DECODING CYBER TERRORISM: TOWARDS A CULTURE OF INTERNATIONAL CO-OPERATION

M.K. SHARMA

The collective consciousness of the global society today has risen to a level wherein nation-states want to be seen as rational. As the large destructive power of nuclear weapons and conventional weapons makes their use on a large scale almost impossible, War By Other Means (WBOM), and cyber warfare are seen as more benevolent yet effective tools of exercising power in this age. Cyber warfare, in many ways is the smartest way of realising the famous saying of Sun Tzu "A victorious army first wins, and then seeks battle, a defeated army first battles then seeks victory".

While it may be true that technology permeates war but does not govern it, one must appreciate that it is not the technology per-se, but how it is organised that shapes what kinds of threats we would face in the future. The world today is faced with a newer and more potent threat called terrorism, which, when fuelled by information technological innovations, is called cyber terrorism.

Wing Commander **M.K. Sharma**, is a Research Fellow at the Centre for Air Power Studies, New Delhi.

Exploitation of cyber space is becoming easier each passing day mainly due to the inherent anonymity attached to it.

AIM

This paper addresses the dynamics of cyber terrorism as a threat to the National Critical Information Infrastructure (NCII) and how the international community, regulatory and legal systems should respond to this increasingly potent security threat to nation-states.

SCOPE

The scope of this paper is to understand cyber terrorism tools that could be used against a nation-state's critical information infrastructure while deliberating on how different nations look at NCII, with the help of a survey of ten countries. The paper intends to bring forth the concept of 'Cyber Centres of Gravity' as a new way of looking at NCII. 'Offence, Defence and Deterrence Dynamics' as a counter-cyber terrorism strategy has been discussed, with focus on the contrast of economic efforts involved in creating cyber defences for NCII vis-a-vis cyber offensive tools available in the hands of terrorists. The paper also discusses the different ways in which the internet is being leveraged by cyber terrorists and the role the international community can play in securing cyber space.

CYBER WAR-MAKING TOOLS

Exploitation of cyber space is becoming easier each passing day mainly due to the inherent anonymity attached to it. In fact, one of the major factors responsible for the rising vulnerabilities in cyber space is the rising sophistication in hacker tools that has come of age from mere password guessing ability and self-replicating codes in the 1980s, to password cracking, exploiting known vulnerabilities, back doors and disabling audits in the 1990s and gaining new heights of sophistication with techniques like sweepers, sniffers, hijacking sensors, stealth diagnostics and packet forging or spoofing today. This has resulted in the availability of phenomenally powerful hacking tools with a simultaneous sharp drop in the technical knowledge required to use them.

CONCEPT OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE (NCII)

Over a period of time, the concept of criticality has also undergone change, and the criteria for determining infrastructures that qualify as critical have expanded over time.

An analysis of the most frequently mentioned critical sectors in various countries indicates that there are fifteen core sectors of modern societies, that are possibly the areas where a large-scale interruption would be most devastating. A "critically important part of the information infrastructure" as defined in UN Resolution A/RES/65/41 is "a part (element) of an information infrastructure, actions against which could have consequences directly connected to national security, including the security of individuals, society, and the government".

Over a period of time, the concept of criticality has also undergone change, and the criteria for determining infrastructures that qualify as critical have expanded over time. The President's Commission on Critical Infrastructure (PCCIP) of the US, for example, defined eight sectors as critical for the US initially; however, today, there are more than 18 critical infrastructures in the US today.[1] There are mainly two interrelated perceptions of viewing criticality by the nation-states:[2]

Criticality as a Systemic Concept: This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus, reinforces interdependencies.

Criticality as a Symbolic Concept: This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependency is secondary – the inherent symbolic meaning of certain infrastructures is enough to make

1. CIIP Handbooks 2002, 2004, and 2006
2. Metzger, "The Concept of Critical Infrastructure Protection (CIP)" in A. J. K. Bailes, and Isabelle Frommelt, eds., *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford: Oxford University Press), pp. 197–209.

them interesting targets.[3]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical sites with a strong symbolic character. Additionally, the symbolic approach allows essential assets to be defined more easily than the systemic one, because in a socio-political context, the defining element is not interdependency as such, but the role, relevance, and symbolic value of specific infrastructures.

Table 1: Overview of Critical Sectors and Sub-Sectors Identified by Surveyed Countries.[4]

Country Specific Critical Sectors	**US**	**IND**	**GER**	**CAN**	**JAP**	**RUS**	**UK**	**MAL**	**EST**	**AUS**
Banking and Finance	*	*	*	*	*	*	*	*	*	*
Central Government /Govt. Services	*		*	*	*	*	*	*	*	
Chemical and Nuclear Industry	*	*		*				*		
Emergency / Rescue Services	*	*		*		*	*	*	*	*
Energy / Electricity	*	*	*	*	*		*		*	*
Food / Agriculture	*		*	*	*		*		*	*
Health Services	*			*			*	*	*	*
Information Services / Media	*					*				*

3. Critical Assessment Without Interdependencies: United States General Accounting Office (GAO). Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform. "Homeland Security: Key Elements of a Risk Management". Statement of Raymond J. Decker, Director, Defence Capabilities and Management, October 12, 2001, p. 6. http://www.gao. gov/new.items/d02150t.pdf, accessed in June 2008.
4. Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, *International **CIIP Handbook** 2008 / 2009*, pp.530-531.

Military Defence / Defence Facilities	*	*				*	*	*		
National Icons and Monuments	*									*
Sewerage / Waste Management	*						*	*		*
Telecommunications	*	*	*	*	*	*	*		*	*
Transportation Logistics	*	*	*	*	*		*	*	*	*
Water Infrastructure	*								*	
Water (Supply)	*		*		*		*	*	*	*

Survey Findings on Approaches to NCII: Different countries view criticality differently. In some countries, Critical Information Infrastructure Protection (CIIP) efforts are mainly led by the defence establishment, whereas in other countries, such as the UK, the efforts towards CIIP are jointly led by the business community and public agencies. Furthermore, in Australia as well as in the US, CIIP is integrated into the overall counter-terrorism efforts, where the intelligence community plays an important role. In India, Korea, and Japan, the fostering of the information society and economic growth through safe information infrastructures is at the forefront.

It is evident from the ongoing analysis that current methodologies for identifying Critical Information Infrastructure (CII) are insufficient in a number of ways. One of the major shortcomings is that the majority of nation-states fail to address the issue of interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focussed on a single infrastructure and do not take into account the strategic, security-related, and economic importance of CII.

Presently, India has adopted the US (PCIIP) way of identifying NCII which is based on almost a one-to-one mapping between infrastructures identified as critical and the members of the commission. This approach

may altogether omit some critical infrastructure from the list just because it did not fall in the area of their expertise.[5] How can we ensure that the list is complete and the most critical infrastructures are identified? Therefore, a different approach based on scientific methods such as modelling and simulation techniques for identifying CII is required. This could be approached either on the basis of 'minimum flow' or be 'economic-based'.

Minimum Flow-Based Approach to NCII: Survival of any system, civil or military, would depend on flow of data (in turn, flow of deliverables, goods through the distribution network). Any type of attack (bombs or sabotage) which is likely to disable some nodes will not necessarily cripple the system. Through modelling, we can arrive at some minimum data flow rate for any system below which it would become mission critical. This approach is different from the other approaches such as intrusion detection, which are limited to computer security. The minimum flow-based approach analyses the damage that the enemy can cause to the critical infrastructure if he succeeds in an attack. This would help build the optimum redundant flow models, making it hard for the enemy (insider and outsider both) to choose an optimal winning strategy.

During World War II, a PERT digraph of the then mechanical model showed ball bearings as the most critical component in the war-making industry, as removing this single node could affect several outputs such as manufacturing of tanks, aircraft, trucks, cars, etc. Therefore, targeting, Nazi Germany's factories involved in making ball bearings by bombing campaigns proved to be decisive.

An Economic-Based Approach to NCII: This approach takes into account what an enemy can attack. For any attack, there is a corresponding cost involved (in terms of the enemy's budget or the free time the hacker has got, etc). Say the enemy will be able to take over a set of nodes and edges within its budget. However, the factors affecting the enemy's potential are not necessarily related linearly like the enemy's capability for a given budget will come down drastically if so many different operating systems are in use.

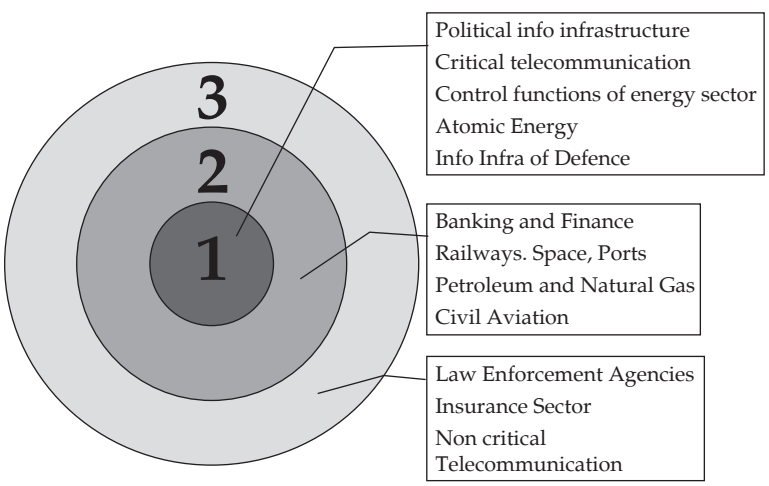
5. The food distribution and production industry was one of the many critical infrastructures that was not included, which later got included in the list of the President's National Strategy for Homeland Security, htttp://www.ciao.gov/publicaffairs/qsandas.htm.

Also the combined effect of the degradation of multiple essential systems just above critical values would need development of more comprehensive models based on approximation techniques to improve predictability of critical infrastructures' survivability.

To identify which infrastructures are truly the most critical, more refined alternative models will have to be developed, taking into account the dynamic aspect of our society. The time aspect would have to be included in the models. This would enable us to deal with buffers and recovery, which are time critical processes. Another point to be taken care of while developing the model is that all the damaged nodes are not necessarily destroyed. In a flow model, a damaged node may correspond to reduced flow or incorrect flow, resulting in a faulty product from a factory, having ripple effects.

CYBER CENTRES OF GRAVITY

Fig 1: Cyber Centres of Gravity



India's NCII as defined are banking and finance, insurance, civil aviation, telecommunications, atomic energy, power, ports, railways, space, petroleum and natural gas, defence, law enforcement agencies. All national

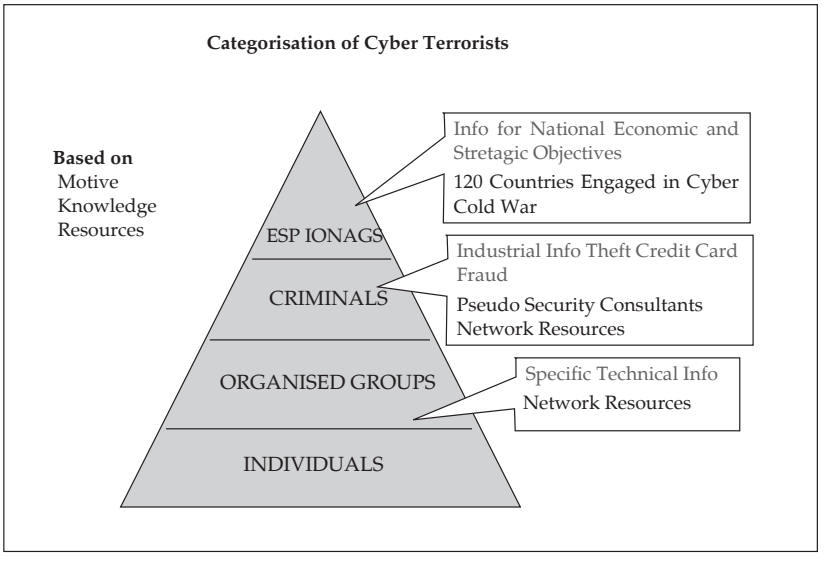
cyber assets could be grouped on the basis of centres of gravity for national security (say, in a three tier arrangement).

The innermost cyber centre of gravity would consist of those components of NCII that are critical to national security and sustaining human life such as: political information infrastructure, critical telecommunication sector, control functions of the energy sector and information infrastructure of the defence sector, etc. This must be made as robust as possible. The next centre of gravity would consist of those cyber assets which are important to the country's economy even if they are not likely to cause physical harm such as banking and finance, railways, space, ports, petroleum and natural gas, atomic energy and civil aviation, etc.

The third tier, the outermost centre of gravity, would consist of systems whose disruption would cause considerable personal inconvenience or economic loss but would not present a threat to the existence of the society as a whole, such as law enforcement agencies, the insurance sector and the non-critical telecommunication sector, etc.

CATEGORIES OF CYBER INTRUDERS

Fig 2: Categorisation of Cyber Intruders



There are different categories of intruders based on their motive, knowledge level and the resources at their disposal. 'Individual intruders' are generally motivated by thrill, or challenge without any strategic planning e.g. Gary McKinnon of north London is accused of committing the "biggest military computer hack of all times", on the Pentagon and National Aeronautics and Space Agency (NASA) systems and the cost of repairing the shutdown was $70 million dollars.

Investments in cyber defence have a diminishing marginal return per rupee spent on security. Extrapolating from it, the larger the attack, the less cost-effective the defence is in preventing harmful effects.

There are 'organised groups' with the common goal of getting access to specific information like proprietary technical information of credit reports, etc. The 'criminals category' of intruders is growing at the highest rate, motivated to gain unauthorised access to systems for monetary profit or unfair market share. They are involved in wire transfer theft, industrial espionage, credit card theft, or become pseudo security consultants. It is believed that the development of the Tupolev Tu-144 supersonic aircraft, with its rapid design similarity to Concorde, was one of the most prominent examples of industrial espionage in the 20th century.

The 'espionage category' of intrusions has the greatest variety and complexity of methods and resources. Often, the resources available (equipment, manpower and technical knowledge) are limited only by cost versus the potential gain, and many a times these are sponsored by state and non-state actors. With the primary motive of access to systems or information for national, economic or strategic objectives—this category has direct national security ramifications.

To be prepared for the worst, we have to assess the potential damage by the worst kind of intrusion 'espionage' on our innermost cyber centre of gravity. And this requires further in-depth model-based research.

OFFENCE-DEFENCE AND DETERRENCE DYNAMICS

Investments in cyber defence have a diminishing marginal return per rupee spent on security. Extrapolating from it, the larger the attack, the less cost-effective the defence is in preventing harmful effects. The diminishing returns on investment in defence relative to offence are especially conspicuous when considering the disparity between "hacking" and "patching" in complexity, cost, and time required. For example, a sophisticated network defence software contains between 5 million and 10 million lines of code, whereas an attack malware contains an average of 170 lines of code. Also, protection of critical government networks typically requires standard government competition and contracting, which can take years before solutions are initiated, whereas designing an attack can be accomplished in weeks. While network defence against sophisticated attackers requires advanced work by highly specialised firms, network attack is literally a cottage industry.

Deterrence: Is it fair to draw a direct analogy between nuclear deterrence or traditional military deterrence and cyber deterrence wherein we may not know exactly who did it? Or what is the assessment of collateral damage due to interdependence on target infrastructure? Or how much are we prepared to absorb a retaliatory cyber attack? The notion of deterrence in cyber space is something that works today but may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and war-fighting tenets established in other media do not necessarily translate reliably into cyber space. Such tenets must be rethought.

The attraction of cyber deterrence is that, if it works, it can reduce the cost of defending systems How do we build credible cyber deterrence? One chief way any deterrence works on the minds of the attackers is the defender's coercive power. It can be made visible very easily in real space by positioning kinetic weapon systems such as tanks, missiles, aircraft and carriers but to demonstrate coercion capability in cyber space, the biggest challenge is of credibility. The attacker may not be sure of what a cyber attack may do to the defender's economy or society because the attacker may neither be sure of his own vulnerabilities nor of the defender's capabilities.

In such a credibility crisis, to ensure that cyber deterrence remains effective, the defender may have to strike the attacker to demonstrate some coercive capability. At the same time, it is important on the part of the defender to signal that a specific attack on the attacker's vulnerability was to coerce in order to accrue maximum deterrence credibility.

It is noteworthy that so far terrorists have not carried out any visible attacks against internet infrastructure.

The calculus of the deterrence should be based on the principle that the lower the chances of getting caught, the higher the penalty required to drive the message to the potential attackers that what they might want to try is not worth the cost they would have to pay. Like having established the source of cyber espionage, if the NTRO (National Technical Research Organisation) is able to demonstrate stern punitive and surgical action in cyber space, it would enhance the credibility of cyber deterrence and, thus, increase the cost of such misadventures in the future in the minds of opponents. But the problem is that this calculus is not applicable to terrorists' organisations as they have nothing much at stake in the cyber domain. Therefore, non-state actors and rogue states, with little to lose in the cyber domain probably cannot be deterred by the threat of cyber retaliation.

LEVERAGING THE INTERNET: NEW TRENDS IN CYBER TERRORISM

There are different shades of terrorism painted through the virtues of the internet. Some would call themselves Islamist, Marxist, nationalist, Maoists, separatist, or racist. All of them use the virtues of the internet such as: it is ubiquitous, unregulated, and inexpensive; its potential audience is huge, worldwide, and it has easy access; communication is anonymous, fast, and robust. The multi-media environment facilitates development, maintenance and download. And, finally, it can shape coverage in the traditional mass media.

It is noteworthy that so far, terrorists have not carried out any visible attacks against internet infrastructure. The reason could be the fact that they need the internet as a recruitment tool and do not want to harm

the major medium facilitating their communication. Some of the many ways the internet is being exploited by the terrorists are as follows:

- **Convergence of Terrorism and Cyber Space:** On further investigation and a look beyond the definitional boundaries of 'pure cyber-terrorism', it is realised that cyber terrorism is not only when the attack is launched against computers but when many other factors and abilities of cyber-space are leveraged by the terrorists in order to accomplish their missions. For example, to get the Voice Over Internet Protocol (VOIP) facility which was used as a real-time tactical support to commit an act of terror in Mumbai on November 26, 2008, the terrorists used cyber space and globalisation to their advantage. They paid $220 in Spain and $229 in Italy that was channelised from Pakistan to Italy and then to Callphonex company in New Jersey to get this VOIP facility.
- **Internet as Terrorism Force Multiplier:** A computer is a technological tool that can be a force multiplier. What does that mean to terrorists? Just as the distinction between war and peace or criminality and political protest is blurring, so is the distinction between cyber disruption and cyber terrorism. Terrorists are taking full advantage of the force multiplier effect of cyber space. Firstly, the mass media are manipulated to expand the aura of the group. Secondly, trans-national support networks give small groups logistic support and mobility and, lastly, technology allows terrorists to increase the striking power of their weapons.
- **Cyber Planning: A Dangerous Weapon in the Terrorists' Arsenal:** While the internet still offers its old promise of unparalleled opportunities, in some respects, it has also become a digital menace. It is providing a virtual battlefield for peace-time hostilities between Taiwan and China, Israel and Palestine, India and Pakistan and also China and the US.[6] During both wars of Kosovo and in the aftermath of the collision between the US Navy EP-3 aircraft and Chinese J-8-IIM fighter[7], there have been digital battles. In the times of actual conflict, the internet was used as virtual battleground between NATO's coalition forces and

6. William Mathews , "China Cited as Biggest Cyber Threat to US" *Defense News* February, 8, 2010, p. 24.
7. http://en.wikipedia.org/wiki/Hainan_Island_incident

elements of the Serbian population. There is strong evidence that Al Qaeda terrorists used the internet to plan 9/11. Al Qaeda cells operating from the US were using internet-based phone services to communicate with cells overseas till September 2002.[8] In this regard, cyber planning seems a more dangerous tool with terrorists than the much feared cyber terrorism options of attacking NCII, etc.

- **Internet as an Ideological Weapon:** As internet access can be controlled and its use can be directed according to server configuration, this makes the internet a true ideological weapon. In earlier days, most governments could censor or filter the content being shown on TV or published in newspapers if there was something offensive but this is not the case with the internet. The internet serves as the terrorists' international newspaper, TV station or radio station or journal. There are two distinct advantages accrued by the terrorists: firstly, the cost advantage as the web allows an uncensored and unfiltered version of an event to be broadcast worldwide at almost no cost. Secondly, the internet provides the most congenial environment for these underfunded groups to offset both internal and international condemnation of their acts by explaining their viewpoint to the target viewers, especially when using specific servers.
- **Internet Creates Virtual Army for Small Terrorist Groups:** The internet can empower the terrorist groups by making us believe that they are bigger than they are actually are through news reports, etc claiming that there are hundreds of thousands of operatives working on the net on a daily basis. This way they can spread cyber fear by exploiting the public psyche of: what will happen.. if? What will happen if they disrupt the critical information infrastructure, or disrupt the Air Traffic Control (ATC) or destroy the stock market? What if they reveal secret military computer network or the Indian Space Research Organisation's (ISRO's) research? However, in reality, the terrorists may not possess such capability.
- **Internet as Fund Raiser Apparatus:** The internet is being used in many ways to raise funds for terrorist organisations, including criminal

8. Timothy L. Thomas, *Cyberterrorism* (Ashgate: UK 2004), Ch. 13, p. 112.

The internet's command and control potential can vastly improve an organisation's effectiveness—more so when it does not have a well defined organisational structure.

activities like credit card frauds, piracy or *hawala* transactions. As Jean-Fracois Ricard, one of France's top anti-terrorism investigators puts it, many Islamic terror plots in Europe and North America were financed through such methods. In other 'noble' ways of raising funds, it was found that Al Qaeda and humanitarian agencies were using the same bank account numbers on numerous occasions as a result of which many US-based Islamic charities were shut down.[9] The Sunni extremist group Hizb al–Tahrir uses an integrated web of internet sites from Europe to Africa to call for the return of an Islamic caliphate, stating that it desires to carry out *jihad* by peaceful means.[10]

- **Internet as Intelligence Gathering Tool on Potential Enemy:** On January 15, 2003, the then US Defence Secretary Donald Rumsfeld had observed, as quoted in an Al Qaeda training manual recovered from Afghanistan, that using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about an enemy.[11] Over a period of time, the terrorist organisations have become quite methodical in their approach to intelligence gathering. The discussions now include targets such as Supervisory Control and Data Access (SCADA) systems, money movement control systems, and facilities controlling the flow of information over the internet.[12]
- **Internet as an Outstanding Command and Control Mechanism:** The internet's command and control potential can vastly improve an organisation's effectiveness—more so when it does not have a well defined organisational structure. The terrorists now have access to the

9. Colin Soloway, Rod Norland, and Barbie Nadeau, "Hiding (and Seeking) Messages on the Web," *Newsweek*, June 17, 2002.
10. Timothy L. Thomas, "Al Qaeda and the Interent: The Danger of Cyber Planning, in *Cyber Terrorism* (Ashgate UK: 2004) , Ch. 13, p 114.
11. "Citing Al Qaeda Manual, Rumsfeld Re-emphasises Web Security," insidedefense.com, http://www.inside defence.com/, January 15, 2003.
12. Tom Squitieri, "Cyber Space Full of Terror Targets" *USA Today*, June, 5, 2002.

means of command and control to plan and coordinate attacks. Another aspect unique of cyber command and control is that through this, the terrorists today can control resources (i.e. men, computers, servers, links and electrons) that belong to others, including their adversaries. Command and control on the internet is not hindered by geographical distances, or by lack of sophisticated communication equipment

- **Internet to Study Anti–Terror Mechanism:** Terrorists are aware of the fact that their net communication is being monitored. When governments discover some imminent threat, a warning is issued to the security agencies. The terrorists could include fake information about a terror plot via routine media to check and measure the response of a security agency.

COUNTER-CYBER TERRORISM STRATEGIES

The consequences of technologies are frequently unplanned and grossly unpredictable and best left that way as far as possible. To the counter-cyber terrorist agencies, even a threat of cyber terrorist attack comprises cyber terrorism to the extent that a mere possibility of a cyber attack against NCII components even without an explicit threat, is a matter of great concern. The counter-cyber terrorism professionals are faced with the reality of terrorists using advanced technology to hide their communications from prying eyes. Any terrorist organisation or group trying to evolve into a violent political movement would use cyber space to advance its cause. This is also the reality that counter-terrorism agencies are not organisationally prepared to defend against such advances in technology.[13]

Cyber Forensics: Cyber forensics is seen more as a tool used to investigate a chain of events once the crime has taken place. But it needs to be seen as a preemptive measure to stop terror incidents. Hence, a two-way consolidated model needs to be put in place to track terrorist activities and curb criminals.

- **Pre-event:** This model is predictive in nature and is driven by intelligence collected through the use of technology. As terrorists have increased

13. Arquilla and Ronfeldt, *The Advent of Netwar* (RAND Monograph Report, 1996), p. 96.

dependence on the internet and on web technology, they are using cyber space for planning, communications, and logistics control. Network monitoring and forensics can pick up the indicators and triggers before the actual event takes place and generate intelligence inputs for agencies to investigate further. The process encompasses regular monitoring and collecting evidence through 'packet' level forensics, whereby packets of information moving in and going out are monitored. Subsequent analysis through data mining generates trends and patterns almost in real-time for further intelligence. The analysis can help in isolating patterns based on previously known 'suspicious' entities or on new ones, identifying and investigating 'triggers' or any unusual developments for future analysis and threat assessment.

- **Post-event:** This deals with the forensic science of all the equipment containing digital evidence such as computers, laptops, palmtops, mobile phones, satellite phones, GPS (Global Positioning System) devices, etc. In high profile cases and incidents, such as the Parliament attack in New Delhi in 2001, the Mumbai serial train blasts in 2006, and the 26/11 Mumbai attacks, cyber forensics played a decisive role in gathering e-evidence and collating the sequence of events for the prosecution of the suspects. This also provided the necessary breakthroughs and insights of how terrorists are masking their identities and executing their plans. Detailed post-event forensics is the critical component of intelligence gathering. It generates information and an evidence chain that then facilitates monitoring and tracking.

Net-Centric Counter-Terrorism: The key learning for intelligence agencies is that any activity over the internet leaves traces and communication patterns that can be tracked with a great degree of accuracy. However, the caveat here is that inflow and outflow of information have to be continuously and rigorously monitored. And here, cyber forensics plays a crucial role in investigations and intelligence gathering to curb and preempt terrorist activities. The pre- and post-event techniques of cyber forensics (supported by the evidence chain management) can help in anticipating, and appropriately reacting to, terrorist activities over cyber space.

To counter cyber terrorism, 'mapping the loose ends' is a very important component. In India, there are over 52 million internet users[14] and over 200,000 cyber cafés. The Indian government has asked café owners to authenticate internet users through their identity cards and to place CCTV (Closed Circuit TV) cameras in the cyber cafés. While it is a challenge for the law enforcement agencies to monitor every cyber café, it is here that cyber forensics-based audits and evidence gathering can play a pivotal role in preventing criminal use of the cyber cafés. Similarly, Internet Service Providers (ISPs) can use that technology to monitor the traffic data of the cyber cafés to a greater degree, and develop (real-time) trends and patterns at the micro level. Cyber forensics can be applied to networks and in the case of any red flags or once the IP is tracked, it can help in imaging the hard disk and track the individuals responsible for the activity. The metadata of the files or any document can be analysed and matched with the log maintained by the cyber café. Some of these measures would require policy and legal changes to ensure compliance and prevent misuse.

Neither prevention nor preemption is possible in cyber space. Only effective countering can deny the terrorists the advantages presently enjoyed by them.

Neither prevention nor preemption is possible in cyber space. Only effective countering can deny the terrorists the advantages presently enjoyed by them. Countering their innumerable websites by suppressing them would be counter-productive. The websites 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 need to be suppressed are those pages or sections of their websites which disseminate information about how to commit an act of terrorism. An effective counter to their use of the web for propaganda and psy-war purposes is not suppressing them, but the state developing better means of dissemination of information and a better psy-war capability in order to discredit the terrorist organisations and wean their followers away from them.

14. http://trak.in/tags/business/2010/04/07/internet-usage-india-report-2010/

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 cooperation by way of intelligence sharing, there is very little cooperation by way of technology sharing.

Technology Sharing: A Double-Edged Sword: 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 cooperation would, therefore, continue to be limited. The post-9/11 period has seen greater bilateral and multilateral cooperation 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.

Implanting Human Moles: 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 so far received.

SOCIAL, REGULATORY AND LEGAL ISSUES

A discussion on the threat of cyber terrorism is generally focussed on the successful missions of the cyber terrorists and, in the bargain, the day-to-day usage of the internet by the terrorists that could decode their modus operandi is ignored. For terrorists, the internet is the most dynamic tool—the websites suddenly emerge, change, disappear, or, change their URL, but the contents remain the same.

Cyber terrorists mainly target three types of audience: current and potential supporters, international public opinion and citizens of the states against which the terrorists are fighting (to stimulate public debate).

Challenges for Law Enforcement Agencies: The challenges that cyber terrorism poses to the society and the Law Enforcement Agencies (LEAs) are two-fold:

- **The Terrorism in the Real World Using Cyber Space as a Conduit:** Terrorism in the physical world results in an adverse effect on the real world society, persons and property. Al Qaeda terrorists used the internet to download the topography of the Indian Parliament building and plan an attack based on such information. The internet was used to communicate amongst the members of the attacking team to carry out the act of terror in the real world. Similarly, when an e-mail chain is set-off on the internet, spreading a false story on the Godhra tragedy or a website such as daliststan.org is being published, there is an attempted use of cyber space to further the terrorist movement in the physical space.
- **Terrorism in Cyber Space Involving Destruction of Cyber Properties:** When the hackers of the Anti-India Force of Pakistan attack Indian websites and deface them, it is the cyber property of an Indian being attacked. In a more sophisticated attack, the website of economic significance such as the National Stock Exchange may be disabled through a virus or a Distributed Denial of Service Attack (DDoS) attack causing stoppage of a vital commercial activity.

Since real world terrorism laws are sometimes inadequate to meet the contingencies of cyber space and cyber society laws may be inadequate to deal with terrorist acts, there is enough scope for cyber terrorists to slip between the two legislations and escape conviction. The most important challenge before LEAs is, therefore, to understand the legal framework applicable to cyber terrorism and work within its limitations and yet meet the expectations of the society.

Additionally, like in the case of real world terrorism, the LEAs will have to neutralise the motivating forces behind the rise of terrorist movements in

A very likely scenario in future modern conflicts that include cyber methods is the use of members of organised crime or half-legal entities for organising and covering up attacks.

an accepted, civilised manner, not providing an opportunity for terrorists to hide behind human rights activists. This may require careful handling of the intelligence related functions without being accused of privacy invasion or censorship.

Also, since the cyber environment is built on networks and communication, cyber terrorism can be operated remotely with a highly distributed network of operators, creating all kinds of jurisdictional problems relating to intelligence gathering, investigation and conviction.

ROLE OF THE INTERNATIONAL COMMUNITY

Reduce the Vulnerabilities to Asymmetric Threats: The states will have to address potential threats to security that are likely to emerge as a result of an unequal distribution of soft power. Countries, regions and various groups already suffering economic hardship and political and cultural alienation are unlikely to feel the benefits of information technology easily.[15] Thus, while developed states may be tempted to exploit the opportunities afforded to them by information technologies in order to gain advantages over their rivals, they will have to weigh this against the cost of ignoring their vulnerability to asymmetrical threats.

A very likely scenario in future modern conflicts that include cyber methods is the use of members of organised crime or half-legal entities for organising and covering up attacks. It is still possible to lose traces and hide behind the fact that national regulations in criminalising cyber crime are very uneven, law enforcement personnel are overburdened

15. The term and concept of security has been discussed by a great many scholars. Examples of this debate include: Barry Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post–Cold War Era* (Harlow, 1991); David Baldwin, "Security Studies and the End of the Cold War", *World Politics*, 48/1 (1995): 117–41; Stephen Walt, "The Renaissance of Security Studies", *International Studies Quarterly*, 1991, p. 35.

in this area and there is not enough attention given to the issue of international cyber crime.

CONCLUSION

The cyber terrorism issue is neither a collection of incidents that have already occurred, nor only a matter of what might happen in the future. It is to be understood as a strategic tool in the power game by terrorists, non-state and near-state actors. Computers can play an enormous role in terrorism and, at the same time, they can provide perhaps the most potent defence against terrorism if we use them to our advantage. It would be a grave mistake if we try to tackle pure cyber terrorism or cyber terrorism separately from the big picture of terrorism. In which case we would miss the true threat posed by the additional factors of cyber space in the playbooks of the terrorists.

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 their flow of volunteers and funds. An important component of cyber counter-terrorism is, therefore, devising ways of denying them success in cyber space. But the international community is nowhere near achieving it.

As some opine, the threat of cyber terrorism is still a kind of ghost story without enough evidence to believe that the threat entails actual damage or death through its use. And that the scarce resources being drained in building counter-cyber terrorism may find a better use, especially in a developing economy like India. This argument is analogous to what the Japanese presented as they prepared to take on an expected Allied amphibious invasion in August 1945, while neglecting the defence of facilities located at Hiroshima and Nagasaki despite forewarnings.[16]

16 krex.k-state.edu/dspace/bitstream/2097/2161/1/JamesIsemann2009.pdf