Exploitation of Information and Communication Technology by Terrorist Organisations

Shitanshu Mishra

Abstract

Almost every new technology developed has brought great benefits attached with some risks. To each 'technology', there is an 'anti-technology', making it a double edged weapon. But whatever be the risks, the progress just carries on, and new methods are found to tackle the risks. The phenomenal growth of computer and communication technologies, or ICT, is no exception and the main risk it has brought along with its benefits is that it has provided terrorist organisations great advantage in their nefarious activities. The ICT has also greatly facilitated cultural invasions, resulting in real or imagined resentments and revulsions, which are one of the causes of international terrorism.

ICT is exploited by the terrorist organisations in two ways—as a tool and as a target of attack. Used as a tool, communications are used in support of their operations providing for control of all their activities. Terrorists can also operate in cyber space to destroy or manipulate information for their own purpose. There are numerous known cases of exploitation of ICT by the terrorist organizations, both, globally as well as in India.

This paper aims to study the past patterns of exploitation of ICT by domestic and international terrorists to predict the future eventualities so that they can adopt preventive measures in a pro-active manner. Subsequent studies under the same project will focus on the counter-measures in a more detailed manner.

Introduction

There are certain truisms about terrorism, such as "Terrorism is a weapon of weak", and " Terrorists want a lot of people watching, not a lot of people

Strategic Analysis, Vol. 27, No. 3, Jul-Sep 2003

Revised paper received on September 5, 2003

dead". Communication scholars, however, conceptualise modern terrorism within the framework of symbolic communication theory. P. Kraber states that " as a symbolic act, terrorism can be analysed much like other media of communication, consisting of four basic components: transmitter (the terrorist), intended recipient or receiver (target), message (bombing, ambush) and feedback (reaction of target audience)".[1] Thus, modern terrorism may be construed as an attempt to communicate messages through the use of orchestrated violence.[2]

The concept of warfare has always changed with the times. More often than not, international terrorism is the use of terrorist violence against a given nation by another state (or a loose conglomeration of states), which uses the terrorists to fight a proxy war as an alternative to conventional war. Such support provides for professional training and equipment for covert operations by the terrorists, diplomatic cover and other logistic aid, besides continuous flow of funds and ensures a safe haven to which the terrorists can escape and emerge anew. Information and Communication Technologies (ICT) have become an important weapon of this warfare, whether it is for command and control of such operations, or for logistic support.

Cyber Space: The term Cyber Space has come to acquire a meaning which encompasses all forms of computer-mediated communications. Even the plain old telephone systems (POTS), which have now been digitised, fall within the ambit of cyber space. Broadly speaking, the cyber space has following components[3]:

- Digital computers (ranging from laptops or palmtops to expert systems).
- Voice, fax, telex, video and other forms of communication systems.
- Digitally operated transportation systems, such as cars, trains, aeroplanes, elevators, etc. These can be remotely monitored or controlled over a network.
- Digital control systems, such as are applied in chemical processes, health care or energy provision.
- Digitally-operated appliances such as watches, microwave ovens, digital cameras and video recorders. The Blue tooth technology, which is now a reality, would allow such systems to be connected to the internet and act 'intelligent'.
- Robots that independently run automated systems.

- High tech weapon systems, missiles, Global Positioning System (GPS), Space vehicles and satellites, etc.
- Communication technologies that include switching systems, broadcasting, various audio-visual devices, local area networks (LANs), cellular/WLL phones, modems, satellite systems, laser/ microwave/ HF/VHF/UHF radio systems, optical fibre and other cable systems.

The digital world is moving to the era of convergence, where all types of information, be it voice, text or video images, travel over the same media and are processed accordingly. The ICT is marked by miniaturisation and larger capacity packaging, enabling storage and passage of large volumes of information in real time over large distances. The satellite systems and high capacity optical fiber cables (OFC) have come to play a big role in this, allowing worldwide reach to anyone and everyone who can pay for it. The ICTs have also greatly facilitated cultural invasions, resulting in real or imagined resentments and revulsions, which are one of the causes of international terrorism.

Terrorism: Components and Inter-linkages

The WTC attacks on September 11, 2001 as also the subsequent attack on Indian Parliament on December 13, the same year are evidence that the international terrorists have organised themselves in a manner of a large multinational conglomerate. Lengthy preparatory phases preceded several of the more devastating attacks during the past decade. A typical global/trans-national terrorist attack consists of a year-long preparatory phase, a very brief crisis phase and a long consequence phase. During these phases, new capabilities are developed, operatives are recruited and trained, resources are positioned, and the attack is researched and planned.[4] It is for this reason that the Security Agencies or the law enforcing agencies more often than not, are taken by surprise, and are found to be only reacting to the actions of the terrorists. In order to be able to act in a pro-active manner, it is essential to visualise and identify various components of terrorists' networks and their inter-connectivities.

The 'T' Chakra

The wheel of terrorism or the 'T' Chakra, has a strong and charismatic leadership- either a single individual or a group- at its core, with a number of spokes which add strength to it and make it roll with full speed. To be able to

put brakes to it, one must first understand these strength members (Fig-1). A brief description of these, referenced from the web site of the Terrorism Research Center[5] is given below:

- *Organisation:* Terrorists organize themselves to function in the environment where they have to carry out their acts. Organisational details are situation-specific. Because terrorists must operate in a hostile environment, security is their primary concern, and it is best served by a cellular structure in which members do not know and can not identify more than a few of their colleagues in the event of their capture or defection. Defection is rare in most groups; defectors or even dissidents are frequently killed or maimed.

- *Motivation:* Terrorists are inspired by several motivations, which can be broadly classified into three categories- Rational, Psychological and Cultural motivations. The rational terrorist thinks through his goals and options, making a cost-benefit analysis similar to that of a military commander or a business entrepreneur considering available courses of action. Psychological motivation for terrorism comes from the terrorist's personal dissatisfaction with his life and accomplishments so much so that he finds his raison d'etre in dedicated terrorist actions, and turns into a 'true believer'. There is also a pronounced need to belong to a group. Terrorist groups are characterised by a group dynamics trying to maintain self-esteem and legitimacy. They tend to demand unanimity and become intolerant of any dissent. The groups are prone to fracturing, with the splinter groups more violent than their parent group. Lastly, the cultural motivation is a determinate of perception of 'outsiders' and anticipation of a threat to ethnic group's survival, leading to violence which may seem irrational to an outsider. The perceived threats are to the group values, such as language, religion, group membership, homeland or native territory, deeply held by the members.

- *Recruitment and Training:* Recruitment of terrorist and their training are, predictably, security-sensitive. Among groups that are not ethnic-based, the usual source of recruits are high school and college students who show commitment to the cause. Ethnically based terrorist groups recruit new members personally known to them, people whose backgrounds are known and who often have family ties to the organisation. The training varies considerably. Those with military experience or who have received prolonged training at sophisticated facilities are the equals of most state security forces. On the other end of spectrum are 'throw away' operatives who get little more than inspirational talks before being activated. Typical training includes

instructions in the use of small arms and explosives along with intelligence collection and indoctrination in the group's cause.

- *Weapons, Ammunition and Explosives:* Contemporary terrorist actions include traditional assassinations, bombings, arson, hostage-taking, hijacking, kidnapping, seizure and occupation of a building, attacks on a facility, sabotage, and perpetration of hoaxes. Newer categories of operations include ecological terrorism and still largely potential 'high-tech' terrorism using chemical, biological, radiological and nuclear (CBRN) weapons and materials. The weapons and ammunition for all such operations range from indigenously produced crude items to highly sophisticated ones, mostly smuggled in from across the borders.

- *Targets:* Modern terrorism offers many advantages to its practitioners. By not recognizing innocents, terrorists have an infinite number of targets. They select their target(s) depending upon the target's value in terms of its contribution to the group's goals, its accessibility given group capabilities, and the purpose of the attack, and then determine when, where and how to attack. This gives them a high probability of success with minimum risk.

- *Information (Intelligence) Gathering and Planning:* Often, the terrorist's acts are planned well in advance, and even rehearsed. The sites are reconnoitered and alternates are explored over a period of time. All possible sources are used for collection of information about the likely target(s).

- *Movement of Personnel:* Generally, an operation will involve movement of personnel. This brings up the need for passports, valid visa, driving licenses, etc., in case of a trans-border move, as also the requirements of passenger tickets, local public transport or hired vehicles to reach the site and for get away, and other associated logistics. Most of the official documents are forged using computers.

- *Bases and Hideouts:* Both, prior to an operation as also subsequent to it, the terrorists need safe sanctuaries, not only for hiding themselves, but also for their equipment and weapons, etc. They normally seek a place which is not conspicuous, and provides them with the required degree of privacy so that they can carry out their planning and preparations without raising any suspicion.

- *Support Structure*: Terrorist groups that are not supported by a government usually create a support structure of their own sympathizers and people who have been coerced into helping them. The support structure may comprise of active and passive members who furnish the active terrorists

with logistic support, intelligence, dissemination of propaganda, recruiting and money. There are 'sleeper' agents too, who hibernate for a long time, living as normal peace-loving and law-abiding citizens, and are activated when the real need arises through a coded signal or message through other agents.

- *Publicity:* The terrorists need to publicize their attacks, in order to generate fear. The need for publicity often drives target selection and the timing of the attacks. Hence unlike criminals, the terrorists usually claim a responsibility for their actions and are in direct or indirect contact with the media representatives.

- *Finances:* No terrorist organisation can survive without the financial back up. This comes from varied sources. The domestic terrorism is mostly supported by contributions/extortion from local populace as also from criminal activities such as looting and kidnappings. The international brand of terrorism, however has a wider network of support from some State governments, a diaspora of sympathisers, certain religious or charitable institutions supporting the cause of the organisation, as also from mafia groups, drug cartels, etc. Funds are also generated through underworld activities such as counterfeiting currencies, contract killings, kidnappings, extortions and smuggling of goods and human beings. Maximum support, however stems from narcotics business[6]. The flow of funds has many channels, including the infamous hawala. Legal and illegal banking transactions are not unknown for such support. E banking has further facilitated such transactions.

- *Command and Control:* The terrorist organisations usually activities have a well-defined command and control system in place with due considerations to maintaining their security and the principle of 'need to know'. This provides the inter-linkages between all the spokes of the 'T' Chakra. Communications play a very important role in this. Breaking this important linkage would help the governments in countering the terror menace with a very high degree of success.

However, at the same time it is important to note that in a democracy, terrorism finds less hurdles for growth. Yet, control of terrorism in democracies should not be at the cost of democratic freedom and rights. Denying the technology to the people fearing that it would be misused by the terrorists, would be counter-productive.

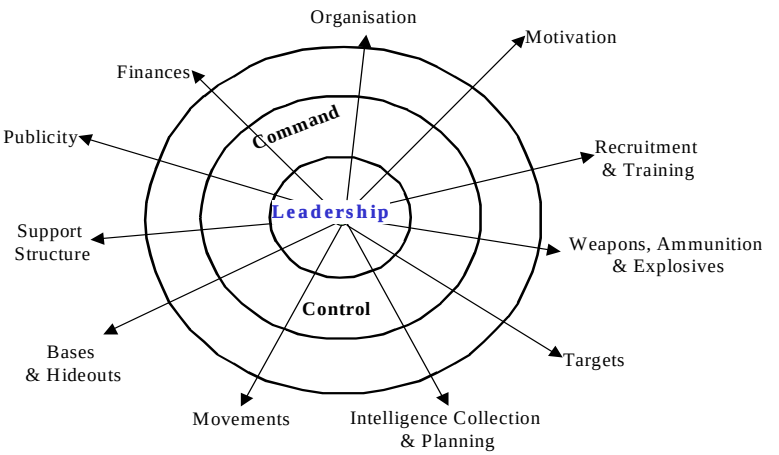


Fig-1: The 'T' Chakra

Exploitation of ICT by Terrorists

ICT is exploited by the terrorist organizations in two ways—as a tool and as a target of attack. As a tool, communications are used in support of their operations providing for control of all their activities. Terrorists can also operate in cyber space to destroy or manipulate information for their own purpose. Skilled hackers with terrorist intent can access all but the most secure databanks, stealing or changing information, or destroying it. The targets of terrorists could be ranging from financial institutions to nuclear installations, besides the civil and military communication systems. There are numerous known cases of exploitation of ICT by the terrorist organisations, both, globally as well as within India. These generally pertain to the following:-

- Communications, for command and control, issue of instructions/ orders/directions, etc.
- Perception management.
- Intelligence gathering.
- Financing support operations.
- Cyber attacks.

The future, however, is beset with many unforeseen possibilities. It will be worthwhile to study the past patterns to predict the future eventualities so as to be able to adopt preventive measures in a pro-active manner.

Criminal Terrorist Activities

May 1997, Columbia: In a hangar west of Bogota, Columbian police and Drug Enforcement Administration (DEA) agents uncovered a tele-communications station containing at least $ 10 million worth of hi-tech material including signal scanning equipment to intercept phone calls, fax messages and ATC operations.. Established by the drug lord Efrain 'Don Efra' Hernandez, murdered in 1996, the station enabled all the cartels, on a time sharing basis, to maintain constant satellite contacts with their fleets of aircrafts or boats (on the high seas and high in the skies), and with their representatives throughout the world[7]. DEA also discovered drug laden Columbian jets that had been outfitted with air to air signal interceptors to monitor the routes of US military jets flying over the Gulf of Mexico and Caribbean Sea [8].

Before the 1998 peace agreement, the Irish Republican Army was said to have developed a sophisticated computerized intelligence bank using databases in the Irish Republic, America and France. A sympathiser employed by British Telecom stole telephone billing records in order to determine the addresses of potential murder targets. The IRA also sifted through customer databases maintained by the private health care company BUPA and Thomas Cook's travel agents. The high-tech intelligence network was uncovered after authorities seized a batch of computer disks in Belfast. The disks contained copies of the electoral register, which was used to find the names of police officers and other potential targets. The IRA used encryption to conceal their files, but the officers were able to decrypt the disks after months of efforts[9].

In what some US intelligence authorities characterize as the first known attack by terrorists against a country's computer systems, ethnic Tamil guerillas were said to have swamped Sri Lankan embassies with thousands of electronic mail messages. The messages read, "We are the Internet Black Tigers and we are doing this to disrupt your communications. An offshoot of the Liberation Tigers of Tamil Eelam (LTTE) was responsible for this incident [10].

Dutch organized crime offers an interesting case study in the use of Information Warfare (IW). The gangsters have their own IW division that combines muscles, brains, know-how, guts and money to achieve their goals. The division works for anyone willing to pay them. They work in cell structures, loosely coupled and hard to get. The Amsterdam police faced severe IW attacks when investigating two major drug organizations, known as the cases of

"Charles Z", and "De Hackelaar". The criminals were found tapping the phone lines of safe houses and the homes of high police officials. They broke the analog encryption used by many Dutch government services. They built receivers to monitor nation wide pager networks. Intercepted information was fed into a database, where it was further processed to determine, for example, which special units were cooperating with one another. The criminals burglarized the houses of the district attorney (DA) and police officers. They spread rumours to discredit DA and the investigation. They stole PCs and diskettes publishing their contents during the trials. In short, everything was done to obstruct justice and the trials although some were convicted anyway[11].

One of the dark sides of open source media is that they are equally available to the criminals, terrorists and other enemies who may use them to find 'how to' guides for building bombs, making chemical and biological weapons, and computer hacking. One website was said to have offered, with the aid of graphics, 218 ways to make a bomb, including tennis ball bomb, napalm bombs, letter bomb, underwater bomb, smoke bombs, cigarette pack bomb, etc. A variety of hacking tools can be downloaded from the web including manuals for breaking into computer systems, evading detection, stealing phone service, listening in on phone calls, and cracking locks, along with the programs and command scripts[12].

Inoue, a 25 year old chief of Ministry of Intelligence of Aum Shinrikyo cult, which was responsible for the Sarin gas killings in Tokyo's subway train in March 1995, had copied information from NEC Laser Research Laboratory on laser beam amplification. From the home of an employee of Nippon Oil and Fats company, which made rocket fuels for Japan's Space programme, they stole documents in their efforts to develop chemical and biological weapons of mass destruction (WMD). They were on the road to develop nuclear capability, and had tried but failed, to buy a laser gun from USA[13].

Encryption has been encountered in major criminal and terrorist investigations, including that of Aum Shinrikyo[14]. Other terrorist groups have used encryption as a defensive tool. Ramzi Yousef, the mastermind behind the 1994 World Trade Center bombing and 1995 bombing of a Manila Airliner, encrypted files stored on his laptop PC. When authorities seized his computer in Manila and decrypted the files, they found information pertaining to further plans to blow up 11 US-owned commercial airliners in the Far East [15].

The chief architect of the 11 September attack on World Trade Center towers, Osama Bin Laden is known to have build a vast empire of terrorist network. Despite being stuck in a country without roads, let alone telephones, he was powerful because of modern communications, using it in every possible manner for command and control, intelligence and perception management. In the past, bin Laden had been known to utilize high-technology in his communications with his associates, including satellite communications and cellular phones, but after the American missile attacks in August 1998, which were pointed onto him based on satellite telephone tracking, and very narrowly missed him, he became careful and avoided using the same himself. *The Aviation Week & Space Technology* has reported that Al Qaida uses secure links to track US troops in combat, even now. [16] It states that the commander who controlled Al Qaida's reaction to 'Operation Anaconda' earlier in 2002, causing dozens of US casualties, was a veteran of the fighting against Soviet Union. He simultaneously used at least five radio operators and communication channels, each involving one or more languages for each ethnic group involved (Arab, Pakistani, Uzbek, Afghan, etc.). The wireless telephones, (the best equipment money can buy, according to US intelligence officials), tied the observer corps(some of whom also monitor aircraft flying out of allied bases) to the Al Qaida and Taliban combat forces and the overall tactical commander. The system was efficient enough so that Al Qaida had a 48-hour warning of Operation Anaconda, said the Special Operations member.

The Times of India, quoting AFP, reported that the Bali bombers massacred their victims using mobile phone technology. Police in Jakarta said that a Mitsubishi van packed with explosives stopped briefly in front of the Sari nightclub on October 12, 2002, before it exploded with the help of a cellular phone, killing 190 people, almost half of them Australians. Ironically, the report also stated that the same technology was probably responsible for the arrest of Imam Samudra, the mastermind of the plot.[17]

Earlier, in another report, it was brought out that Islamic militants, who did not identify themselves, but said that they were mujahideens who support Al Qaida, had warned of an attack in Kenya on internet chat rooms, one week prior to the actual attacks on Israeli Paradise hotel in Mombassa.[18]

ICT for Perception Management

Radio, television and now internet, with their much wider reach than the word of mouth or the print media, offer the best means of publicising views

and opinions of any organisation. With the availability of satellite media, all electronic broadcasts can have a global coverage, without any constraints on geographic location of the transmitting station, as was the case in the past. The convergence of voice, imagery, video and text has further facilitated the propagandists in creating impressions on the mind, which may not be entirely based on truth.

FARC (Fuerzas Armadas de Columbia or Armed Revolutionary Force of Columbia), the well known terrorist organisation, for example, broadcasts "La Voz de La Resistentia", (The Voice of resistance). "The Voice of Sudan", run by the anti-Khartoum National Democratic Alliance is heard from 4.00 AM to 6.00 AM GMT and again from 4.00 to 6.00 PM GMT daily on 8000, 9025, 10000 and 12000 or 12008 kHz. The "Voice of the Sudan Alliance Forces", also known as the "Voice of Popular Armed Uprisings", can be heard in Arabic from 4.00 to 5.00 AM and from 4.00 to 5.00 PM at 7000 kHz.[19]

Al Jazeera TV has acquired its popularity, especially in the Arab world, due to its access to Al Qaida operatives, including Osama bin Laden. Laden has been repeatedly appearing on the TV (through pre recorded video cassettes), issuing new threats.[20]

Al Qaida is also known to maintain certain websites on internet. One of these, the Arabic language website http://www.mojahedoon.net, announced in December 2002, the formation of a new Al Qaida branch, the Islamic Al Qaida Organisation in Palestine, which said it would work to undermine any talks between Israel and Palestine authorities, as reported by the Washington Post. The site also called for a close cooperation between the Palestine authorities and Hamas.[21] Terrorists have become so confident that they sponsor websites to solicit funds from supporters worldwide. As per Los Angeles Times, two such internet-savvy groups, Pakistan-based Harkat Ul Mujahedeen and Lebanon's Hezbollah, have been linked to Bin Laden. Dru C. Gladney has brought out the role being played by Uyghur separatists, in their demand for freedom in China's Xinjiang province. He has termed it as 'Cyber Separatism'. [22]

Yariv Tsfati and Gabriel Weimann, conducted a detailed research on use of internet by modern terrorist organisations and their results are summarised below. [23]

Who Are the Terrorists on the Internet?

The important organisations on the internet include Hamas, the Lebanese Hizbollah, the Egyptian Al Gama'a al Islamiyya, the Popular Front for the Liberation of Palestine(PFLP), the Palestinian Islamic Jihad, the Peruvian Tupak-Amaru (MRTA) and the "Shining Path" (Sendero Luminoso), the Kahane Lives Movement, the Basque ETA Movement, the Irish Republican Army(IRA), "Supreme Truth" (Aum Shinrikyo), the Columbian National Liberation Army (ELN-Columbia), the Liberation Tigers of Tamil Eelam (LTTE), the Armed Revolutionary Force of Columbia (FARC), the Popular Democratic Liberation Front Party in Turkey (DHKP/C), the Kurdish Workers' Party (PKK), the Zapatista National Liberation Army (ELNZ), the Japanese Red Army (JRA), and the Islamic Movement of Uzbekistan (IMU). There are a few more sites which do not have an English version. Except two European sites, all other sites were based in the Third World countries in South America, East Asia and the Middle-East and sponsoring organisations could be characterised as national, revolutionary, and religious movements or a combination of these.

The Contents

The most important content is, expectedly, information about the organisation including its history, leaders, political and ideological goals, etc., as also the latest update on news. The goals are explained either explicitly or indirectly. Almost all the sites avoid presenting and detailing their violent activities; exceptions being Hizbollah and Hamas; Hizbollah shows updated statistical reports of its actions ('daily operations'). The Hamas site contains lengthy discussions in Arabic of military operations in its news and views sections. However, while avoiding the violent aspects of their activities, the Internet terrorists usually stress upon two issues: freedom of expression and political prisoners. The anti-establishment terrorists enjoy representing themselves as the victims, appealing to the democratic values of the Internet users.

The Rhetoric of Terror

Terrorist rhetoric on the internet tries to present a mix of images and arguments in which the terrorists appear as victims forced to turn to violence to achieve their just goals in the face of a brutal, merciless

enemy, devoid of moral restraints. The major arguments for this are: First, that there is 'no choice', second, legitimacy of use of violence due to demon-like behaviour of the enemy; and the third is an attempt to substantiate the claim that terror is the weapon of the weak. Some of the sites are replete with the rhetoric of non-violence, messages of love and peace, and of a non-violent solution, reached through diplomatic or international pressure.

The Target Audiences

The sites attempt to address their potential supporters, their enemies (including the opposing sociopolitical community in the conflict) as also the international public opinion. The last is evidenced by the fact that the sites make use of English in addition to the local language of the organisation's supporters. The journalists constitute another bystander target audience. In contrast to the appeals for active violence, there is a highly conspicuous effort at many terror sites to obtain supporters for nonviolent activity, especially through the signing of petitions and financial donations. The communicators of online information are probably more educated than other members of the terrorist organization, and hence the difference in the rhetoric contents. It was observed that many of the sites change their address frequently. Some sites disappear from the net for a while, but only to return after some time. Any efforts to block them will therefore be futile.

ICT for Financial Support Operations

The Washington Times, dated September 26, 2001 reported, "Radical Islamic militants looking to raise millions of dollars for various terrorist organizations have created dozens of Web sites featuring a hailstorm of slogans and selective verse to help bankroll the purchase of weapons and fund terrorist training camps. The sites offer instructions on where donations can be sent or smuggled, and explanations on why the funds are needed. Some even have online shopping, mostly books. The Internet has proved to be effective, cheap and accessible to terrorists and some of the sites draw thousands of the curious visitors per month. Many of the sites direct funds to the Taliban in Afghanistan, or to banks and trust accounts in Pakistan…. Last month, one site posted an 'urgent' appeal for cash, suggesting that the money—preferably U.S. currency—be sent to the Taliban consignee in Karachi, Pakistan.The web sites are also

created under aliases, designed to prevent audit trails and lead investigators to 'proxy servers', sites that can disguise the actual user.

Cyber Terrorism

Cyber-terrorism is an extension of terrorism, which does not lend itself to just one medium. Using cyberspace as a method to enhance an attack would be a logical thing to do. There are countless types of cyber terrorism scenarios, ranging from slow degradation of important but non-critical systems to wholesale broad attacks on critical infrastructure systems and anything in between them.

Experts involved in protection of critical infrastructure believe that sleeper units used in cyber attacks are already in place in the US and other countries, much like terrorist experts in physical attacks. *The SC Magazine*[24] reported that London security firm mi2g noted towards end of last year (2002) an increase in pro-Islamic groups uniting against America, UK, Australia, India and Israel, as tensions grew over political issues, such as the US/UK policy on Iraq, the Israel-Palestine conflict and the India-Pakistan stand-off over Kashmir, and as a result, corresponding digital attacks were seen to occur in cyberspace . It further reported that persistent conflict in the Middle East had prompted Israelis and Palestinians to wage a continual electronic war against each other.

Jane's Intelligence Review dated September 25, 2001 reported an increase in malicious Internet activity following September 11 attacks on WTC towers. It said that a new Internet worm, 'W32.Nimda.A@mm' supposedly circulated as a result of the suicide attacks in Washington D.C. and New York. The worm began to propagate very quickly exactly one week after the attacks, hunting for the vulnerable servers. The National Infrastructure Protection Center (NIPC), an agency run by FBI, held a press conference wherein Attorney General John Ashcroft concluded that there was no apparent connection with the attacks. However, there were at least three other hacking incidents that were related to the events of 9/11.

A similar reaction was noticed after the 'spy plane incident' in China when numerous proclamations from the hacker underground concerning the need for online retaliation were posted onto various websites.[25] Another such activity on behalf of terrorist organizations, and at a much larger scale, cannot be ruled out for future. However, the alarmist view of a cyber terrorism act resulting in death and devastation, may not come true in the near future, since there is sufficient human involvement in the control processes used today in

every critical system. Hopefully, tomorrow's fully digitised and automated systems will also have enough inbuilt protections in place.

The Indian Scene

In India, the use of ICT by terrorist organizations needs to be considered in two parts: first, in general, and second specific to the ongoing proxy war in the state of Jammu and Kashmir (J&K).

The infrastructural development of communication networks throughout the country, even to the villages, in the past decade, and easy STD/ISD access enabled the mafia/terrorist bosses to control their activities from far off places. Instances of persons like Dawood Ibrahim controlling their Indian operations from Pakistan or some Gulf country are all very well known. The availability of mobile cellular phone services towards the end of the last decade in major metropolis further facilitated their operations, and the expansion of these services all over the country is going to assist them more in the future. The mobile services and Internet were not allowed in the states of J&K and the North Eastern states till late, due to the security concerns of the LEAs (Law Enforcement Agencies). But in August 2002, a decision was taken by the government to open up these areas too so that the general public is not deprived of the technological developments and gains thereof.

Use of ICT by the terrorists in India is generally evidenced in following activities:

- Increasing use of e-mail in place of cell phones.
- SMS messages.
- Wireless Access Protocol (WAP) based telephony.
- E-banking transactions.
- Use of remote control devices, such as that for Improvised Explosive Devices (IEDs).
- Counterfeiting of currency.

The most common purpose of using the communication media, be it landline telephone, cell phone, e-mail or SMS, is the extortion threat. A study of the charge sheet filed by Delhi Police against Abu Salem Ansari and others makes an interesting reading in this regard. The complainant, Mr Ashok Gupta reported to the police that a person claiming to be Abu Salem called him and asked him to call back on either of the following three numbers-

00971507367248 (roaming), 0060193034859 (roaming) and 00871665341860 (satellite phone) in Dubai - for further instructions. A threat of dire consequences to his family also accompanied these instructions. A similar call was earlier received on his mobile by Mr Abhishek Gupta, son of Mr Ashok Gupta. Two more numbers of Abu Salem were known to police and all these were monitored. This monitoring revealed that a total of six mobile phones in Delhi were in contact with Abu Salem group. Further monitoring of these cell phones led to some other landline numbers, and the modus operandi became clear. Pawan Kumar Mittal aka Raja Bhai and Sajjan Kumar Soni aka Babu Bhai, both of Haveli Haider Quli, Chandni Chowk were found to be contacting Abu Salem, giving him information about the financial status of Mr Gupta. Another mobile phone was being used by one Asharaf aka Babloo, who was also making threats to Mr Gupta, and was a shooter of Abu Salem's 'organised crime syndicate' in Delhi. The printouts of the mobile numbers proved the association of all the accused in their crime. Even though the persons involved tried to change SIM cards of their cell phones, it was easier for the police to track them with the help of International Mobile Equipment Identity (IMEI), which is specific to a handset, and is also transmitted over the air prior to setting up the call.[26]

In another interesting case, a chance discovery of a cryptic message stored in the personal computer of a cyber cafe in Kolkata spawned fears of a terror strike in the city, during December 2002. S.Kundu, the owner of the cyber café said that a technician was overhauling the computer, when he found a file named "PAKI_G.BABA0241" in the D-Drive. Curious about the contents of the file, he opened it and found misspelt names of four prominent buildings: "Raiters Building, Bikash Bhawan, 2nd Hogly Bridge and Fharakka Bridge." Each location carried a date and time; for example, Writers' Building was having December 25, 2002, 3.45 PM. Though there was no subsequent activity related to this, the police were put on alert.[27]

Computer assisted forgery with the help of a Desk Top Printer (DTP) and Image Scanning technology is extensively being used by the criminals and terrorists for creating false documents, identity cards, authorization permits, certificates, bonds, letters of credit, cheques, credit cards, invoices, payment instructions and stamp papers, etc., with high impunity. Modern laser colour printers can easily deceive the unassisted eye. In the attack on the Indian Parliament on December 13, 2001, this technique was used by the attackers most successfully to forge the gate pass (a sticker bearing the title of 'Ministry

of Home Affairs'), identity cards of Xansa Websity Computer Education in the names of all the attackers and various other documents. The Internet was used for downloading the official logo of Ministry of Home Affairs and the layout of Parliament building. The laptop computer recovered subsequently from the accused, Mohammed Afzal and Shuakat Hussain Guru was found to have accessed Internet through Pakistan based ISPs (Internet Service Providers). It also had incomplete identity card of Indian Army and the e-mail address of 'burger'. It was disclosed by one of the accused, Mohd Afzal, that the deceased terrorist Mohammed was also involved in the hijacking of the Indian Airlines flight No. IC 814 in December 1999 and that during that operation he was code named 'Burger'. Mohammed was identified as Sunny Ahmed Quasi aka Burger aka Mansoor, involved in the hijacking. The investigations in this case were also helped by the tracing of calls to/from the cell phone numbers found with the killed terrorists. The cell phones with the accused were found to be receiving calls from Ghazi Baba (through satellite phone No. 008821651150059). [28]

The cyber terrorist activities in India have mostly been limited to network break-ins or hacking and publishing of hate material. Other criminal cases such as forgery, ATM and Credit card theft, impersonation, Internet hour theft, cyber stalking, threat, extortion and sabotage, cyber pornography, deliberate virus intrusions, database theft and file manipulation, etc., are not totally absent, though yet to pick up. There have been some cases of espionage and mail interceptions as well. However, as the digitization progresses, these threats would also increase. There have been many instances of hacking and defacement of websites with anti-India propaganda in recent past. According to CBI, the average number of web page defacements investigated per month in 2001 were in the range of 40.[29]

Use of ICT in Jammu and Kashmir

The terrorist communication network in J&K is well organized and fairly stable. Latest trans-receiver sets of Japanese and US origin have been provided to them by Pakistan, The terrorists have been imparted training by Pak Army regulars on use of these sets. The terrorists mostly use VHF (Very High Frequency)/UHF (Ultra High Frequency) radio networks for intra regional communications due to its limited (line of sight) range. Since the Pir Panjal range obstructs the LoS (line of site) between Kashmir valley and Doda-Udhampur-Rajouri regions, they have set up repeater stations, North and South of Pir Panjal. HF (High Frequency) radio network is also used by terrorists for

communication between control station and senior commanders in the valley. However, its use is restricted since communication is of long range. High Frequency radio is primarily used by terrorists for communicating with their mentors across the border. It is also used for data using data appliqué devices with secrecy. Secrecy devices are also used for voice communications at times. The VHF/UHF generally operate on Citizens band, using commercial off the shelf (COTS) equipment. In the Hilkaka operations conducted by the Army in Surankot area during April-May 2003, a satellite phone and three cellular phones were also recovered along with other weapons and ammunition. [30]

The low visibility of the terrorists and local support to them facilitate their use of the vast public communication network and they make extensive use of the BSNL network including STD. With ISD to Pakistan not being available in J&K, indirect use of ISD and STD to contact their mentors in Pak cannot be ruled out. The possibility of some important terrorists using satellite communications based on Inmarsat (International Maritime Satellite) to contact their mentors outside the country has also been reported.

Level of Communications

To cover the vast geographical area and hierarchical levels, terrorist communications are organised at different levels:-

- Across the Border: The terrorists need to maintain contact with their mentors, their supreme commander and training camps across the border. This is also required to coordinate infiltration / exfiltration of terrorists across the Line of Control (LoC).
- Inter-regional: Hierarchically, the terrorists have divided the area into various divisions. Although the divisions function quite independently, many aspects have to be coordinated among these. Long distance communications, generally over HF are used for this purpose.
- Intra-regional: The third tier is the communication between the divisional commanders and subordinate district/ battalion/ company commanders and the active terrorists operating under them within the geographical area of their control.

Pattern of Communications

There is no set pattern of communications. Terrorists ensure that there is minimum use of radio prior to infiltration, during and even afterwards, until they reach at a pre-determined point just to establish contact. Strict radio

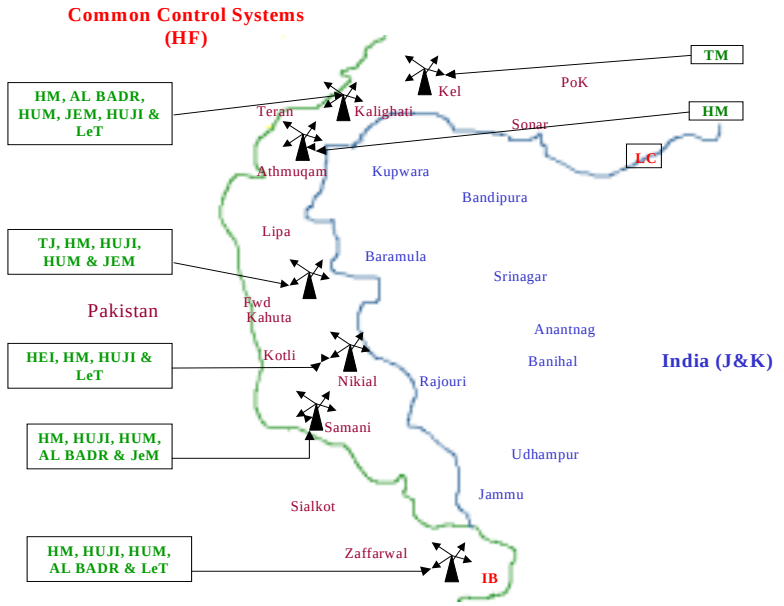
discipline is maintained during infiltration or exfiltration.

Communication Control Stations

Most of the communication control stations are set up all along the LoC and a few of them are located along the IB (International Border) as well (see Fig-2). These are established at higher mountain features starting from Kalighati in POK to Zaffarwal in Pakistan. A particular location may house many different control stations of various outfits, co-located with mutual understanding, to assist one another. Some of the control stations are at Kalighati, Tejian, Muzaffarabad, Forward Kahuta, Nikial, Samani and Zaffarwal. There are a number of repeater stations within J&K to assist the control stations to contact the remotest areas as well. The HF control setup is primarily for communicating with those in Pakistan. Almost all the HF control stations are along the LoC/IB in POK and Pakistan, except one in Srinagar.

Languages Used

The terrorists generally speak in their local Kashmiri language and dialects. There are certain terrorist groups which converse in Urdu, Punjabi, Pushto, Baluchi, Balti, Sheena and occasionally Arabic to denote numbers and words; recital of Quraan and other religious discourse including 'Tarana', a motivational song of the terrorists aired on the radio is generally in Arabic followed by its translation in Urdu and Punjabi. Terrorists of LeT, JeM and HUM groups communicate in Kashmiri. In other *tanzeems*, the local terrorists and foreign terrorists use different languages. However, the use of Arabic is very common in matrices and codes used for change of call signs and frequencies. The numerous languages used play a significant role in concealing the identity of Control Stations and Outstations. Use of English is restricted only to a few common words. Pushto and Baluchi are mainly used by the terrorists of Afghan, Baluch and Pathan origin. Opposite Kargil and Leh sectors, Sheena and Balti are more commonly used.



A restructuring of terrorist communication infrastructure was undertaken in mid-2002, to improve quality and security. Some control stations were re-sited and/or renamed. The use of satellite phones and Internet has been witnessing an increase. E-mail offers a very convenient mean of communicating to the mentors across the borders or the LoC, and it is being used by agents and sympathizers alike. The cyber cafes provide the anonymity to the sender, who can go to different cafes at irregular routine in order to avoid detection. The terrorists in J&K have quite successfully used the remote-controlled IEDs (Improvised Explosive Devices) using radio/ infra red control devices in causing death and destruction. Suicide bombing cases, in comparison, have been very few.

The escalation of tensions after December 2001 was further accentuated by a flurry of attacks in cyberspace, carried out by groups claiming to represent Islam and the interests of Pakistan. These groups united with other groups in the world in order to collaborate on causes that ranged from 'freedom' for Kashmir and a Palestinian state to support for Al Qaida and Bin Laden. The attacks against India for its Kashmir policy have mainly been limited to politically motivated website defacements. Most of these appear to have been carried out by young, pro-Pak hacker groups, such as Anti-India Crew (AIC), Pakistani Hackerz Club(PHC) and G-Force Pakistan. These groups have

recently joined to form the 'Al Qaida Muslim Alliance'. In October 2001, G-Force Pakistan pierced the firewalls of India Today news group, while the PHC, represented by Doctor Nuker, hacked the Zeenews website. It is believed that Doctor Nuker was the first hacker whose skills were recognised by the ISI, and who, under the latter's directives, focused attention on critical Indian government servers. In an interview, an AIC hacker said, "…message is for the innocent people being killed in jammu kashmir…and u know whats the reason behind all this killing? PIECE OF LAND…I will keep on defacing and passing out this word around all the world proving our point…how lame Indians are and their network security is even worse!"(sic).[31]

The Future

What is worrisome is the fact that a realisation is setting among the terrorists about the possibilities of misuse of ICT beyond communications, information and perception management—moving to more destructive domains of cyber terrorism. It has already been acknowledged that members of Al Qaida cells may have developed the skills and capabilities towards this. Increased capabilities would include coordinated, nearly simultaneous attacks in several countries, e-mail / fax death threats, and compilation of target lists by computer. Skilled hackers will access all but the most secure data banks, stealing or changing information, or destroying it. This may give them the potential for, say, manipulating the stock market for their own profit or to precipitate inflation or depression. Access to police and other security files can keep terrorists one step ahead of the LEAs (Law Enforcement Agencies). Counterfeiting of currencies for purchase of weapons and economic disruption is already affecting USA as well as India. The Internet will allow the terrorist organisations to abandon their cell structures, moving to structures only one level deep, permitting direct control, yet maintaining operational unit isolation if necessary; communications gain security and authentication with the use of available cryptography; training can be managed with multimedia tools and virtual-reality simulations for operational walkthroughs; funding comes through Internet, or it can be laundered using it (termed as Cyber laundering); conventional targeting is aided with target profiling and research; the possibilities are infinite.

Use of encryption will make it increasingly difficult for the investigating agencies to track a crime. Digitisation, video compression and Direct-to-Home (DTH) TV technologies would enable satellite telecasting of a very large number of channels in the most economic way, allowing any of the terrorist

groups to broadcast false propaganda 24 hours a day to focus specifically on their target audience over a very wide geographic area. Use of steganography (technique of hiding a message in a picture) would further facilitate passage of hidden instructions to the sleeper agents using some of these channels in a predetermined manner.

The technology is also bringing up many new types of weapons—E-Bomb, High Energy Radio Frequency (HERF) guns, High Power Microwave(HMP) bombs, Laser bombs and High Altitude Nuclear Explosions (HANE); this last is sure to deliver such a high dose of radiation that 90 per cent of the Low Earth Orbit (LEO) satellites around the globe will be lost within a month.[32] The nano-devices or micro-electromechanical (MEMs) devices coupled with robotics would allow the terrorists to enter the most secured places and act. Miniaturised UAVs (Unmanned Aerial Vehicles) can carry explosives and land at a place and time of choice. A terrorism sponsoring state, with such capabilities may use such weapons in utter desperation, resulting in great catastrophes.

The Counter Measures

The principles and methods of Network Centric Warfare or Information Warfare need to be applied to fight this second type of proxy war, being fought in the cyber space. There is an urgent need to frame rules and regulations for technological governance of the cyber space. Since the cyber space is not limited to national boundaries, international cooperation in this regard is most essential. In India, a beginning has been made through Information Technology Act 2000, which recognizes electronic documents and transactions, but a lot is yet to be achieved for the right kind of cyber space governance, leaving little maneuverability for criminals and terrorists.

The anti-technology can be defeated only with technology, and hence the scientific minds and international organisations such as International Telecommunication Union (ITU), Institution of Electrical and Electronics Engineers (IEEE) ought to apply their ingenuity in this regard, by devising more secure means of communications, and for enabling tracing and tracking of crimes, or even criminal intentions before much harm is perpetrated.

Moreover, the people too must accept that their activities in the virtual space are subject to scrutiny by the governments and their law enforcement agencies, under certain conditions and for the benefit of everyone. Cyber

surveillance will have to be accepted as a way of life, at the cost of individual privacy.

Conclusion

The terrorists are usually a step ahead of the government agencies in making use of the latest technical gadgetry for their own purposes, be it for communications or information collection. The normal response of government agencies is, mostly reactive. The intelligence agencies need to act in cohesion and in a continuously proactive manner to defeat such forces that are out to destabilise a country.

It must be recognised that the same science and technology which gives such a dreadful capability in the hands of terrorists, will also provide the mantra for defeating the terrorists' designs, provided we are alert and learn the new rules of the game and new technologies and bring in new players in the field. International cooperation in countering terrorism is also equally important, without which the battle will be difficult to win. Lastly, we ought to be prepared to sacrifice individual privacy in order to secure the society and empower the security agencies to carry out rightful surveillance of the information pathways and storehouses in the cyber space so that they are able to pre-empt terror attacks Such privacy infringements in physical space are gradually being accepted in the interests of security.

References / Endnotes

1 Kraber, P., Urban Terrorism: Baseline Data and A conceptual Framework. *Social Science Quarterly*.1971, **52** 527-533.
2 Tsfati, Yariv, and Gabriel Weimann, Terror on the Internet. *Studies in Conflict and Terrorism*. 2002, **25** 317-332 at www.terrorism.com
3 Hamelink, Cees J., The Ethics of Cyberspace. 2000. Sage; London. p 9.
4 Smith, Andrew J., Combating Terrorism. *USI Digest*. March-August 2002, **4** (8).
5 www.trc.org.
6 Head, Graham, The Future is Bright…But Whom For? *In* Max Taylor and John Horgan *Ed.* The Future of Terrorism. 2000. Frank Cass; London.
7 Raufer, Xavier, New World Disorder, New Terrorisms: New Threats for Europe and the Western World. *In* Max Taylor and John Horgan, *Ed.* Ibid.
8 Denning, Dorothy E., Information Warfare and Security. 1999. Addison Wesley, Indian reprint; p. 166.
9 Ibid., p. 68.
10 Ibid., p. 69.
11 Ibid., p. 60.

12 Ibid., p. 98.
13 Ibid., p. 156.
14 no. 9
15 Ibid., p. 159.
16 *Aviation Week & Space Technology*. November 25, 2002.
17 *The Times of India*. New Delhi. November 23, 2002.
18 Ibid., December 01, 2002.
19 Murphy, John E. Jr, Sword of Islam. 2002. Prometheus Books; New York. p. 156.
20 *The Times of India*. New Delhi. November 21, 2002; NDTV news, November 13, 2002.
21 *The Times of India*. New Delhi. December 07, 2002.
22 Gladney, Dru C., *5th Asian Security Conference*. Institute for Defence Studies and Analyses. New Delhi. January 2003.
23 Tsfati, Yariv, and Gabriel Weimann, no. 2.
24 *SC Magazine*. January 2003, **6** (1) Asia Pacific Edition at www.scmagazine.com.
25 *Jane's Intelligence Review*. September 25, 2001.
26 Chargesheet filed by Delhi Police in response to FIR No. 88/2002, Greater Kailash Police Station. New Delhi.
27 *The Times of India*. New Delhi. January 09, 2003.
28 Chargesheet filed by Delhi Police in response to FIR No. 417/2001, Parliament Street Police Station. New Delhi.
29 Presentation made to the Joint Indo-US Initiative on Cyber Terrorism, August 2002.
30 J&K Shock and Awe Operation. *The Times of India*. New Delhi. May 24, 2003.
31 Anhal, Aarti, Hackers Take Kashmir Dispute to Cyber space. *Jane's Intelligence Review*. October 2002.
32 *Jane's Defence Weekly*. October 23, 2002.

Col Shitanshu Mishra is Research Fellow in IDSA, and is presently working on 'Communication Technology and Counter Terrorism'.

He is Fellow of Institution of Telecommunication and Electronics Engineers (IETE) for more than 10 years, and a member of Computer Society of India (CSI) for well over 15 years. He is one of the founding members of 'Association for Security of Information Systems'.