe bomber based in Paris, to embark on his terrorist mission came from someone in Karachi through an E-mail. Pearl wanted to establish the identity of the individual in Karachi, who sent this message, and his organisational linkages. He made his preparations for his visit to Karachi from Mumbai through E-mails exchanged with known and unknown people in Pakistan.

47. Pearl was keen to meet Mubarik Shah Gilani, the leader of a Pakistan-based organisation called Jamaat-ul-Furqa (JUF), which had a large number of members in the Afro-American community in the US and in the Caribbean. He entered into E-mail correspondence with a number of persons in Pakistan in order to seek their help for arranging an interview with Gilani. One day, an individual, who claimed to know Gilani, sent him an E-mail offering to arrange the interview and asked him to come to a Karachi hotel for the initial meeting.

48. Without knowing about the real identity of this individual, Pearl agreed to come for the meeting and landed himself in a terrorist trap, which led to his kidnapping and murder. After the kidnapping, the terrorists involved in the plot were exchanging many E-mails among themselves, with the media and others relating to the conditions for the release of Pearl. Through a study of these messages and other enquiries, the Pakistani intelligence agencies were ultimately able to establish the identities of the perpetrators and arrest them, but they could not establish where Pearl was kept hostage and rescue him before he was murdered.

49. The use of Messenger Services, Message Boards and Chat Rooms by the terrorists to discuss their plans and to convey instructions poses similar difficulties to the intelligence agencies in their collection of Technical Intelligence (TECHINT). This should explain why there have been very few confirmed instances of specific terrorist operations being thwarted and terrorists arrested through timely interceptions on the Internet.

50. Intelligence agencies monitoring the use of the Internet by the terrorist groups are often able to pick up general intelligence of the likely or planned targets of the terrorists and not details of their specific plans. Thus, through the Internet chatter, the intelligence agencies had assessed that Spain and the UK were the likely next targets, but they were unable to collect specific intelligence about when, where and how the terrorists would carry out the strikes.

51. The terrorists also use the Internet for commercial purposes under cover names for augmenting their funds and for the procurement of arms and ammunition. The LTTE, for example, regularly uses the Internet for communications relating to its commercial fleet of ships and for remaining in touch with its arms procurement networks in Thailand, East Europe and other places. It was reported to have procured a microlite aircraft through the Internet.

52. It is not possible to prevent the terrorists from using the Internet for communication purposes, but it should be possible to intercept their messages and chats, break the codes used by them and collect timely preventive intelligence. In

view of the millions, if not billions, of messages in different languages passing through the Internet, identifying suspect messages in this traffic, decoding them, translating them if they are not in English, understanding their significance and implications and taking effective follow-up action is a phenomenal task.

53. Such a task requires human and material resources, powerful super computers, linguistic competence and a large database built up with the help of intercepts broken in the past. Very few countries can mobilise such multi-dimensional resources. When the jihadi terrorists are increasingly becoming global in their thinking, planning and execution of their operations, national technical capabilities alone, however good, would not help in countering them. There has to be an international networking of the national capabilities, which is superior to the network of the terrorists. Such an international networking of national capabilities is yet to emerge.

DATA MINING

54. Not much elaboration is required regarding the terrorists' use of the Internet for data mining. This refers to the collection of data for propaganda, PSYWAR and operational purposes. The trend towards greater transparency in the working of Governments and the private sector, the mushrooming of online journals and the availability of the print media, specialised journals and research products of think tanks etc on the Internet place at the disposal of the terrorists a large volume of essential/useful data, to which they might not otherwise have access. The kind of data, which the terrorists can now get with the help of the Internet search engines, is as follows:

- Details regarding sensitive infrastructure such as the location etc of sensitive Government offices, banks and other financial institutions, stock exchanges, power stations, nuclear establishments, airports, railway stations, traffic choke-points etc
- Reports of parliamentary and Congressional proceedings.
- Details of parliamentary and other enquiries into the functioning of intelligence and security agencies, which often highlight their deficiencies.
- Case studies of important terrorist incidents giving details of how the terrorists operated.
- Case studies of the successes and failures of the counter-terrorism agencies.
- Testimonies given by intelligence and security managers before parliamentary and congressional hearings.
- Articles on arms, ammunition, different kinds of explosives, weapons of mass destruction material etc
- Articles on the counter-terrorism methods of the intelligence and security agencies.
- Articles on the threat and vulnerability perception of the security agencies etc etc

55. A careful collection of the relevant material from the Internet would facilitate the commission of terrorism by placing at the hands of terrorists considerable material, which they would require for a successful strike. Before the advent of the Internet, the terrorists had to spend a lot of money and time to case their targets through spot visits and enquiries. Now, much of the preliminary work could be done through the

Internet. Their knowledge of the working of intelligence and security agencies and their weak and strong points has improved and copy cat terrorism has become easier.

56. How to counter this and deny the terrorists the information they need? The answer lies not in reversing the process of greater transparency, but in carefully monitored and controlled transparency in order to exclude from the Internet information, which might not otherwise be available to the terrorists and which could directly facilitate commission of acts of terrorism. There is now a greater awareness of the need for this all over the world.

CYBER WARFARE

57. Cyber warfare essentially refers to the techniques of massive disruptions in the economy and the critical infrastructure of the adversary and denying to the adversary the ability to effectively use the Internet for operational purposes, such as waging a conventional or unconventional warfare. As the world, its economy and infrastructure become more and more Internet dependent and driven, they become more and more vulnerable to catastrophic acts of mass disruption not only by States and non-State actors such as terrorists, trans-national crime syndicates etc, but also by lone-wolf cyber warriors, working either independently, or in tandem with other lone-wolf warriors or at the instance of States or non-State actors. Cyber warfare provides the means of conducting covert actions such as sabotage, subversion, mass disruption etc without having to physically cross borders or travel.

58. While many States are believed to be acquiring a capability for waging a cyber warfare, evidence is still lacking as to whether the terrorist organisations too have been doing so. The terrorists have definitely acquired a capability for disfiguring the web sites of their adversaries. There have been innumerable instances of terrorists doing so. Are they also trying to acquire a capability for mass disruption operations through the Internet against economic and other critical infrastructure? The evidence regarding this is still incomplete and weak.

59. Much has been written and discussed on the dangers of cyber warfare by terrorists, involving mass disruption covert actions against their adversary States. The debate on this subject is based on perceptions of vulnerabilities than on those of real threats. However, intelligence and counter-terrorism agencies cannot afford to overlook this possibility while developing their capabilities in the field of net-centric counter-terrorism.

OTHER ASPECTS

60. Since 9/11, the jihadi terrorists have been increasingly using the cyber space for some of their activities. The remarkable manner in which they have built up their cyber capabilities speak of the availability to them of a fairly large reservoir of information technology (IT) proficient volunteers who are prepared to place their services at their disposal for operational purposes. One is already aware of some IT experts whom they had in their ranks and who helped them in this field. Prominent amongst them were Abu Zubaidah, a Palestinian, who was arrested at Faisalabad in Pakistani Punjab in March 2002 and handed over to the US authorities and Mohd.Naeem Noor Khan, of Pakistani origin, who was arrested at Lahore in August,

2004. At the time of the arrest of Abu Zubaidah, sections of the Pakistani media had reported that he had done a course in computer technology at Pune, India, before crossing over into Pakistan and joining the Al Qaeda.

61. Many madrasas in Pakistan---some on their own and others at the prodding of the State---have been teaching IT to their students from different countries in addition to lessons in religion and the techniques of waging jihad. While the aim of the State in pressurising the madrasas to include IT in the syllabus is to provide the students with legitimate means of livelihood after they come out of the madrasas in order to wean them away from terrorism, many of these IT-trained and religiously-motivated students add to the reservoir of IT-proficient volunteers available to the Al Qaeda and the IIF.

62. There is reason to believe that in addition to these, there are many lone-wolf Muslim cyber professionals living all over the world who have been assisting the jihadi terrorists in the cyber space. As a result of this, the international jihadi terrorists have never been in short of competent cyber professionals, who either act at the instance of the Al Qaeda and the IIF or on their own in the pursuit of common objectives.

63. While their increasing web presence has enabled the jihadi terrorists and their objective allies in the community of free-lance jihadis and lone-wolf cyber activists to promote and strengthen feelings of Islamic solidarity and to give a push to the trend towards the monolithisation of the community, though this objective is still far away, its actual contribution to the success of specific acts of terrorism is difficult to quantify. However, their ability to communicate with each other through the Internet without their planned operations being detected by the intelligence agencies has definitely been an important factor in some of their successful terrorist strikes.

64. Terrorist organisations cannot be defeated in the military sense. They can only be made to wither away by repeatedly denying them success, by diluting the motivation of their cadres and by drying up the flow of volunteers and funds. An important component of cyber counter-terrorism is, therefore, devising ways of denying them success in the cyber space. The international community is nowhere near achieving it.

65. Most of what the intelligence agencies know about the web network of the jihadi terrorist organisations seems to be based on their observations in the web space and the interrogation of arrested terrorists. Inadequate human intelligence (HUMINT), which is one of the serious deficiencies of the counter-terrorism agencies of the world, comes in the way of their being able to penetrate the web network of the jihadi terrorists too. Penetration through human sources would enable them to break through their secret communications. In the absence of penetration, which could provide them inside information about the kind of encryption used, how and when it is changed etc, code breaking becomes time-consuming and often a matter of luck.

NET-CENTRIC COUNTER-TERRORISM

65. Neither prevention nor pre-emption is possible in cyber-space. Only effective countering can deny the terrorists the advantages presently enjoyed by them. Countering their innumerable web sites by suppressing them would be counter-

productive. The web sites run by the jihadi organisations and their associates are a valuable source of open information regarding the terrorists. There would be no point in suppressing them. What needs to be suppressed are those pages or sections of their web sites, which disseminate information about how to commit an act of terrorism. An effective counter to their use of the web for propaganda and PSYWAR purposes is not by suppressing them, but by the State developing better means of dissemination of information and a better PSYWAR capability in order to discredit the terrorist organisations and wean their followers away from them.

66. The most important component of net-centric counter-terrorism is the capability to monitor/intercept their communications through the Internet, to break their codes and take timely action on the intelligence thus collected. Very few countries in the world presently have the human, financial and technical resources required for this. It would be very difficult to undertake this task through national capabilities alone. While there has been an increase in international co-operation by way of intelligence sharing, there is very little co-operation by way of technology sharing.

67. Technology, which could facilitate better countering of the web presence of any entity, is a dual-target one. What can assist in countering the web presence of non-State actors would be equally helpful against States. Hence, the reluctance to share this technology. The scope for co-operation would, therefore, continue to be limited. The post-9/11 period has seen greater bilateral and multilateral co-operation in cyber security, but this is presently restricted to sharing of training facilities and transfer of low-tech expertise. Every country, faced with threats from international jihadi terrorists and other terrorist organisations, has to invest considerable resources, time and effort in developing a national capability for Internet communication penetration.

68. The Internet provides a means of penetrating terrorist organisations through human moles by taking advantage of their online recruiting. This is an area of intelligence exploration, which deserves better attention than it has received so far.

69. The objective of counter-data mining has already been touched upon above. As regards, cyber warfare, the fact that the terrorists have not so far made any attempt in this direction. Should not give rise to any complacency that they are unlikely to do so in future too. This is an area of serious vulnerability, which should continue to receive the required attention.

(The writer is Additional Secretary (retd), Cabinet Secretariat, Govt. of India, and, presently, Director, Institute For Topical Studies, Chennai, and Distinguished Fellow, International Terrorism Watch Programme, Observer Research Foundation, (ORF), and Convenor of its Chennai Chapter. E-mail: itschen36@gmail.com)

<http://www.saag.org/papers16/paper1584.html>