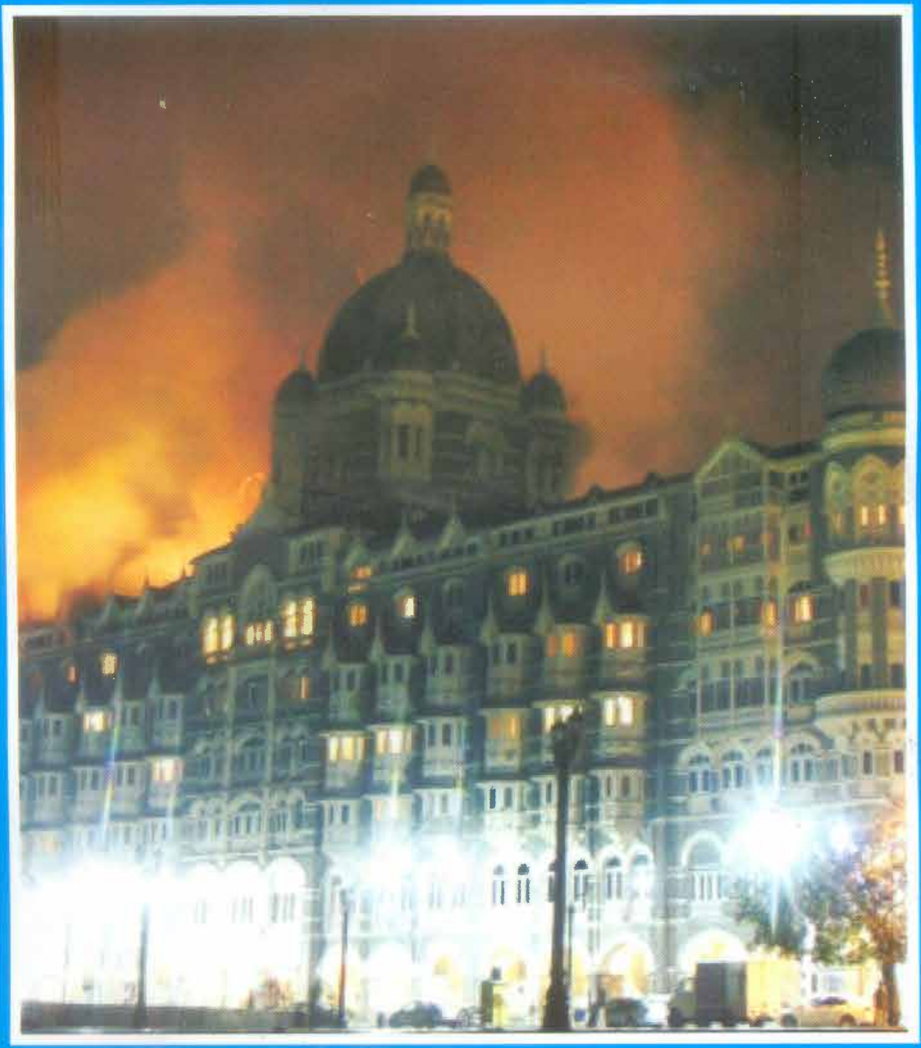
"TECHNOLOGY & TERROR – ROLE OF ICT IN WAR AGAINST TERROR"

IETE-SPECIAL ISSUE

COMMEMORATING 52nd ATC-2009



सह वीर्यं करवावहै

THE INSTITUTION OF ELECTRONICS AND TELECOMMUNICATION ENGINEERS (IETE)
#2, Institutional Area, Lodi Road, New Delhi-110003; Tel. : 011-43538855/56, 43538821/22, Fax : 011-24649429
E-mail : membership@iete.org, sec.gen@iete.org; Website : www.iete.org, www.iete.info

IETE-SPECIAL ISSUE
COMMEMORATING 52ND ATC-2009

The Institution of Electronics and Telecommunication Engineers (IETE)

COPYRIGHT

CONTENTS

PREFACE

"Quality is never an accident: it is always the result of high intention, sincere effort, intelligent direction and skillful execution; it represents the wise choice of many alternatives." The saying holds true for our 52nd Annual Technical Convention which reflects our continuous efforts towards learning, growing and improving. This activity with time & advancement has become a very important annual event for IETE.

Modern Technology ingrained deeply in the today's society continues to evolve at such a fast rate that compels us to believe that we cannot survive without it. Everyone wants to be a gadget guru. But what if it gets out of control and used for wrong reasons? The terrorist attacks at Mumbai last year shocked the whole world with a very negative impact on general public. This induced IETE to devote this year's Annual Technical Convention to the theme "Technology & Terror- Role of ICT in War against Terror" and to bring out this special issue on the theme.

There are fifteen articles in this special issue by experts and eminent personalities and are dedicated to the role of Information and Telecommunication Technologies (ICTs), analysis of the severity of the situation and have suggested some possible measures as a result of their research and surveys.

This issue is basically aimed to emphasize the role of information technology in countering terrorism in an era of globalization. Modern terrorism has been characterized as a negative response to globalization. At the same time, terrorism has become very effective by exploiting the engines of globalization. Terrorists have shown the ability to exploit information technology and using it as a weapon. To address all these related issues a few articles outline the role of information technology in fighting terrorism, especially in intelligence analysis, some articles bring out the challenges that lie ahead and some articles leverage information technology in its war against terrorism. An attempt has been to strike a balance of security, civil & economic liberty and technology and law.

In summing up, this special issue aims to help our readers gain a better understanding of the issues related to technology & terror and suggesting ways to use ICT more productively as a counter measure to terrorism. Hopefully this special issue would enable the readers to have better understanding of the issues involved.

I am sure members of IETE fraternity, scientists and engineers will greatly benefit and enjoy reading this special issue. I would like to express my gratitude to Shri P N Chopra, Chairman, Technical Programmes Committee and the contributors of articles in bringing out this very important and timely special issue on the occasion of IETE ATC-2009.

Lt Gen Ashok Agrawal, PVSM (Retd)
President IETE

19 Sep 2009
New Delhi

FOREWORD

It is interesting to observe that during the 20th century, technology has been developed to travel faster, higher and further than ever before in the history. Now Electronics, Computer, Information and Communication Technologies (ICT) have made the transfer of information and ideas almost instantaneous. The world and universe around us is shrinking in technological time and distance.

The key to a national prosperity, apart from the spirit of its people lies with the effective combination of 3 factors—technology, raw materials and capital. Out of these 3 factors, the technology development through ICT is perhaps the most important to make up for a deficiency in natural resources and reduce the high capital demand. India has achieved a distinctive position for itself in developing ICT based solutions and ICT enabled services and have created a strong skill base. Now, we need to ensure to utilize this technology to the best of our capability and have to ensure that this capability is not misused.

If we look at the National connectivity figure, it is very encouraging ,Tele Density of the Country which was 0.8 % in 1995 (all fixed lines and no mobiles) has reached 39.86 per cent in June 2009. The wireless (GSM and CDMA) segment adds almost 10 to 12 million new subscribers each month,with ours being the 2nd largest cellular mobile phone network in the world and the Broadband connections have reached 6.4 million at the end of May while the total number of licences issued for Internet service providers (ISPs) is 375, under the Bharat Nirman programme, public telephones were provided to 264 villages in May 09 In the Internet/Web arena, we have of at the end of May 2009, 11 million people in the country who have access to the Internet with, 6.4 million broadband internet users, There are two million domain addresses and this numbers is going up. We can now host ".com" servers in the country, unlike few years ago where ".com" servers meant it is somewhere in U.S.A.

The Computer networks are increasingly becoming an essential part of our daily life. Today we are pumping somewhere around 70 gigabyte of Internet bandwidth. Different submarine cables are installed linking the country to carry traffic out of the country, in fact every submarine cable in the world, want to connect India on their network.

We are talking about 10 million broadband connections by the year 2010. The Internet has also been spreading at a reasonably fast pace and the urban society is quite Net savvy The concept of a connected society is getting a shape.

The information and communication technologies of the 1990s which triggered the growth of telephony also enabled us to develop enough intelligence to integrate the 'islands' of information irrespective of Banner, Boundary and Border. One of the important outcomes was the evolution of Internet. Because of the Internet, any information, residing on any computer in any corner of the world is just a click away.

With a very large teledensity and rural connectivity increasing rapidly we are marching towards a reasonably connected Nation, but there is need for caution in the light what the country has recently witnessed havocs caused by nature and holocaust, perpetrated by terrorists and anti social elements. Such calamities and rising threats have heightened need for organized measures to prevent lapses in national security, once such situation arises. There is a concern for security throughout the world, e-safety and security systems and devices are more relevant today than ever before when cyber crimes are on the rise .With human safety being the top priority the world over, research and development in the field of safety sensors, RDX sensors, fire sensors, explosives detectors, CCTVs etc. have become very important. Likewise modern Communication System and Interactive Multimedia devices are need of the hour. there is need to correctly channel our ICT capabilities the face these Natural and manmade challenges. IETE has chosen the theme of its 52nd Annual Technical Convention on " Technology & Terror – Role of ICT in War against Terror".

On the eve of the convention we bring out a special publication which is a compilation of a number of papers specially written by experts to discuss different aspects of the theme which can provide orientation for deliberation in the convention.

We have got very encouraging response and have received a large number of papers which deliberate different aspects of the theme. Due to paucity of space we have selected only15 paper which are being published in this special issue. I take this opportunity to thank all the authors for their efforts and hope that their contribution will meet the requirement for bring out this issue .

With the aim to explore the best possible solution for fighting terrorism and also to bring together experts in technologies of IT Telecom and broadcasting, as well as related business, on a common platform. The convention shall provide an ideal forum for professionals in the field ICT to share their thoughts and interact.

P N Chopra
DIG BSF(Retd)

Overview

The United Nations Organisation (UNO) through its organ -ITU is constantly busy in the developmental activities of human race using the power of ICT. On the other hand the world of terrorism is engaged in its global terrorism- destruction of mankind and its creations. India has been raising this alarm in the international forum for quite sometime. But the world attention was focussed to this issue only after the devastating terror attack of 9/11 in the USA. ITU has been working on this important issue through its various Study Groups and disseminating the knowledge to the member nations- as to how to proceed to handle the menace of global terrorism.

Considering the extraordinary importance of the subject, IETE considered it necessary to have a focussed deliberation on various aspects concerning use of ICT in our march to 'War Against Terror' and the same has been chosen as the theme of the '52nd ATC-2009' of IETE. A special publication of IETE on this subject has been brought out in commemoration of this '52nd ATC-2009' which contains the thoughts and visions of a wide spectrum of experts in the field.

Cybercrime is one of the very prominent act of global terrorism. Measures to be taken to handle this crime, have been dealt with in a number of articles. Crisis Management through use of ICT is another important issue which has also been presented. We have various agencies dealing with intelligence matters. But due to lack of proper co-ordination among these agencies, the final result is not positive. So a centralized command and control system, synergy of efforts of the agencies is the key to success in meeting the challenges arising out of to-day's terrorism. This has been elaborated in the presentation.

Importance of surveillance system, cryptography and near real time search and identification from a large distributed data base is a challenging task. The proper instrumentation with appropriate sensing devices in the surveillance system for monitoring terror attacks is at the core of early warning and corrective measures. These subjects have been dealt with in papers from experts. Moving further a detail account on the trends in 'Remotely Controlled Improvised Explosive Device' (RCIED) and the role of counter RCIED equipment to defeat the actions of the RCIED's – has been presented.

The details of a system – 'Terrestrial Trunked Radio' (TETRA) has been presented. TETRA provides challenging communication tasks and applications like - High secure communications; Simultaneous voice and data transmission ; Priority channel override; GPS and GIS applications for vehicle tracking and Picture and video applications ; etc. This also provides integration with existing VHF and land line communication links .

World Radio Conference (WRC-2003) of ITU paved the way for deployment of new technologies for Wide Band (384 Kbps – 500 Kbps) and Broad Band (1 – 100 Mbps) public protection and Disaster Relief applications. Harmonisation of communication spectrum is important for - international interoperability of equipment, increased spectrum efficiency, increased effective response to disaster relief besides the economy of scale in equipment manufacture, etc. This spectrum issue has been highlighted in the presentation. Beside the above, an article giving a conceptual system required to be designed/deployed and necessary recommendations to frustrate the acts of terrorism; has been presented.

Importance of Reinforcement of R&D in Intelligence wing; Role of Broadcasting; Need for a dedicated communication and surveillance network; Importance of Spectrum, Legal and Regulatory framework and the ITU activities in the related fields of Security and Disaster Management have been brought out.

On behalf of IETE, I thank the authors of all the articles presented in this Special Publication of IETE for sharing their very valuable knowledge and vision on this important subject. I believe the contents of this publication will enrich and empower the readers with knowledge on this special subject of global concern.

K M Paul

ICT in Crisis Management
Man and Technology – Bridging the Gap

Brig X P Adrinyanwala (Retd.)

Abstract

In today's world hardly any issue gets greater attention and concern of the international community than the question of how to respond to terrorist attacks and the security threat that they pose. Globalisation has further made such concerns universal. In our interconnected world, security is increasingly indivisible and transcends national borders and organisational boundaries.

Crisis emanating from terrorism is a reality and here to stay. Whereas Security forces always seem to fight the previous war, the disruptive elements of society always do it differently the next time, no two attacks are the same. After every terrorist incident we hear the oft repeated lament about the lack of intelligence. Data and intelligence are available in plenty; the drawback is its effective analysis and dissemination to the right stakeholders. It is a reality today that there is an information overflow resulting in an intelligence white out.

Recent terror incidents, particularly the 26/11 attack in Mumbai, have shown that in the field of crisis management a great number of agencies confront the same problems but lack a sure or consistent knowledge, coordination or communication technology or user culture. As a result, the different organisations work wastefully, on the same problems, plan and take decisions without consulting with one another or without access to up-to-date or adequate knowledge. There is also a need to achieve a great conceptual coherence about the overall strategy and goals of the crisis management mission at the civilian/military/security forces interface.

Modern ICT is a key enabler to many of these objectives. ICT allows holistic and seamless integration of multiple agencies in crisis management. A word of caution though, ICT is a small part of a complex organisation consisting primarily of humans. Technology, as such, is hardly a driver of organisational change, but it can provide decisive support for the organisation's information management and communication strategy resulting in a new kind of thinking on the tools of overall work. A truly effective ICT architecture seamlessly blends man and machine into a networked whole.

Preview

A discussion in the use of ICT in crisis needs to include the major stake holders in the security and crisis management paradigm, these are:

- The Nature of Crises.
- The man behind the gun – the user.
- Use of ICT by public and private organisation in the war on terror
- Denying the use of ICT to disruptive non-state actors

The Nature of Crises

In today's world, the main threat to states and organisations, no longer comes from other states. Instead, it comes from small groups and other organisations which are not states. Either we make the necessary changes and face them today, or in the future the modern world will lose all sense of security and will dwell in perpetual fear. Meanwhile, for the past several years, terrorism experts have broadly concurred that this phenomenon will persist, if not get worse and develop into various scenarios.

The war on terrorism is not necessarily a war in a traditional sense, but a mixture of kinetic warfare and a war about ideas and ideals. Contemporary terrorism is a complex phenomenon involving a range of interstate actors linked in a networked organisation. All these entities pose security threats to a nation as well as to the collective regional and global security.

This manner of warfare has necessitated changes in organisation, doctrine, strategy, and technology that, taken together, point to the emergence of a "new terrorism" attuned to the information age. The furure target of terrorism will be ICT.

The Man behind the Gun

A major flaw in the International Community's approach to date has been to leave ICT issues to IT departments without proper guidance on what we want to achieve. It should be the leaders and the victims who decide what data and information we need. IT specialists need to facilitate these information and knowledge flows and not act as gatekeepers. The problem is not in technology per se but in organisation, leadership and resources. Senior management need to be more involved in ICT and information-related issues, both at headquarters and in the field. Current levels of disengagement reflect the low value attached to information – it is seen as a cost, rather than an investment.

Technology in itself has limited use unless used by trained operators. As all engineers would know, technologically almost anything is achievable; but the user has to decide as to what it is that he really needs. Can an average practitioner use it and what is the level, duration and type of training required to allow the person to use it instinctively during crisis. The important aspects of the use of ICT by operational practitioners are:

- Training to users, especially for rapid response to emergencies, must be more realistic and more frequent. Training must endeavour to make users reach a level of instinctive usage, where in an incident he can employ a system without diverting attention from his primary task.

- Training must be based in local contexts and in realistic foreseeable situations. Training should provide exposure to future envisaged realities, here it is important to note that most security forces "fight the last war". It is important to develop an ICT architecture that has inherent flexibility to handle diverse situations.

- Teams must learn how to work together in a smooth inter-agency collaboration. Effective ICT can only succeed in the environment of organisational harmony.

Use of ICT by Public and Private Agencies in the War against Terror

There is no gain saying the fact that ICT is a vital ingredient in an organisation fighting terror. However, very few states and organisations have really come to grips with this important aspect. There are no organised methods for various actors and stakeholders to interact on a common network; resulting in wasteful energy where multiple agencies address the same problem.

Ideally, there is a need for a Wikipedia type of structure which will enable the cooperation between various elements of organisation using a trusted info sharing environment supported by an up-to-date technology. ICTs must adapt to emerging situations and in the war against terror and when handling terror related crisis, there is need for ICTs to be fixed and mobile. There are many systems today that enable building a common operational picture by bringing operations and intelligence data together in one place. This facilitates collaborative operational planning, allowing various users to achieve comprehensive situation awareness.

Capabilities of an Effective ICT. In crisis management such a system should enable at least the following:

- Custom mapping capabilities.

- Easy to use tools, both in hardware and software.

- Standardised report formats.

- Shared security incident data presented on digital maps and in narrative formats.

- Evacuation and emergency response planning tools.

- Personnel accountability.

- Radio room tools.

- Location monitoring.

Principles of Employment. Some of the important principles in the employment of ICT in crisis management and combating terror are as given below:

- **Accessibility** of various stakeholders, agencies and organisations which are involved in operations.

- Information management and exchange should be based on a system of **inclusiveness** which implies two way communication, partnership and sharing with a high degree of participation and ownership by multiple stakeholders.

- **Inter-operability** to ensure that all sharable data and information is available in formats that can be retrieved, shared and used by various agencies involved.

- Information providers should be **accountable** to their partners and stakeholders for the accuracy of the contents they publish and disseminate.
- **Verifiability** means that the information

provided is accurate, consistent and validated by external sources.

- Information collected and put on such a network should **relevant**.

- It is important to provide information in a **timely** manner.

System Redundancy and Reliability. ICTs are generally designed to work in ideal conditions, often failing in the harsh environment of counter terror operations. The system architecture should be such that there should be adequate redundancy in the system to enable all or essential functions to work even if substantial portions of the network have failed. Reliability in operations requires that the following five essentials are present in the employment of ICT:

1) Reliable voice and data communication which is regularly tested.

2) Standard processes and the operator's capability in using systems available.

3) Practical training in field conditions to gain full proficiency in the use of ICTs.

4) Crisis managers need to be familiar and proficient with ICTs to include current technology development. It is not advisable to delegate full responsibility for ICT to a technical specialist.

5) The potential for GIS (Geospatial Information Service) for situational awareness and operational planning is enormous. However, there is a long learning curve and suitable process development required before a GIS solution is optimally operational.

ICT and Disruptive Elements

Media exposure is normally the primary goal of those carrying out terrorism, to expose issues that would otherwise be ignored by the media. Some consider this to be manipulation and exploitation of the media. Others consider terrorism itself to be a symptom of a highly controlled mass media, which does not otherwise give voice to alternative viewpoints, a view often expressed is that controlled media is responsible for terrorism, because "you cannot get your information across any other way".

With the advance in technology being available to disruptive elements also, there is likely to be paradigm shift in the waging of unconventional war in a form that for want of a better word should be labelled "new terrorism" attuned to the information age. If the new terrorism directs its energies toward information warfare, its destructive power will be exponentially greater than any it wielded in the past—greater even than it would be with biological and chemical weapons.

What has long been emerging in the business world is now becoming apparent in the organizational structures of net war actors. In an archetypal net war, the protagonists are likely to amount to a set of diverse, dispersed "nodes" who share a set of ideas and interests and who are arrayed to act in a fully internetted "all-channel" manner.

Some of the key characteristics in the use of ICT by non-state disruptive elements would be:

1) **Organisational**: Terrorists will continue to move their hierarchical organisation towards information age network designs within groups "Great Man" relationship will make way to a flatter decentralised business. More effort will come into building arrays of transnational interknitted groups rather than building stand alone groups.

2) **Doctrine and Strategy**: Terrorists are likely to gain new capability for lethal acts. Introduction to acts of physical violence, terrorists are more likely to move towards "Information Operation" for achieving their goals where systemic disruption may become as much an objective as target destruction.

3) **Technology**: Terrorists are likely to increasingly use advanced information technologies for offensive and defensive purpose as also to support their organisational structures.

A review of patterns and trends in the Middle East substantiates speculations that the new terrorism is evolving in the direction of net war, along the following lines:

- An increasing number of terrorist groups are adopting networked forms of organization and relying on information technology to support such structures.
- Newer groups (those established in the 1980s and

1990s) are more networked than traditional groups.

- A positive correlation is emerging between the degree of activity of a group and the degree to which it adopts a networked structure.
- Information technology is as likely to be used for organizational
- Support as for offensive warfare.
- The likelihood that young recruits will be familiar with information technology implies that terrorist groups will be increasing.

It is important to deny terrorist organisations the oxygen of publicity; to this effect certain restrictive rules regarding ICT may have to evolved and instituted. However it is pertinent to note that the aim of many anti-national movements is often to force the Government to enact such repressive laws causing the public to detest the Government for doing so. Thus it is important to ensure that any regulations or acts should be as unobtrusive as possible.

The mass media too will often censor organizations involved in terrorism (through self-restraint or regulation) to discourage further terrorism. However, this may encourage terror organisations to perform more extreme acts of terrorism to be shown in the mass media.

Conclusion

It is important to understand that ICT should not focus purely on technology as this can obscure organisational and process factors. ICT is not an end in itself but must be seen as a means to support strong and capable crisis management organisation.

The internet has created a new channel for groups to spread their messages. This has created a cycle of measures and counter measures by groups in support of and in opposition to terrorist movements. In fact, the United Nations has created its own online counter-terrorism resource.

Cybercrime: A growing threat

Kiran Bhandari

Abstract

Cybercrime is one of the fastest growing areas of crime, as more and more criminals exploit the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of crimes. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, and Internet auction fraud.

The global nature of the Internet allows criminals to commit almost any illegal activity anywhere in the world, which makes it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security.

1. Introduction

What ,is this Cyber crime? We read about it in newspapers very often. Let's look at the dictionary definition of Cybercrime: "It is a criminal activity committed on the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money".

2. CYBERCRIMES CAN BE BASICALLY DIVIDED INTO 3 MAJOR CATEGORIES:

- Cybercrimes against persons.
- Cybercrimes against property.
- Cybercrimes against government.

2.1 Cybercrimes against persons : Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

A minor girl in Ahmedabad was lured to a private place through cyberchat by a man, who, along with his friends, attempted to gangrape her. As some passersby heard her cry, she was rescued.

Another example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers. worldwide. In the United States alone, the virus made its way through 1.2 million computers in one-fifth of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug".

2.2 Cybercrimes against property : The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyberspy.

2.3 Cybercrimes against government : The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

In a report of expressindia.com, it was said that internet was becoming a boon for the terrorist organisations. According to Mr. A.K. Gupta, Deputy Director (Co-ordination), CBI, terrorist outfits are increasingly using internet to communicate and move funds. "Lashker-e-Toiba is collecting contributions online from its sympathisers all over the world. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathisers and also using the medium for intra-bank transfer of funds".

Cracking is amongst the gravest Cyber-crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

Coupled with this the actuality is that no computer system in the world is cracking proof. It is unanimously agreed that any and every system in the bay, Yahoo, Amazon and others are a new category of Cyber-crimes which are slowly emerging as being extremely dangerous.

3. PROMINENT TYPES OF CYBERCRIMES

3.1 Phishing : This is a high-tech scam that uses spam or pop-up messages to deceive consumers into disclosing their card numbers, bank account information, social security numbers, passwords, or other personal information. Phishers send an email or pop-up message that claims to be from a business or organization that you deal with — for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your personal information, such as user names, passwords, credit cards, social security numbers, and bank accounts.

3.2 Spoofing : In this scam, the spoofer creates a false or shadow copy of a real website or email in a way that misleads the recipient. All network traffic between the victim's browser and the shadow page are sent through the spoofer's machine. It allows the spoofer to acquire personal information, such as passwords, credit card numbers, and account numbers.

3.3 Spam : Spam is a term for the sending of unsolicited bulk email. Unsolicited means the recipient has not granted verifiable permission for the message to be sent. Bulk means the message is sent as part of a larger collection of messages, all having substantively identical content. With improved technology and world-wide Internet access, spam is now a widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others.

3.4 Hacking : Hacking is the illegal access by unknown and unauthorized party(s) to a computer system to destroy or disrupt the system or to use it to world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E- carry out illegal activities.

3.5 Spyware : Spyware is software that collects personal information from your computer without your knowledge. It can look at which sites you're visiting or access information like usernames and passwords. What's worse, it can send this information to a third party without you knowing it. The software may also perform several different unwanted functions, including the delivery of pop-up ads or harvesting private information. It can serve up inappropriate ads to you and your children, and can seriously slow your computer down, as it attempts to run spyware processes instead of the programs you are trying to use.

3.6 Identity Theft: Identity theft is a criminal offense : It occurs when a person knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law.

4. MEASURES TO BE TAKEN FOR SECURITY

A broad, inclusive focus is necessary to address problems of cybercrime, going beyond criminal law, penal procedures and law enforcement. The focus should include requirements for the secure functioning of a cyber-economy optimizing business confidence and individual privacy, as well as strategies to promote and protect the innovation and wealth-creating potential and opportunities of information and computing technologies, including early warning and response mechanisms in case of cyber attacks. Behind the prevention and prosecution of computer-related crime looms the larger challenge of creating a global culture of cyber security, addressing the needs of all societies, including and protection of cyberspace so that it is not abused or exploited by criminals or terrorists. In particular, the United Nations system should be instrumental in advancing global approaches to combating cybercrime and to procedures for international cooperation, with a view to averting and mitigating the negative impact of cybercrime on critical infrastructure, sustainable development, protection of privacy, e-commerce, banking and trade.

All States should be encouraged to update their criminal laws as soon as possible, in order to address the particular nature of cybercrime. With respect to traditional forms of crime committed through the use of new technologies, this updating may be done by clarifying or abolishing provisions that are no longer completely adequate, such as statutes unable to address destruction or theft of intangibles, or by creating new provisions for new crimes, such as unauthorized access to computers or computer networks. Such updating should also include procedural laws (for tracing communications, for example) and laws, agreements or arrangements on mutual legal assistance (for rapid preservation of data, for example). In determining the strength of new legislation, States should be encouraged to be inspired by the provisions of the Council of Europe Convention on Cybercrime.

Governments, the private sector and non-governmental organizations should work together to bridge the digital divide, to raise public awareness about the risks of cybercrime and introduce appropriate countermeasures and to enhance the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. For this purpose, national judicial administrations and institutions of legal learning should include comprehensive curricula on computer related crime in their teaching schedules. Cybercrime policy should be evidence-based and subject to rigorous developing countries, with their emerging and still vulnerable information technology structures.

International cooperation at all levels should be developed further. Because of its universal character, the United Nations system, with improved internal coordination mechanisms called for by the General Assembly, should have the leading role in intergovernmental activities to ensure the functioning evaluation to ensure efficiency and effectiveness. Therefore, concerted and coordinated efforts at the international level should be made to establish funding mechanisms to facilitate practical research and curb many types of newly emerging cybercrime. It is, however, equally important to ensure that research be internationally coordinated and that research results be made widely available.

5. FIVE PILLARS FOR SECURITY

The GSI sets out a new approach to address the challenges of 21st century security, focusing on five pillars that are vital to INTERPOL's role in enhancing the safety of citizens globally.

These build on the Organization's current priorities and underpin a framework of far-reaching future activities. These five pillars are:

5.1 Global Security through Enhanced Information Sharing and Connectivity : INTERPOL's communications systems, databases and analysis have consistently proven their value in addressing our most pressing global threats. We now need to extend the quantity and availability of information to the law enforcement community, and develop programmes and tools that focus on securing physical and virtual borders.

5.2. Secure Global Infrastructure : Advances in information and communications technology have brought huge personal and economic benefits, but a crucial commitment to online security must be met: the commitment to protect citizens and businesses online to the same extent as we protect them in their communities and on the streets. Countering the misuse of technology will require the involvement and expertise of the companies and individuals who invented it. INTERPOL will serve as the strategic link between public and private interests committed to developing ways to combat the cyber-security threat.

5.3. Global Law Enforcement Capacity : There is a pressing need to help countries that lack the financial, technical and human resources needed to address today's law enforcement challenges. INTERPOL's aim is to provide the right training and tools to law enforcement bodies around the world. We need to empower our National Central Bureaus as the focus for international police co-operation within their countries and tailor our services to the needs of member countries.

5.4. Strategic Global Partnerships : Today's security challenges require significant funding if they are to be tackled effectively. INTERPOL cannot rely on member country contributions alone to meet the growing global security need. Public and private partnerships and investments are essential if our strategic vision is to be realized.

5.5. Innovation : We must actively involve our global membership, academia and strategic thinkers in the world of law enforcement in shaping our future. By encouraging innovative thinking we can create an environment for success, conducive to delivering cutting-edge crime-fighting tools, technology, and a strategy to combat 21st century crime.

6. CONCLUSION

This paper has provided various resources to help individual to have a better understanding of the different type of threats to the computer or networking systems and what you can do to protect self. Measures at Individual level are not enough to prevent cybercrimes. Global law enforcement through enhanced information sharing and connectivity is the need of the day.

7. REFERENCES

http://asianlaws.org
http://hoaxbusters.ciac.org
http://vil.mcafee.com/newVirus.asp
http://vil.mcafee.com/hoax.asp
http://www.stiller.com/hoaxa.htm
http://www.snopes.com

About Author

Shri Kiran Ashok Bhandari (DoB 4th July 1978), has completed his Degree in Electronics Engineering in 1999 with first class. After working as Asst. R&D Engineer for nearly two years he completed his Masters in Electronics Engineering from SGGS COE Nanded in 2003. He scored 72.4% and secured second rank in the class. He has presented 2 papers at reputed conferences and conducted and participated various STTPs in his area of interest in Image Processing. He has more than 8 years of teaching experience at renowned Engineering colleges in Mumbai. Presently he is working as Asst. Prof. and Deputy HOD in CMPN Dept. at TCET Kandivali(E).

Contact

e-mail : kiran.bhandari@thakureducation.org
Mobile : 09320631501

Advanced Public Safety Communications : An Important Breakthrough by ITU : Harmonized Spectrum for Public Protection and Disaster Relief (PPDR)[1]

Bharat Bhatia

Abstract

A major milestone was reached at the World Radio Conference (WRC-2003) convened by the Geneva based UN specialized agency for telecommunications, the International Telecommunications Union (ITU),) with the approval of a new Resolution that will pave the way for the deployment of new technologies for wideband and broadband public protection and disaster relief applications. At present, public protection and disaster relief applications are mostly narrow-band supporting voice and low data-rate applications, typically in channel bandwidths of 25 kHz or less. It is anticipated that many future applications will be wideband-based (with data rates in the range of 384-500 kbit/s) and/or broadband-based (with data rates in the range of 1-100 Mbit/s).

Future Advanced Solutions for PPDR will have voice, data,graphics and video capabilities

As PPDR operations become more reliant on electronic databases and data processing, access to accurate and detailed information by staff in the field such as police, firefighters and medical emergency personnel is critical to improving the effectiveness of the staff in resolving emergency situations. This information is typically held in office based database systems and includes images, maps, architectural plans of buildings, and locations of hazardous materials systems.

In the other direction, the flow of information back from units in the field to operational control centers and specialist knowledge centers is equally important. Examples to note are the remote monitoring of patients and remote real-time video monitoring of civil emergency situations including the use of remote control robotic devices. Moreover, in disaster and emergency situations, critical decisions to be made by controlling authorities are often impacted by the quality and timeliness of the information received from the field. These applications in general require higher bit-rate data communications than can be provided by current PPDR applications. The availability of future advanced solutions is expected to be of benefit to PPDR operations.

Advantages with future technologies

While voice communications will remain a critical component of PPDR operations, new data and video services will play a key role. For instance, PPDR agencies today use applications such as video for surveillance of crime scenes and of highways, to monitor and conduct damage assessment of wild land fire scenes from airborne platforms to provide real-time video back to emergency command centers. Also, there is a growing need for full motion video for other uses such as robotic devices in emergency situations. These types of future advanced solutions will be capable of providing local voice, video and data networks, thereby serving the needs of emergency personnel responding to an incident. If these future technologies were implemented globally, it could reduce the cost of equipment, increase availability of equipment, increase potential for interoperability, may provide for a wider range of capabilities and reduce network infrastructure rollout time. Introduction of these technologies may enable PPDR agencies and organizations to keep up with increasing demands but also may enable them to implement advanced voice, text, video and other intensive data applications and services designed to enhance service delivery. In this regard, it should be noted that any development or planning for the use of future technologies may require that consideration be given to spectrum aspects for PPDR applications.

Narrowband, wideband, broadband

Communications supporting PPDR operations cover a range of radiocommunication services such as fixed, mobile, amateur and satellite. Typically, narrowband technologies are used for PPDR communications within the terrestrial mobile service, while wideband and broadband technologies are finding PPDR applications within all radiocommunication services.

Narrowband (NB)

To provide PPDR narrowband applications, the trend is to implement wide area networks including digital conventional and trunked radio networks providing digital voice and low speed data applications (e.g. pre-

[1] In ITU terminology the term PPDR is used to denote all Public safety and disaster related communications.

defined status messages, data transmissions of forms and messages, access to databases). ITU Report ITU-R M.2014 lists a number of technologies, with typical channel bandwidths up to 25 kHz, that are currently used to deliver narrowband PPDR applications. Some countries do not mandate specific technology, but promote the use of spectrum-efficient technology.

Wideband (WB)

It is expected that the wideband technologies will carry data rates of several hundred kilobits per second (e.g. in the range of 384-500 kbit/s). It is expected that networks and future technologies may require higher data rates, a whole new class of applications including: wireless transmission of large blocks of data, video and Internet protocol-based connections in mobile PPDR may be introduced. The use of relatively high-speed data in commercial activities gives a wide base of technology availability and will therefore spur the development of specialist mobile data applications. Short message and e-mail are now being seen as a fundamental part of any communications control and command system and therefore could most likely be an integral part of any future PPDR capability. A wideband wireless system may be able to reduce response times of accessing the Internet and other information databases directly from the scene of an incident or emergency. It is expected that this will initiate the development of a range of new and secure applications for PPDR organizations. Systems for wideband applications to support PPDR are under development in various standards organizations.

Broadband (BB)

Broadband technology could be seen as a natural evolutionary trend from wideband. Broadband applications enable an entirely new level of functionality with additional capacity to support higher speed data and higher resolution images. It should be noted that the demand for multimedia capabilities (several simultaneous wideband and/or broadband applications running in parallel) puts a huge demand with very high bit rates on a wireless system deployed in a localized area with intensive on-scene requirements (often referred to as "hot spot" areas) where PPDR personnel are operating. Broadband applications could typically be tailored to service localized areas (e.g. 1 km^2 or less) providing voice, high-speed data, high quality digital real time video and multimedia (indicative data rates in range of 1-100 Mbit/s) with channel bandwidths dependent on the use of spectrally efficient technologies. Examples of possible applications include:

1) high-resolution video communications from wireless clip-on cameras to a vehicle-mounted laptop computer, used during traffic stops or responses to other incidents and video surveillance of security entry points such as airports with automatic detection based on reference images, hazardous material or other relevant parameters;

2) Remote monitoring of patients and remote real-time video view of the single patient demanding up to 1 Mbit/s. The demand for capacity can easily be envisioned during the rescue operation following a major disaster. This may equate to a net hot spot capacity of over 100 Mbit/s.

Broadband systems may have inherent noise and interference tradeoffs with data rates and associated coverage. Depending on the technology deployed, a single broadband network may have different coverage areas in the range of a few meters up to hundreds of meters, providing a wide range in spectrum reuse capability. Collectively, the high data speeds and localized coverage area open up numerous new possibilities for PPDR applications (Tailored Area Networks, hot spot deployment and ad-hoc networks).

Harmonization of spectrum

Significant amounts of spectrum are already in use in various bands in various countries for narrowband PPDR applications, however, it should be noted that sufficient spectrum capacity will be required to accommodate future operational needs including narrowband, wideband and broadband applications. Experience has shown that spectrum that is harmonized has benefits that include economic benefits, the development of compatible networks and effective services and the promotion of interoperability of equipment internationally and nationally for those agencies that require national and cross-border cooperation with other PPDR agencies and organizations. Specifically, some potential benefits are as follows:

- Economies of scale in the manufacturing of equipment;
- Competitive market for equipment procurement;
- increased spectrum efficiency;
- stability in band planning, that is, evolving to globally/regionally harmonized spectrum arrangements may assist in more efficient planning of land mobile spectrum; and
- increased effective response to disaster relief.

When considering appropriate frequencies for PPDR, WRC-03 recognized that the propagation characteristics of lower frequencies allow them to travel farther than higher frequencies, making low frequency systems potentially less costly to deploy. Lower frequencies are also sometimes preferred in urban settings due to their superior building penetration.

The more bands that may be identified with different propagation characteristics the more difficult it becomes to benefit from economies of scale. Therefore, a balance needs to be struck between the number and location of the bands identified.

Based upon an international survey of PPDR communications conducted in the 2000-2003 study period from over 40 ITU members and international organizations and consequent considerations, ITU has noted:

a) There is little uniformity in regard to frequency bands that are used for PPDR in different countries.

b) While in most countries the bands used for public protection are the same as those used for disaster relief, in some countries separate bands are used.

c) Many administrations have designated one or more frequency bands for narrowband PPDR operations. It should be noted that only particular sub-bands of the frequency ranges or parts thereof listed below are utilized in an exclusive manner for PPDR radiocommunications: 3-30, 68-88, 138-144, 148-174, 380-400 MHz (including CEPT designation of 380-385/390-395 MHz), 400-430, 440-470,764-776,794-806, and 806-869 MHz (including CITEL designation of 821-824/866-869 MHz). One administration has designated PPDR spectrum for wideband and broadband applications.

d) Some administrations in Asia are using or plan to use or have identified parts of the frequency bands 68-88 MHz, 138-144 MHz, 148-174 MHz, 380-399.9 MHz, 406.1-430 MHz and 440-502 MHz, 746-806 MHz, 806-824 MHz and 851-869 MHz for PPDR applications. Some administrations in Region 3 are also using the bands 380-399.9 MHz, 746-806 MHz and 806-824 MHz paired with 851-869 MHz for Government communications.

Therefore WRC 2003 resolution on PPDR notes that currently the bands 3-30, 68-88, 138-144, 148-174, 380-400 MHz (including CEPT designation of 380-385/390-395 MHz), 400-430, 440-470, 764-776, 794-806 and 806-869 MHz (including CITEL designation of 821-824/866-869 MHz). or parts thereof have been designated for public protection and disaster relief operations, as documented in ITU Report ITU-R.M.2033;

With regards to future advanced solutions for PPDR, WRC-03 resolution encourages administrations to consider the following identified frequency bands/ranges or parts thereof when undertaking their national planning:

- **Europe, Middle East and Africa:** 380-470 MHz as the frequency range within which the band 380-385/390-395 MHz is a preferred core harmonized band for permanent public protection activities within certain agreed countries of Region 1.
- **The Americas:** 746-806 MHz, 806-869 MHz, 4 940-4 990 MHz.
- **Asia:** 406.1-430 MHz, 440-470 MHz, 806-824/851-869 MHz, 4 940-4 990 MHz and 5 850-5 925 MHz (some countries in Region 3 have also identified the bands 380-400 MHz and 746-806 MHz for public protection and disaster relief applications).

Administrations are urged, through this Resolution, to use regionally harmonized bands for public protection and disaster relief to the maximum extent possible, taking into account the national and regional requirements and also having regard to any needed consultation and cooperation with other concerned countries. They are further called upon to encourage public protection and disaster relief agencies and organizations to utilize relevant ITU-R Recommendations in planning spectrum use and implementing technology and systems supporting public protections and disaster relief.

The WRC-03 resolution also clearly resolves that the identification of the frequency bands/ranges for future advanced solutions to meet the needs of public protection and disaster relief does not preclude the use of nor establish priority over any other frequencies for public protection and disaster relief in accordance with the Radio Regulations.

Further, the ITU-R will continue its technical studies and make recommendations, as necessary, to meet the needs of public protection and disaster relief radiocommunication applications. Such studies would also take account of any resulting transition requirements of the existing systems, particularly those of many developing countries, for national and international operations.

Contact

An ideal ICT Setup to Combat Information Terrorism

P N Chopra, DIG, BSF (Retd)

Abstract

Information communication technology (ICT) is revolutionizing the world. Besides making communications and availability of information easy, it is also an index of the growth of a country and to our good luck India is advancing well in all facets of ICT. Besides the good that it is doing, it is also throwing up challenges related to security. We have to be alive to these challenges. A centralized command and control system and synergy of effort amongst the intelligence agencies is the key to facing up to these challenges. Analysis of information related to computer crimes is becoming important hence besides extraction of digital evidence, correct analysis of the same, to connect the crime with the criminal and provide appropriate leads in investigation, is absolutely necessary.

General

Information communication technology (ICT) is revolutionizing the world. Besides making communications and availability of information easy, it is also an index of the growth of a country and to our good luck India is advancing well in all facets of ICT. This is contributing in a significant manner to the national economy. The IT sector is contributing in the area of software development and other IT based solutions not only for the national consumption but for export to other countries and this is one area where we have a marked edge over China. Besides the good that ICT is doing, it is also throwing up challenges related to security. We have to be alive to these challenges.

Internet

In the Internet/Web arena, 11 million people in the country who have access to the Internet with 6.4 million broadband connections at the end of May 2009. There are two million domain addresses and this number is going up. The total number of licenses issued for Internet Service Providers (ISPs) is 375. We can now host ".com" servers in the country, unlike a few years ago when "com" servers meant it is U.S.A only. Lot many services or lot many web hosting services are shifting to our country with a large number of players in this field.

Computer networks are increasingly becoming an essential part of our daily life. Today we are pumping somewhere around 70 gigabyte of Internet bandwidth. Different submarine cables are installed linking the country to carry traffic out of the country; in fact the world wants to connect India on their submarine cable networks. Internet traffic used to be America-centric till about 5 years ago. The same is no longer happening as agencies in America are now indicating that flow of data pattern is changing. Americans are engaged in devising ways and means to arrest this trend. We already have VoIP and IPTV is coming up. There are some 134 plus active ISP's in the country and we are talking of about 10 million broadband connections by the year 2010. Internet has been spreading at a reasonably fast pace and the urban society is quite net savvy.

Telecom Sector

Now let us look at the Telecom Sector the other component of ICT, The national picture is very encouraging, India's telecom industry continued its robust growth story in June 2009 by adding 11.91 million new subscribers to take the total subscriber base to 464.82 million. Tele density of the country *which was 0.8 % in 1995* (all fixed lines and no mobiles) reached 39.86 per cent in June 2009 as compared to 28.33 per cent in the same period last year, India is thus the world's fastest-growing mobile phone market.

The two cities Delhi and Mumbai have 45.67 million mobile phone customers or 5.28% of India's 286.86-million mobile phone customers. The growth is poised to continue through the forecast period, and India is expected to remain the world's second largest wireless market after China in terms of mobile connections. Telecommunications is powerful vehicle for achieving sustainable economic growth and social empowerment.

Under the Bharat Nirman programme, public telephones were provided to 264 villages in May this year. The contribution of cellular mobile phones, to this performance is significant as we have the second largest mobile subscriber base with about 140 operational networks, with investments of around Rs. 150,000 crores. Currently mobile phones are covering almost 75% of population & about 50% of geographic area. The rural subscriber base is also growing at around 3 million every month, India's cellular services market is projected to surpass $37 billion by 2012, and the nation's mobile subscriber base is also set to exceed 737 million connections also by 2012, growing at a CAGR of 21 per cent during the same period.

ICT Implications

Though the National ICT scenario is bright it is also vulnerable to negative influences, some of which can have serious ramifications. As we are aware, computers and communications can be misused by undesirable elements both for petty crimes as well as for heinous terrorist activities, the recent terrorist attack in Mumbai is an example of this. ICT is therefore a conduit for nefarious activities. With the number of internet users going up there are an upward surge in the number cyber crimes in the country from the low end ones like exchange of MMS amongst students to defame a fellow student and simple extortion to the high end ones like complicated trans national money laundering. We have been recently reading with interest the use a Wi-Fi connection of a computer user in Mumbai for sending a spam mail for committing a terror attack.

The present digital multimedia revolution has provided an avenue of teleshopping and ordering goods via internet as also conducting financial transactions via internet by using credit and debit cards. This opens up another avenue for cyber crimes in the country. We need to ***understand*** the gravity and the need of cyber security. With the rapid advancement in the country in respect of extensive use of on line services and popularizing of tele banking which though very useful also carry a great risk factor with it the concomitant risks of cyber crimes. Technology particularly in the field of ICT is changing fast. We can appreciate that we are a fairly connected society but concurrently anti-social activities are also on the rise following adoption of modern technology and new ICT Systems.

Some times back NASSCOM estimated that about $7-8 billion worth of work may not have come to India because of security concerns among clients. Today, clients are convinced about delivery of IT and BPO services from India, but security concerns loom large in any discussion around off shoring IT services and BPO work to India. Even though as per a senior functionary of NASSCOM "Security issues are being used as an excuse not to offshore work to India," we cannot ignore the issue.

Earlier wars were fought between two countries on the border; this has given way in recent times to stoking of insurgencies, which then bring terrorism in their wake, causing serious damage to life and property. This new form of threat is a national challenge in general and in particular to the professionals in the field of ICT. Recent strikes of terror the world over have changed national priorities in many countries. National Governments are pondering over augmenting safety and security systems and putting minds individually and jointly to combat such terror activities by modernizing the ICT Systems apart from other measures. It is in this context that the need for modern communication systems and interactive media systems becomes relevant.

Issues

The few salient issues which need to be analyzed in this context are. How secure are we in this information age? How to catch a computer criminal who leaves no trace of evidence? How to combat a computer crime?, How to collect digital evidence and how to analyze this type of evidence. No universally accepted mechanism has yet been established for handling such crimes and such situations; in terms of searching, seizing, analyzing the digital evidence and finally brings the computer criminal so identified to book.

Ideal ICT Setup

What then is the ideal ICT set up, which will help us combat terrorism effectively? The important components and related aspects required to make such a set up effective are.

Centralized Command and Control : The first and foremost is a centralized command and control centre to coordinate actions of all agencies during anti-terror operations in case of a terror attacks. It has been observed that the lack of synergy among different forces tackling an emergency can result in the delay in eliminating terrorists, when they strike. In such situations if different agencies work in isolation it leads to under-utilization of available capability. There is a need to establish an integrated control room making use of available ICT devices to help share information and coordinate the activities of all the agencies involved in the conduct of operations.

Communications : It is also necessary to have state of the art communication systems for providing speedy response and interactivity in handling adverse situations to ensure safety of life and property. To this end the industry and research institutions needs to collaborate and develop a strategy to meet the connectivity requirements by optimally utilizing ICT to combat the menace of terrorism. The current advances in multimedia must be used to our advantage to counter security threats.

Intelligence Set up : There is also need for synergy among all intelligence gathering and disseminating agencies before and during anti-terrorist operations. After Kargil, in 1999, a comprehensive review of the intelligence set up in the country was undertaken. This included the work of the Saxena Committee which examined the state of the country's intelligence apparatus. The Committee's report pointed out the gaping holes that existed in the country's intelligence establishment, and made several recommendations to improve the system including up gradation of technical, imaging, signal, electronic counter-intelligence capabilities, and a system-wide reform of conventional human-intelligence gathering. Every suggestion in the Report was accepted by the Group of Ministers (GoM), in February 2001. However, the recommendations of the Report remain largely unimplemented. Given such circumstances, it is imperative that the intelligence effort is coordinated and collection and dissemination of intelligence from all available sources needs to be a concerted effort and the entire ICT facility needs to be utilized for the purpose.

Monitoring and Censor : Systems must be in place to curb the menace of miss-use of internet services. Terrorists in the Mumbai carnage, extensively used VoIP communication facilities for getting directions from their masters and such a facility could have been easily denied if we had in place measures to monitor such communication along with the wherewith all to deny this unauthorized connectivity. This is nothing uncommon as in the recent nation wide commotion in Iran after the election of the National president the Iranian government went all out to monitor all internet activity in the country and provide an effective control over all the internet traffic being exchanged in the country and thus exercised a tighter control over undesirable organizations. The Iranian regime has developed web spying services with the assistance of European telecommunications companies. This is one of the world's most sophisticated mechanisms for controlling and censoring the internet, allowing it to examine the content of individual online communications on a massive scale. This practice is often called deep packet inspection, which enables authorities to not only block communications but also to monitor them to gather information about individuals as well as alter it for disinformation purposes. We may not resort to such repressive measures but such systems are required to be in place for use when required for National purposes.

Forensic Analysis : Analysis related to computer crimes is becoming important hence besides extraction of digital evidence, correct analysis of the same, to connect the crime with the criminal and provide appropriate leads in investigation, is absolutely necessary. We must therefore train our personnel accordingly, in the fields of computer and network analysis.

Computer Forensics : Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics. The goal of computer forensics is to explain the current state of a *digital artifact.* The term digital artifact can include a computer system, storage medium (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network. The explanation can be as straightforward as "what information is here?" and as detailed as "what is the sequence of events responsible for the present situation?"

Network Forensics : Is the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities. Network forensics is basically about monitoring network traffic, determining if there is an anomaly in the traffic and whether the anomaly can be an attack. If it is an attack, the nature of the attack is also determined. Important aspects include traffic capture, preservation, analysis and visualization of the results. Forensic specialists will understand these results and will invoke an incident response immediately. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis when dealing with a skilled attacker.The goal of network forensics is, however, somewhat different when it is performed by law enforcement rather than security operations. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.

Conclusion : It's time the country demanded long-term strategic vision for war against terrorism from various stakeholders. War against terrorism is to be fought jointly and hence each and every citizen and organization involved should come to a common platform. The onus should not be put on the government alone but each and every citizen and organization must be vigilant and contribute to the effort, the government on its part must provide the wherewithal and also educate its citizens.

About Author

Shri P N Chopra, DIG, BSF(Retd), Managing Editor, Bitcom India, Consultant to reputed companies including Devas Multimedia, had helped World Space from concept to launch and getting regulatory support *for growth of service in India. After 39 years of uniform service joined corporate sector and steered an important telecom journal Telematics India for over 10 years.*

Founder Fellow & Former Secretary General, National Telematics Forum, Chartered Engineer. A Radio Engineer by profession having received training in Communication Engineering at Marconi (UK), Philips (Holland), Budavox (Hungary), Fellow Institution of Electronics and Telecommunication Engineers (IETE), Member : British Institute of Electronics and Radio Engineers, Fellow –Broadcasting Engineering Society, Senior Member- Computer Society of India, Life Member, Indian Science Congress Association. During the last 30 years he is associated with IETE in various capacities and presently he is Vice President of IETE for the year 2008-09 and Chairman, Technical Programmes Committee. As Deputy Inspector General, looked after Communication Policy and planning at BSF HQ.

Have been awarded a number of prestigious awards in recognition of meritorious service including Police Medal for Meritorious Services, President Medal for Distinguished Services & BSF Gold Medal with cash reward, for Scientific Innovations and many other cash awards.

Travelled extensively and visited a large number of communication establishments world over.

Contact

e-mail : bitcomin@nda.vsnl.net.in
digbsfpnchopra@yahoo.co.in
pnchopradigbsf@gmail.com

Mobile : 09891461144

Terror Hunt: Role of Technology in Spreading Awareness, Tracking, Trailing and Dynamic Crisis Management

Maj Gen Yashwant Deva, AVSM (Retd)

"The role of technology in supporting India's counter terrorism and internal security efforts was not being given adequate emphasis and there is need for greater investment in security technologies. Some of the areas where greater work is required are surveillance systems, cryptography, near real time search and identification from distributed large data bases and computer simulation exercises to enhance our crisis tactics and responses."

–Dr. Manmohan Singh, Prime Minister[1]

Introduction

The IETE conducted an Apex Forum on "Technologies for Combating Terrorism" at Kolkota on 14 February 2002, wherein I wrote the Background Paper for initiating discussions and formulating recommendations.[2] It is a widely read paper on the Web. Whereas the Americans and the Chinese digested and followed it in letter and spirit, we gave it a customary dismissive nod, as is our wont. In the concluding part, besides emphasising R&D, the paper contended that "terrorism is a war between technology and anti-technology. The former has a social purpose; the latter is merely theory and technique sans ethics and humanism. Technology has to be shared amongst the civilised nations. There is no room for denial regimes and sanctions."[3] And then Mumbai, another *ceteris paribus* tragedy, happened. We habitually kicked up a row and instead of getting down to brass-tacks, became embroiled in politico-legal commas, drafting goof-ups, and buck--passing. Alas! We once again failed to heed to technology as abundantly evident from PM's quote. There were sympathies galore; the Federal Bureau of Investigation (FBI) chipping-in a handful of intelligence too, but no sharing of technologies. That dispensation still went to the Inter Services Intelligence (ISI) of Pakistan, the long trusted ally in need, the ally indeed.

However, the IETE is destined to play a lead role in promoting technology to counter anti-technology. The burden has again fallen on us. Let us spread the word and awaken the decision makers through the current Annual Convention. This effort is a continuum of thoughts, earlier conveyed, albeit highlighting what others, the likes of US, are experimenting anew.

Information Communication Technology (ICT) and Total Information Awareness

ICT is the progenitor of myriad projects that focus on applying technology to counter terrorism, and other alike asymmetric threats to national security. The mission is to conceive, develop, and apply in an integrated and closed-loop fashion, information systems that achieve what is called in defence parlance *Total Information Awareness*. In the US, every year, billions of dollars are spent by agencies such as the Information Awareness Office (IAO), the National Security Agency (NSA), and the FBI, to develop and operate systems of the type Echelon,[4] NarusInsight,[5] Genoa,[6] Carnivore,[7] etc.to intercept and analyse voluminous data, and extract only that information which is pertinent to law enforcement and useful to the agencies.[8]

Total Information Awareness, later termed as Terrorism Information Awareness, was designed as a "system of systems" to integrate aforesaid software technologies with a view to providing an information architecture of better tools to detect, classify, and identify potential terrorists and preempt their nefarious designs and hostile actions. The programme was conceived to "virtually aggregate data, to follow subject-oriented link analysis, to develop descriptive and predictive models through data mining or human hypothesis, and to apply such models to additional datasets to identify terrorists and their organisations."[9] Among other programmes that were initiated on data aggregation and automated analysis technologies were the Genisys,[10] Genisys Privacy Protection,[11] Evidence Extraction and Link Discovery,[12] and Scalable Social Network Analysis programmes."[13]

At the heart of Terrorism Information Awareness is the conviction that, by searching a vast range of databases, it will be possible to identify terrorists, even before they can strike.[14] The capability to spot enemy before he can create mayhem is the acme of intelligence. This calls for self monitoring and disciplining and where that fails, social Panoptical, which depends on observation, assessment and analysis as matters of routine [15]

Compromising Emanations

Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. Compromising emanations consist of intentionally or unintentionally emitted electrical, mechanical, or acoustical energy.[16] The nature of these emissions has changed with evolving technology; electromechanical devices have vanished and signal frequencies increased several orders of magnitude. Recently published eavesdropping attacks on modern flat-panel displays and cryptographic coprocessors demonstrate that the risk remains acute for applications with high protection requirements.[17]

Computers have increasingly become surveillance targets because of the incriminating, personal and security-sensitive data stored on them. If someone is able to install key-logger software or imbed spyware, either physically or remotely, such as the FBI's "Magic Lantern"[18] or "Computer and Internet Protocol Address Verifier (CIPAV)"[19] on a computer, he can easily gain illicit entrée to the system and illegal access to this data contained therein.

Surveillance

Surveillance is a broad term that embraces many tasks, vis. keeping a watch, monitoring of behaviour, tracking activities and gathering information of terrorists and anti-social elements in a surreptitious and covert manner. It is broadly sub-categorised in three types, vis. physical observation, signal intelligence (SIGINT), and cyber interception and snooping. Physical observation is through human intelligence (HUMINT) by under cover agents and informants, infiltration by spies and moles, reconnaissance patrols and vital discrete and not so discreet exchanges by diplomats and military attaches, the quality of which has appreciably gone down over the years, a fact publicly acknowledged and bemoaned by the National Security Adviser Sh Narayanan and that too recently. The other two, vis. SIGINT and cyber penetration and probing, are sourced from and are intertwined with the Electromagnetic and ICT, which is the focus and thrust of this special Issue. Both the terrorists and counter terrorists closely and inextricably depend on it.

Mass surveillance is conducted by all the major powers. The views on mass surveillance differ widely: some advocating it with a table-thump; others grudgingly accepting "Big Brother Watching" as an unavoidable and indispensable iniquity; and still others; vocally and raucously denouncing it as infringement of privacy. However if the choice is between security and privacy, citizens other than terror, anarchy and crime pushers and peddlers would opt for the former.

There is abundance of data related to terrorist and other unlawful activities on the Internet. It is sheer impossible for humans to manually search, sift and study it. Further, the Internet offers incalculable opportunities to vend spam and hoaxes to fool and trap the gullible as well as the naïve amongst the "agencies". Intelligence is a game two can play. In India every third day you get a warning for terrorist attack, which never comes about. The terrorists strike when the public and the security personnel get used to the "routine" of bluffs and lower their guard. They strike at the place and time of their own choosing.

Only technology can obviate this human folly and naïveté. Surveillance gadgets and spybots can sift through vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by picking and investigating "trigger" words or phrases, visiting web sites, or pretentiously and scrumptiously communicating with suspicious individuals or groups to gain intelligence.[20] The Echelon after capturing data sifts it using a programme called Dictionary.[21] which finds pertinent information by searching for key words to pare down voluminous data. The NSA also runs a database known as "Pinwale",[22] which stores and indexes large numbers of emails of both American citizens and foreigners.

Bio-Surveillance and ICT.

Bio-Surveillance programme develops "information technologies and resulting prototype capable of early and automatic detection of the covert release of a biological pathogen attack . seeking to achieve its objective by monitoring non-traditional data sources such as animal sentinels, behavioural indicators, and pre-diagnostic medical data.[23] Technical challenges include correlating/integrating information derived from heterogeneous data sources, development of autonomous signal detection algorithms, refinement of disease models for autonomous detection, and ensuring privacy protection while correlating widely differing data and sources.[24]

Aerial surveillance

Aerial surveillance, usually visual imagery or video from an airborne vehicle, is catching on both in mission spread-out and technology sophistication. Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances.[25] The UAVs are being planned to patrol the skies for critical infrastructure protection, border surveillance, terrorist shadowing, "transit monitoring", and general watch. Endowed with vertical take-off and landing; Micro Aerial Vehicles (MAVs) are being made capable of "carrying tasers[26] for crowd control,"[27] or weapons for killing enemy combatants, other technologies that merit cognisance are real-time image and video capture from UAVs; image exploitation in surveillance and reconnaissance missions, multi sensor fusion, Ground Image Exploitation System (GIES), and enhanced vision for situational awareness.[28]

India has got its first Integrated GIS and Image Processing Software (IGiS) developed by Scanpoint Geomatics, a software development firm in partnership with Indian Space Research Organization (ISRO). IGiS is a completely indigenous seamless geomatics application, which includes geographical information system (GIS), image processing and its integration with the real time information, using the global positioning system (GPS).[29] The satellites and aircraft sensors are able to penetrate cioud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and can provide real-time video at much higher resolutions than the still-images produced by programmes such as Google Earth.[30] The official, unofficial and clandestine tapping of telephone lines is widespread in almost all the countries In the US, Communications Assistance for Law Enforcement Act (CALEA)[31] requires that all telephone and VoIP communications be available for real-time wiretapping by federal law enforcement and intelligence agencies. Two major telecommunications companies in the US, viz. AT&T and Verizon have arrangements with the FBI, requiring them to keep their phone call records searchable and accessible by federal agencies

Technological Intelligence (TECHINT)

TECHINT covers a host of intelligence functions under the subdivision of Signal Intelligence and Cyber Intelligence. The former embraces Communication Intelligence (COMINT), Electronic Intelligence (ELINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT) etc. Electronic gadgetry includes Close Circuit Television (CCTV) cameras, biometric devices, bugs, direction and location finders and keystroke loggers. The gadgetry is backed up by programmes and software to carry out "near real time search and identification from distributed large data bases and the computer simulation", a field in which we have much to learn from the US. The programmes, as put into operation by them, include ADVISE,[32] an acronym that stands for Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement – a research and development programme in the ambit of Threat and Vulnerability Testing and Assessment (TVTA) portfolio, TALON[33] an acronym for Threat and Local Observation Notice of the United States Air force, and Guardian[34]of the FBI. These, some of which have been discontinued under pressure from the privacy activists, are reported to be a state of manipulated mutation. .

Cyber Snooping and Interception

A sizable proportion of computer surveillance involves capture of data and traffic on the Internet. The terrorists during the Mumbai attack were using Voice over Internet Protocol (VoIP) and iphones, interception of which paid handsome dividends for post-event analysis. It is a matter of great distress that our intelligence agencies show marked preference, even penchant for interception for fighting later-date legal battles, rather than denial and jamming of communications between front-line suicide operators and their mentors such as those in Pakistan to manage the crisis in real time and save lives. Indian media video coverage at Taj Hotel and other places in Mumbai terror attacks, and response instructions like "Khajoor Khao; Aag Lagao" were passed with impunity and to our incalculable damage and detriment.

Electromagnetic Scanners and Key-Loggers

In the past we assumed that only wireless-connected keyboards could be intercepted by an electronic eavesdropper, but not the wired or laptop keyboards. This presumption stands rebuffed by researchers of Security and Cryptography Laboratory at Lausanne, Switzerland.[35] They .have demonstrated that 12 different keyboards could be eavesdropped by war-driven monitoring of their electromagnetic signatures from up to 65 feet away; that, too, through walls. They devised four separate methods for EM eavesdropping. "The method for intercepting signals involves detecting the full spectrum of electromagnetic radiation emitted by a keyboard and analysing the specific change in signal over a variety of wavelengths for each key press."[36]

The US and the Chinese have exhibited marked and fulsome expertise. In the case of the former, Magic Lantern and CIPAV are keystroke-logging software developed by the FBI. Unlike previous keystroke logger programmes used by the FBI, Magic Lantern can reportedly be installed remotely, via an e-mail attachment or by exploiting common operating system vulnerabilities. It is not known how the programme might store or communicate the recorded keystrokes.

Magic Lantern, however, can be embedded over the Internet by tricking a person into opening an email attachment. It is unclear whether Magic Lantern would transmit keystrokes it records back to the FBI over the Internet or store the information to be seized later in a raid. This is a software application that sits on a computer and runs without the user knowing it's there.[37]

The CIPAV is a data-gathering tool that the FBI uses to track and gather location data on suspects under electronic surveillance. The software operates on the target computer much like spyware, whereas it is unknown to the operator that the software has been installed and is monitoring and reporting on their activities. The CIPAV captures location-related information, such as: IP address, MAC address, open ports, running programmes, operating system and installed application registration and version information, default web browser, and last visited URL.[1]Once that initial inventory is conducted, the CIPAV slips into the background and silently monitors all outbound communication, logging every IP address to which the computer connects, and time and date stamping each.[38]

One of the highly versatile cyber surveillance systems, which can penetrate complex IP networks such as the Internet, is NarusInsight. It can track individual users, monitor applications e.g. web browsers, instant messaging, email and look through activities e.g. web sites visited, contents of emails and instant message conversations and see how users' activities are connected to each other e.g. compiling lists of people who visit a certain type of web site or use certain words or phrases in their emails.[39] It is claimed to be highly reliable with a wide range of functionality The intercepted data flows into NarusInsight Intercept Suite. This data is stored and analyzed for surveillance and forensic analysis purposes. Other capabilities include playback of VoIP, rendering of web pages, examination of e-mails and their attachments, high-speed packet processing performance.[40] In the case of the Chinese, key-loggers are inbuilt in hardware of computer peripherals widely sold in the market all over the globe.

Risk Management vis-à-vis Crisis Management

In India we are not sure about the vital definitive distinction and mission dissimilarity between risk and crisis management. Whereas risk management involves assessing potential threats and finding the best ways to avoid those threats, crisis management entails dealing with the disaster after its occurrence. It is a discipline consisting of skills and techniques required to assess, understand, and cope with any serious situation, especially from the moment it first occurs to the point that it is resolved.[41] National **crisis management** created by terror attacks is the process by which the government authority and security organisations deal with any major unpredictable event that threatens the security, integrity. governance, and economy of the country and harm the general public.

Whereas risk management is essentially an intelligence gathering, diffusion and analysis activity, primarily a prerogative of the intelligence agencies; crisis management involves, interception, interdiction, and physical destruction of terrorists and their bases, counteraction and jamming of communications, and deception and denial of information, a sole prerogative of the armed forces and other security agencies. Tendency to tread on each others toes must be curbed. However Integration and intelligence fusion is a vital prerequisite for counter terror operations. .

Concluding Remark

This paper is a cursory glimpse of a subject which defies intellectual and academic treatment of cavernous depth. We have a long way to go if this menace has to be wiped off the Earth. Technology has to mesh with courage. Of the latter, we have abundance amongst our soldiers. It is the former they seek from us. Let us, the scientists and technocrats, accept the challenge. If junglee software used by the CIA can be made in India, surely we have the capability to rig up algorithms to collect, sift, sort, archive, mine and analyse data and trak, trail and destroy terrorists before they reach the target.

Notes

1. PM speaking at the award giving ceremony of Shanti Swarup Bhatnagar awards for 2007 and 2008 to young scientists See Ians, "Technology vital to counter terror: PM" *Technology News*, 22 December 2008

2. See Yashwant Deva, "Technologies for Combating Terrorism" *IETE Apex Forum*, ttp://www.iete.org/apexforum2002.htm

3. Ibid

4. Echelon is a SIGINT collection and analysis network operated by National Security Agency of the United States, Government Communication Headquarters of Britain, Communication Security Establishment of Canada, Defence Signals Directorate of Australia, and Government Security Bureau of New Zealand. After 9/11, **its focus has shifted to targeting terrorist communications.** http://en.wikipedia.org/wiki/ECHELON

5. NarusInsight Intercept Suite captures and analyzes packet-level, flow-level, and application-level usage information as well as raw user session packets for forensic analysis, surveillance or in satisfying regulatory compliance for lawful intercept. http://www.itsecurity.com/security.htm?s=17338

6. **A controversial programme,** Genoa II focused on building information technologies to help analysts and policy makers anticipate and pre-empt terrorist attacks. Genoa II was renamed Topsail and was moved to ARDA., but reportedly it continues to pursue its original mandate. See Shane Harris, "TIA Lives On,"*National Journal,* Feb. 23, 2006, http://www.nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm

7. The custom-built Carnivore system was used by the FBI to monitor email and other network communication. Carnivore became obsolete when third-party surveillance tools gained in features and filtering abilities. **http://email.about.com/od/staysecureandprivate/a/carnivore.htm**

8. Declan McCullagh, "FBI turns to broad new wiretap method." January 30, 2007. *ZDNet News.* http://news.zdnet.com/2100-9595_22-151059.html.

9. Wikipedia, http://en.wikipedia.org/wiki/Information_Awareness_Office

10. The Genisys Program seeks to produce technology for integrating and broadening databases and other information sources to support effective intelligence analysis aimed at preventing terrorist attacks. Report to Congress regarding the Terrorism Information Awareness Program, www.**epic.org/privacy**/profiling/tia/may03_report. pdf

11. The Genisys Privacy Protection Program aims to create new technologies to ensure personal privacy in the context of improving data analysis for detecting, identifying, and tracking terrorist threats. Ibid.

12. The objective of the **Evidence Extraction and Link Discovery** (EELD) program is to develop a suite of technologies that will automatically extract evidence about relation- ships among people, organizations, places, and things from unstructured textual data, such as intelligence messages or news reports, which are the starting points for further analysis. Ibid.

13. The purpose of the **Scalable Social Network Analysis (SSNA)** algorithms is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people, based on their patterns of interactions, and to identify when a terrorist group plans to execute an attack. Ibid.

14. **Kristie Ball and Frank Webster, "The Intensification of Surveillance", ed, Kristie Ball and Frank Webster, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (London, Sterling and Virginia, Pluto Press, Paperback, 2003) p. 4**

15. R Whitaker, *The end of Privacy: How Total Surveillance is becoming a Reality* (New York, The New Press, 1999) as quoted in **Kristie Ball and Frank Webster, ibid. p 6**

16. See Wikipedia, http://en.wikipedia.org/wiki/TEMPEST

17. "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," at **lasecwww.epfl.ch**/keyboard.

18. **Magic Lantern** is keystroke logging software developed by the FBI Officially it has been described as a database that sorts and matches data gathered using various Carnivore-like methods from e-mail, chat rooms, instant messages, and Internet phone calls. It also matches files with captured encryption keys.

19. CIPAV is a data gathering tool that the FBI uses to track and gather location data on suspects http://en.wikipedia.org/wiki/CIPAV and Kevin Poulsen, "FBI's Secret Spyware Tracks Down. Teen Who Made Bomb Threats", http://www.wired.com/politics/law/news/ 2007/07/fbi_spyware

20. Michael Hill, "Government funds chat room surveillance research", *Associated Press,* October 11, 2004, *USA Today.* http://www.usatoday.com/tech/news/surveillance/2004-10-11-chatroom-surv_x.htm.

21. Steve Wright, *An Appraisal of Technologies for Political Control,* January 6, 1998, http://cryptome.org/stoa-atpc. htm.

22. Wayne Madsen, "NSA's meta-data email surveillance program exposed," *Crimes of the State*, http:// crimesofthestate.blogspot.com/2009/02/online-journal-nsas-meta-data-email.html

23. Visit Information Awareness Office website, http://infowar.net/tia/www.darpa.mil/ iao/ BSS.htm

24. Ibid.

25. HCL Technologies: At the cutting edge, 07 January 2009, **domain-b.com**/companies/companies_h/../20090107_hcl_**technologies**.html

26. A Taser is an electroshock weapon that uses electrical current to disrupt voluntary control of muscles. *Wikipedia*, http://en.wikipedia.org/wiki/Taser.

27 n. 25

28. Ibid.

29. ISRO, Scanpoint Geomatics develop image processing software, 30 July 2009, http://www.domain-b.com/aero/space/20090730_isro.html

30. Ibid.

31. Ryan Singel, "Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates," http://www.wired.com/politics/security/news/2007/08/wiretap

32. **ADVISE** is a research and development program of massive data mining system with the ability to store one quadrillion data entities. http://en.wikipedia.org/wiki/ADVISE

33. **TALON** is a database about possible threats to US servicemen and overseas civilian maintained by the USAF after the 9/11 terrorist attack. http://en.wikipedia.org/wiki/ TALON_(database)

34. The Guardian Threat Tracking System tracks and trails counterterrorism suspicious activities, which can be stored, assigned, triaged, and searched by all FBI employees and other government agency partners. FBI Press Release at www.**fbi.gov**/pressrel/pressrel08/**guardian**110708.htm

35. LASEC/EPFL, "Electromagnetic scanners can detect what you are typing right now," http://gizmodo.com/ 5066156/electromagnetic-scanners-can-detect-what-youre-typing-right-now

36. Ibid

37. Magic Lantern, n. 18.

38. CIPAV, n. 19.

39. NarusInsight, n. 5

40. Ibid.

41. Visit http://en.wikipedia.org/wiki/Crisis_management

About the author

Maj Gen Yashwant Deva, AVSM(Retd) is scholar, writer and defence analyst of repute, Maj. Gen. Yashwant Deva, AVSM (Retd) was President of the Institution of Electronics and Telecommunication Engineers (IETE) for the years 2000-2002. He is a Distinguished Fellow of IETE, and a fellow of other prestigious science and engineering institutions of national and international standing. He served in terrorism inflicted and insurgency prone areas both in India and abroad. His foreign tenures included Vietnam, Afghanistan and Sri Lanka. and home-ground tufts J&K, Nagaland, Manipur, UP Tibet border, Sikkim and Western theatres in 1965 and 1971 wars. He has wide experience in planning and execution of ICT related to counter-terror and asymmetric warfare and has extensively written on it.

He is a recipient of Ati Vishisht Seva Medal for engineering a wide-ranging and integrated network of highly responsive communications over diverse media during Operation Pawan in Sri Lanka spanning the mainland to the island and the operational areas of IPKF; providing electronic support to the force; and for restoring war-ravaged telecommunication services in Jaffna Peninsular, as part of the civic action.

He is widely quoted in India and abroad as an authority on various facets of electrotechnology, e-intelligence, cyber-security, information warfare and cyber and info terrorism. His written works include, Sky is the Limit: Signals in Operation Pawan (2007); Secure or Perish (2001) Dual Use Information Technology: An Indocentric Perspective (1997), an edited compilation Multimedia'98: Shaping the Future (1998), e-monographs, Internet: Challenges, Opportunities and Prospects (2002), ICT (Information Communication Technology) for All: Empowering People to Cross the Digital Divide (2003), and Special Issue of Technical Review on Information Security (2002), published by the IETE. His works have been placed in the national libraries of the various countries including those of the parliaments, and on the "Best of the Web."

He is committed to a life-long two-pronged mission of "Reaching Other Side of the Digital Divide" and "Taking Technology to the Trench". He has a measure of success in his endeavours to sensitise the technology savvy and prod the decision-makers in either field.

Contact

e-mail : deva@nde.vsnl.net.in
Mobile : 07324-273089

Instrumentation for Monitoring Terror Attacks: Emerging Trends

Dr Pawan Kapur

Abstract

Recent technological advances in the field of ICT have affected almost all sectors of our society. To name a few: precision agriculture, food processing, surveillance, warfare, e-health, e-education, e-governance systems etc. One of the misuses of technological evolution has also given way to terrorism and its other shapes. There are several features such as social, political, and economic which lead to such situations but their outcome is more or less the same in terms of destruction and suffering. The extensive uses of latest technology in terrorism are well known: propaganda, intelligence, communication, ICT-enabled weapons systems, jamming/destroying civilian communication systems. One, therefore, needs to combat terrorism by providing better detection, feature extraction, communication and coordination mechanisms, by establishing early warning systems and developing front end devices & modules such as sensors & detectors, biometric systems, signal processing & faster communication etc. Terrorism is becoming highly organised & high tech day by day and a robust system for terror prediction and mitigation is an imperative need of the hour. The existing internet infrastructure, wireless telephony, CCTV/IP camera infrastructure, e-mail scrutiny, satellite network, advanced sensors etc can be networked together to form a powerful system for terror prediction and mitigation. This paper presents current and emerging trends of instrumentation for monitoring terror attacks which can lead to early warning and corrective measures. Focus is made mainly on instrumentation and techniques for surveillance & warfare.

Keywords: *Sensors and devices, feature extraction, networking*

1. Introduction

Historically, terrorism has been a weapon of the weak characterized by the systematic use of actual or threatened physical violence, in pursuit of political objectives, against innocent civilians. Terrorist motives are to create a general climate of fear to coerce governments and the broader citizenry into ceding to the terrorist group's political objectives. Terrorism today is transnational in scope, reach, and presence, and this is perhaps its greatest source of power. The most important aspect of society's defense is the recognition of terrorism as a major threat and challenge of the 21st Century. The events of September 11, 2001 certainly have provided a rude awakening. They have changed the dynamics of war on terror with the development of state-of-art detection techniques for explosive, chemical and biological agents. Chemical weapons and explosives present immediate threats to public health & safety and their detection is therefore of high importance. A great deal of problem is faced by the law enforcement agencies, security personnels and international border regulating agencies because of recent terrorist activities and the consequent loss of human lives and property. The problem is becoming more and more serious, as search for more powerful explosives with new composition is continuous and parallel to these, new methods of packing and transportation of these materials cause failure of existing available detection techniques. That is why, while several detection methods are available, a great concern still exists for the development of methods that allow detection and identification of explosives in close-proximity as well as at a stand off distance. There are many considerations for development of comprehensive detection techniques. For example vast countrywide international borders and extensive cross sections of people are to be scanned, more & more new explosives are being developed, methodology of smuggling and concealment for different explosives are different and explosives debris cause serious environmental problems. With mounting pressure for security measures, innovative and new techniques are being pursued within India and worldwide.

2. Key Technologies for Counter Terrorism

2.1. Detection of Explosives: Basic explosives do not require extensive technical knowledge and can be created with materials commonly available. They can be solids, liquids or a mixture of both, when ignited by heat or shock undergo rapid decomposition or oxidation (explosion) and consist of Nitrogen, Oxygen, Carbon and Hydrogen. The Nitro group in them is mainly responsible for the explosive characteristics. They have high density and low Z. Explosion process releases energy in the form of Heat and light or by breaking down into large volume of gaseous compounds generating shock waves, high temperature and pressure gradients responsible for damage

2.2 Basic requirements of an acceptable Explosive Detector

- Detector should be able to detect all types of explosives under varied conditions (various environments such as border-crossing, air & marine terminal, postal terminal and large gathering at various places) independent of packaging
- High sensitivity, specificity, reliability and better detection ability
- Minimum false alarm and high scan rate (Minimum memory effect)
- Operation of the technique must be safe, cost effective and low power
- Field equipment/ detector must have minimum consumable, fast, handy provide go- no-go detection
- Imaging system should provide an object resolution as small as 1mm i.e. capable of identifying blasting caps and detonators
- *System should not create safety hazard to* operator in terms of health, by product, radiations and disposal
- Forensic identification of captured explosive, Post explosion and hidden and concealed explosive detection

2.3 Detection Methods

Depending upon their characteristics such as geometry, material density, elemental composition and vapour emissions, there are three main categories of explosive detection techniques:

(i) ***Vapour and Trace Detection:*** These methods measure trace of characteristic volatile compound that evaporates from the explosive or present as particulate on the explosives container surface.

- Animal olfaction- dogs, Mongolian Gerbil and rats
- Electron capture Detector (ECD)
- Gas Chromatograph (GC & GC-ECD)
- Ion mobility spectrometry (IMS)
- Mass spectrometry
- Bio-luminescence
- Electronic-nose: Fluorescent-polymer sensor, MEMS, SAW

(ii) ***Bulk Detection***: Detection of bulk explosives is carried out either by imaging characteristics of the explosive device or by detection of the explosive itself. They make use of penetrating radiations that interact with certain nuclei characteristic of explosives.

- X- ray Imaging & Analysis
- Thermal Neutron Activation (Cost :~1 million $)
- Fast Neutron Activation (Accelerator only 0.25 million US$)
- Pulsed Fast Neutron
- Pulsed Neutron Back Scatter
- Nuclear Quadruple resonance (NQR)
- Millimeter wave & Terra Hertz Technology

(iii) ***Integrated (fused) Systems***: These systems integrate two technologies into one system. They can be two different bulk detection technologies or a bulk detection plus a trace detection technique.

- GC-IMS
- NQR-X-Ray Imaging
- CT-IMS

All these detection techniques are limited either by fundamental physical limits or by the circumstances of a particular scenario, for example, background interference.

2.4 International Status

Federal Aviation Administrator (FAA), National Research Council of Canada (NRC) and European Civil Aviation Conference (ECAC) are working together to combat terrorism. Various attempts are underway to replace sniffing capabilities of dog and other animals (animal olfaction) by suitable vapour detectors. Some vapour detection and bulk detection instruments are available worldwide commercially whose price structure vary from simple sniffer US$ 10,000 to X-ray computer Tomography system costing US$ 5,00,000 Main problem with these systems is that no single detector is available to detect all types of explosives and other materials under all conditions. Besides this, work is underway for investigating the latest techniques based on tera hertz spectroscopy, micro cantilever, fluorescence, fiber gratings, nano technology etc

2.5 National Status

Sniffer dogs are most frequently used for detection of explosives and chemicals. Metal detectors and X-ray screening developed by ECIL are available; DRDO had developed a chemical kit for detection of Explosive. Other modern detectors are imported from developed countries. CSIO, Chandigarh has developed a GC-ECD based portable system supported by DRDO and DIT, Non Linear Junction Detector and Electronic Stethoscope supported by (MIT). Besides this, there are a few other labs working in this area but so far no comprehensive developmental program has been generated in this area so far in the country

3. CSIO's Program for Counterterrorism Instrumentation:

3.1 Portable Explosive Detector

A portable explosive detector based on gas chromatography principle was developed. The detector separates the mixture of volatile compounds when these flow through the chromatographic column containing a stationary phase, through which the stream of inert gases pass continuously. As different components in the mixture interact differently with stationary phase, they emerge out of the column after different retention times. All modern organic explosives emit organo-nitro compounds to a greater or less extent, depending on the type of explosives. The detection of explosives is made by utilizing their electron capturing property, common to all organo-nitro compounds. With this technique, the hidden organic explosives (not hermetically sealed) such as TNT, EGDN, NG, PETN, RDX, HMX, RDX/TNT etc can be detected. The technical knowhow of the instrument has been transferred to M/s Security Defence Systems, Chandigarh.

3.2 Non-Linear Junction Detector

A hand held, portable and field operatable non linear junction detector (NLJD) based on harmonic radar principle has been developed for detection of explosives. It is an essential tool for electronic counter measure searches and a variety of security evaluation procedures. The NLJD aids the security personnels in the search of bugging devices and other concealed electronic items such as timers, or remote control receivers for detonation of explosive dormant and non- operational devices. It detects all kinds of non-linear junctions which may be of semiconductor or metallic types. The specific function of the NLJD is to detect electronic devices meant for detonating the Explosive Ordnance Disposal (EOD) and Improvised Explosive Device Disposal (IEDD). In this case, a spectrally pure microwave signal is emitted from the antenna head and this causes the non linear junction of the target - containing semiconductor device to resonate at its natural frequency. This in turn, induces the re-radiation of higher order harmonics of the original signal. It is the first indigenous low cost development of this instrument. Devices like radio transmitters, power amplified microphones and electronic timers etc contain non-linear junctions and will be detected even if they are embedded in the cabinets and either in conducting and non-conducting states. The technical knowhow of this instrument has been transferred to M/s Astra Microwave Products Ltd, Secunderabad (AP).

3.3 Electronic Stethoscope

An electronic stethoscope has been developed which supports the detection and monitoring of air delivered ordnance and improvised bombs based on mechanical/ electronic timers from very close range to several meters depending on position, surrounding and type of timing device used. An improved mechanism employed enhances operator safety by avoiding the direct contact between the target and instrument. The contact less search head used applies a high frequency beam to monitor mechanical noises resulting from timers and mechanisms. When operating at targets supposed to contain improvised explosive or incendiary device, the contact less search head offers many advantages, as no contact with the target is necessary. The instrument comprises of a trans-receiver, which includes a Gunn diode, mixer diode, and horn antenna. The Gunn diode generates a microwave frequency in the range of 10-11 GHz. The mixer diode converts the two microwave signals into an equivalent electrical signal. The horn antenna transmits and receives the microwave signals with out distortion. The technical knowhow of the instrument has been transferred to M/s Rotax Electronics, New Delhi.

3.4 Ion Mobility Explosive Detector

A portable explosive detector based on ion mobility spectrometer is being developed at CSIO. The detection is based on the electron capturing capability of nitro compounds emanating from organic explosives. Sample ions formed in the Ni-63 ionization chamber are made to drift under the influence of uniform electric field in a tube with a velocity depending on their mass/ mobility. One of the challenges in the development of ion gate / shutter lies in the fabrication of a set of two coplanar parallel wire grids separated by less than 1mm subjected to high voltage biasing applied to these grids. The tuning of the system for detection of standards vapours is under progress.

3.5 Fiber Optic Intrusion Detection System (FIDS)

Fiber Optic Intrusion Detection System (FIDS) is a highly reliable and sensitive security system having virtually 100% Detection Rate with negligible false alarm. The system comprises of a uniquely foldable and structured fiber-optic net made of a fiber-optic cable formed into squares, which are crossed at each joint with a plastic crossover button, Zone Processing Unit and Front Panel Display Unit. Infrared light from an LED travels through the fiber net. Any attempt to tamper with the net, causes micro bending of the fiber leading to loss of light and this change of light level detected by a Si PIN photodetector triggers an alarm. The FIDS has the capacity of monitoring eight zones. This system can be beneficially used for guarding ammunition depots, machines, airports, sensitive installations like power plants and nuclear reactors.

3.6 Fiber Optic Speckle Based Intruder Detection System

In this approach, the laser light traveling in a multimode fiber generates a speckle pattern at the other end. This pattern is highly sensitive to perturbations on the fiber, which generate the change in path length of light in various modes leading to movement of the speckle pattern. A CCD camera sees the speckle pattern generated on the fiber and image processing techniques are used to detect an intruder. The technical know-how for these intruder detection systems has been transferred to M/s Security Defence System, Chandigarh.

3.7 Fiber Optic Sensors for Shock Detection

CSIO has developed extrinsic Fabry-Perot interferometric (EFPI) as well as fiber Bragg grating (FBG) based sensors for detection of shock waves. Operation of an EFPI depends on an air cavity which works as a low finesse 2-beam Fabry Perot interferometer. The FP air cavity is realized between cleaved end faces of an input output single mode fiber and a reflecting single mode or multimode fiber aligned in a silica capillary tube. The two reflections from two fiber faces interfere to produce fringes at the detector. Any change in the cavity width causes shift in fringes leading to measurement of strain or pressure. The EFPI sensor offers the advantage of simple construction, single-ended operation, high resolution, accuracy and low cost. The EFPI output is not affected by transverse strains. For shock detection, the reflector fiber is replaced with a membrane. Under the effect of a shock, the reflector membrane caves in creating a optical path difference

Fiber Bragg gratings (FBGs) and long period gratings (LPGs) are the recent important intrinsic fiber elements for sensors and communication applications. FBGs have periods of the order of half a micron for operation around 1550 nm window while LPGs have a period of a few hundred microns. When a light wave enters a medium with varying refractive indices, it undergoes minute reflections from every interface. If all the individual reflections are in phase, then the medium will strongly reflect the incident wave. If the reflected waves are not in phase, the net reflection would be weak. Since, the phase difference between adjacent reflections is dependent on the wavelength; this implies that the overall reflection from such a medium would be strongly wavelength dependent. FBGs are produced by realizing submicron periodic patterns in the fiber core. This is achieved by exposing a step-index germanosilicate core of a single mode fiber to intense UV light typically from a KrF excimer laser at 248 nm or a frequency-doubled argon-ion laser at 244 nm. CSIO has established state of the art facility for writing FBGs and LPGs for sensor applications. Both these sensors with appropriate transducer mechanism can work as very efficient vibration sensors.

3.8 Optical Fiber LPG based Sensors

This is another class of fiber grating sensor which utilizes the high sensitivity characteristics of the gratings to changes in the refractive index of the medium surrounding the cladding. Specific coatings on the silica surface of an LPG can detect trace amount of target molecules. This technology can be used for detection of explosives or chemical and bio warfare agents and organisms.

3.9 FBG based Gait Analysis System for Intrusion Detection

Various types of sensors have been used in tactile sensing schemes, predominantly resistive, capacitive, and piezo-electric. These are not always easy to use due to their size, weight and number of connections needed, and their susceptibility to electromagnetic interference from other equipment operating in the vicinity. Optical fiber sensors by contrast are immune to electrical noise (they could for instance be used inside a magnetic resonance imaging scanner) and in the case of Fiber Bragg Grating (FBG) sensors they can be multiplexed and used in reflection so that only a single connecting fiber is required to serve a group of sensors. FBG sensors described above are basically generic strain sensors. They sense strain through change of pitch of FBG and the consequent shift of the Bragg wavelength

Fiber Bragg gratings have been successfully used in one and two-dimensional tactile sensing systems, offering performance comparable to or better than conventional sensors. Distributive Tactile sensing systems use fewer sensors than conventional sensing regimes and use a fast mathematical algorithm, suitable for operation in real time applications. Potential applications for the two-dimensional sensing surface include human balance and gait monitoring, capable of detecting simultaneously the position and shape of an object placed upon it, for which existing systems use large numbers of sensors or complex imaging systems. Fiber Bragg gratings can be embedded within materials forming a surface without loss of material strength, which would be an advantage in such applications. This capability can be used for detection of intrusion and physical movements of an object that could be a suspicious human being likely to cause harm

4. Future Trends

4.1 Micro-cantilever based System

In this system the cantilever is coated with specific sensitive layer for molecular recognition on which molecular adsorption takes place, resulting in cantilever deflection. This system is specific (vapor/antigen/protein/molecule), highly sensitive & compact but is not available commercially.

4.2 Optical Fiber LPG based Detection

This new class of fiber optic sensor utilizes specific coatings on its surface that can detect trace amount of target molecules up to few hundreds of ppt level. They function in wavelength domain and are immune to source intensity fluctuations and connector losses. Moreover, they provide multiparameter capability due to multi resonance feature.

4.3 Fluorescence based System

Fluorescing chromophores link together in polymers chain, in the absence of explosive compounds, the polymer fluoresces when exposed to light of appropriate wavelength. Binding of the Fluorescent polymers with explosive molecules quenches the brightness of the fluorescence.

4.4 Terahertz Radiation Technique

The technique based on THz frequency band has become an emerging technology for reliable identification of explosives. The frequency band excites vibrational modes of molecules, providing spectroscopic information especially for plastic or low metal content explosives.

4.5 Nanotechnology based Detection System

The unique properties of nanoparticles, nanotubes and nanowires offer great prospects for enhancing the performance of sensors such as nano-dogs for ppt level explosive detection

4.6 Other Technologies

Biometrics : Identify and or verify human terrorist (or watch list) subjects using 2D and 3D modeling approaches over a variety of biometric signatures: face, gait, iris, fingerprint, voice. Also exploit multiple sensor modalities: EO, IR, radar, hyper-spectral.

Categorization, Clustering : Employ numerous technical approaches (natural language processing, AI, machine learning, pattern recognition, statistical analysis, probabilistic techniques) to automatically extract meaning and key concepts from (un)structured data and categorize via an information model (taxonomy, ontology). Cluster documents with similar contents.

Database Processing : Ensure platform, syntactic and semantic consistency and interoperability of multiple types of data stored on multiple storage media (disk, optical, tape) and across multiple database management systems. Desirable aspects include flexible middleware for: data location transparency and uncertainty management, linguistically relevant querying tuned for knowledge discovery and monitoring, scalability and mediation, schema evolution and metadata management, and structuring unstructured data.

Event Detection and Notification : Monitor simple and complex events and notify users (or applications) in real time of their detection. Monitoring can be scheduled a priori, or placed on an ad hoc basis driven by user demands. When an event is detected, automatic notifications can range from simple actions (sending an alert, page, or email) to more complex ones (feeding information into an analytics system).

Geospatial Information Exploitation : Fuse, overlay, register, search, analyze, annotate, and visualize high-resolution satellite and aerial imagery, elevation data, GPS coordinates, maps, demographics, land masses, political boundaries to deliver a streaming 3D map of the entire globe.

Information Management and Filtering : Collect, ingest, index, store, retrieve, extract, integrate, analyze, aggregate, display, and distribute semantically enhanced information from a wide variety of sources. Allow for simultaneous search of any number of information sources, sorting and categorizing various items of information according to query relevance. Provide an overall view of the different topics related to the request, along with the ability to visualize the semantic links relating the various items of information to each other.

Infrastructure : Provide comprehensive infrastructure for capturing, managing, and transferring knowledge and business processes that link enterprise software packages, legacy systems, databases, workflows, and Web services, both within and across enterprises.

Important technologies include Web services, service-oriented grid-computing concepts, extensible component-based modules, P2P techniques, and platforms ranging from enterprise servers to wireless PDAs, Java, and Microsoft, NET implementations.

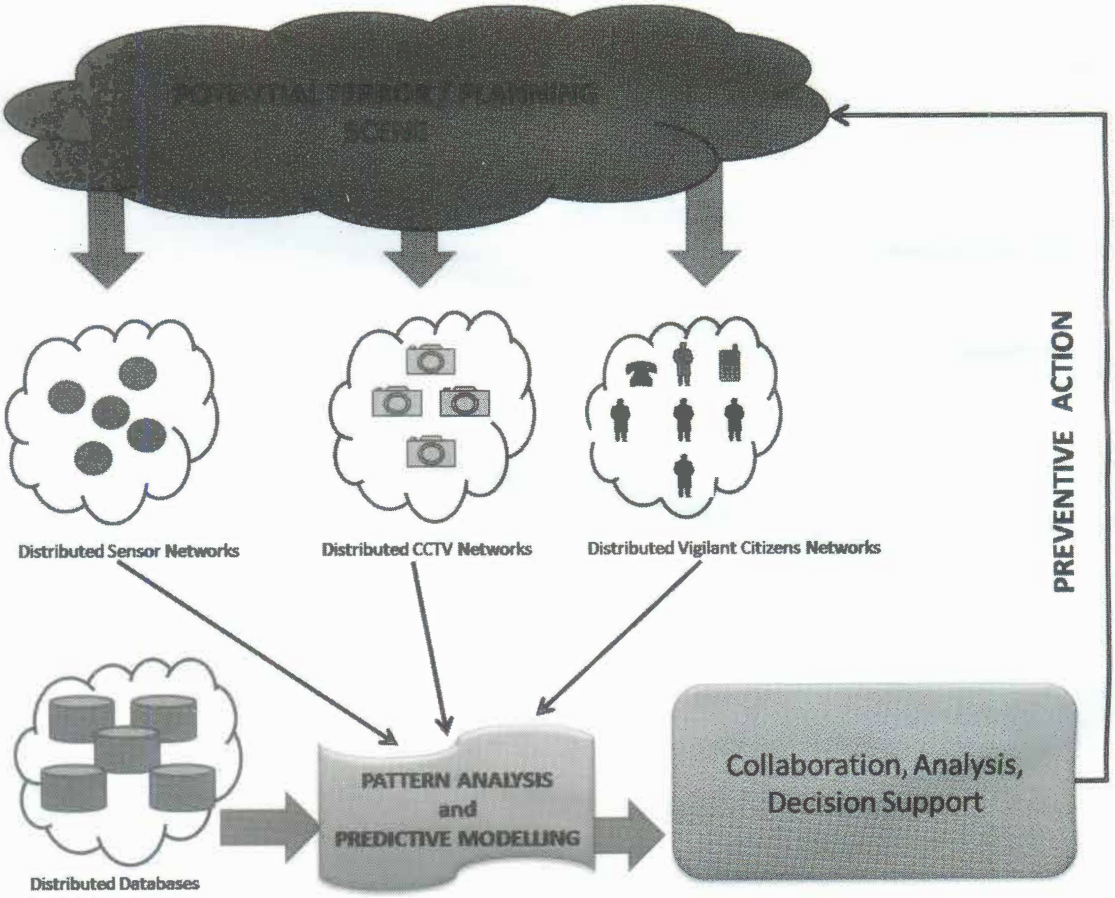
Knowledge Management, Context Development : Use Semantic Web, associative memory, and related technologies to model and make explicit (expose via Web services) an analyst's personal preferences, intellectual capital, multidimensional knowledge, and tacit understanding of a problem domain.

Predictive Modeling : Predict future terrorist group behaviors, events, and attacks, based on past examples and by exploiting a variety of promising approaches, including neural networks. AI, and behavioral sciences techniques, subject matter expertise, and red teams.

Publishing : Generate concise accurate summaries of recent newsworthy items, ensuring users see topics only once, regardless how many times the item appears in data or in the press.

Searching : Allow users to perform more complete and meaningful searches (free text, semantic, similarity, partial or exact match) across a multitude of geographically dispersed, multilingual and diverse (un)structured information repositories within and across enterprises (any document type located on file servers, groupware systems, databases, document management systems, Web servers).

Semantic Consistency, Resolving Terms : Exploit ontologies, taxonomies, and definitions for words, phrases, and acronyms using a variety of schemes so users have a common and consistent understanding of the meaning of words in a specific context. Resolve semantic heterogeneity by capitalizing on Semantic Web technologies.


POTENTIAL TERROR / PLANNING SCENE
Distributed Sensor Networks
Distributed CCTV Networks
Distributed Vigilant Citizens Networks
PREVENTIVE ACTION
Distributed Databases
PATTERN ANALYSIS and PREDICTIVE MODELLING
Collaboration, Analysis, Decision Support

Video Processing : Analyze, detect, extract, and digitally enhance (reduce noise, improve image color and contrast, and increase resolution in selected areas) user-specified behaviors or activities in video (suspicious terrorist-related activities).

Visualization : Provide graphical displays, information landscapes, time-based charts, and built-in drill-down tools to help analysts and investigators discover, discern, and visualize networks of interrelated information (associations between words, concepts, people, places, or events) or visually expose non-obvious patterns, relationships, and anomalies from large data sets.

Workflow Management : Create optimized workflows and activities-based business process maps using techniques, such as intelligent AI engines by watching, learning, and recording/logging the activities of multiple users using multiple applications in multiple sessions.

Conclusion

As new and effective methods are being adopted for concealment of explosives, chemicals & biological agents by terrorists, continuous development of new, safe, and powerful explosives by R&D agencies worldwide is an imperative need of the day. No single technique meets all the requirements to detect all types of explosives under various field conditions, therefore a combination of different techniques is required. A comprehensive & coherent strategy / developmental programs at the national level is important for continuous up-gradation and modification of the existing techniques as well as research, design and development of novel emerging techniques.

AboutAuthor

Dr Pawan Kapur, Director, Central Scientific Instruments Organisation(CSIO), Chandigarh, did his M Tech and PhD in Electronics Engineering from the University of Calcutta. Earlier he was at CEERI Pilani for about 30 years where he guided several projects in the area of electronics instrumentation for a agro- based sector. Number of Technologies developed were commercialized on which include Sugar, Tea, Mashrooms, etc.

After joining CSIO, Chandigarh, Dr Kapur restructured the laboratories laying focus on strategic and societal sectors. The R&D on Societial Instrumentation cover agri-electronics, biomedical engineering, public safety and security etc.

Dr Kapur has over 80 research papers in Journals and Conference proceedings . 4 patents,12 products , 6 book chapters and guided 50 students for their dissertation work.

Dr Kapur is recipient of several prestigious awards including CSIR technology shield, 7th Hari Ram Toshniwal Gold Medal, Neol Deer Gold Medal for successful commercialization ofTechnology in RCM.

He has visited several countries in connection with the research work in the area of instrumentation and control. Dr Kapur is a Member of various National/International societies and has been the Life - Fellow of the Institution of Electronics and Telecommunication Engineers(IETE).

Contact : drpawankapur@yahoo.com

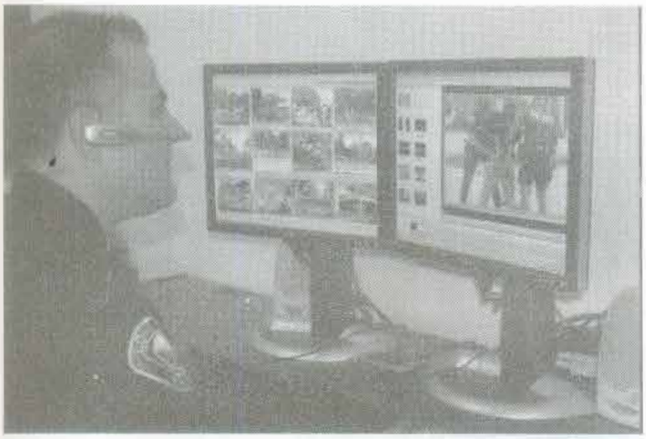
Current Challenges Associated with City Wide Surveillance Deployment

Dhruv Khanna[1] & Col Alok Sardana[2]

Executive Summary

City-wide surveillance was always a need of an hour to fight with crime as a one of the stronger controls that complements police force on ground. With recent attacks and attack sophistication definition of surveillance need to be changed.

Today's businesses and public agencies are faced with a critical need to protect employees, clients, citizens, assets from possible threats with a security system that enables rapid response to security breaches and prompt investigation of events. Organizations are additionally challenged with managing tremendous amounts of information in various forms, including video, voice, electronic data and paper.



Today's Surveillance Challenges

- **Disparate Systems**
  - Information generated by a CCTV system (video) cannot be correlated, viewed and interrogated along with data generated by, for example, an access control system.
  - While systems are moving in this direction there are, as yet, no defined protocols and standards. For years manufacturers have used proprietary protocols as a means of locking the end-user into their technology.
- **Fragmented Information**
  - Control rooms process a great deal of information, often built up over many years of experience of how to react to a given situation. Most have paper-based security policy definitions, extensive training manuals and many sources of inbound information (CCTV, access control, BMS etc). This information is usually out-of-date, not readily available and fragmented.
- **Data Islands**
  - Many control rooms have resorted to bespoke systems for storing operational information such as incident forms and operator statistics. Much of the information used by operators is still paper-based (notes on a pin-board, etc.) and not linked to their operational workstation.
- **Security policy execution in the hands of untrained personnel**
  - The execution of a security policy should be just that, execution. When serious incidents occur there is no room for ambiguity or operator-interpretation of the policy.
  - Systems which require 24 hour monitoring by humans require at least 3 personnel per position per 24 hours.
  - After 22 minutes the average CCTV operator takes in just 5% of the information available.
- **Difficult to extract management and operational information**
  - Often operator efficiency and other management statistics are not readily available in the control room environment. In an IT-based call center for example, the manager would have access to management statistics such as operator performance and call rates etc through the call center management system.
- **Information overload**
  - As security systems become more advanced and are capable of gathering more information, there is an increasing need for management

systems to filter and present that information in a contextual, interpreted manner.

- Tests have demonstrated that after approximately 12 minutes of continuous viewing of 2 or more sequencing monitors, an operator will miss up to 45% of scene activity. After 22 minutes, an operator will miss up to 95% of scene activity.

Second biggest challenge is Analog vs. Digital Technology – In most of the large installations analog based solution has been proposed and running on the ground.

While analog systems have been successfully deployed for a number of years, the inherent shortcomings when compared to digitally based solutions create compelling reasons for replacement:

- **Image Quality**. Image quality using fresh videotape, running on a VCR in excellent working order, is good. But as the tape is re-read or re-written, and as the VCR heads wear, image quality deteriorates quickly. With a digital solution, the original quality of the image is maintained, whether stored on disk, magnetic tape, CD-ROM, or DVD and is routinely accepted to be 3 times the quality of an analog image.

- **Copy Quality**. Duplicating videotape immediately causes loss of quality. Printing an image from videotape suffers from the same problem. There is no quality loss when copying a digital video image from one digital storage media to another. Printing from a digitally stored image can provide photographic quality.

- **Search time** is greatly reduced. Finding a particular activity on videotape can take hours, and in some instances even days. The analog search relies upon the attention of the human eye and is labor intensive. The digital search can take only seconds using pixel based search technology. This is a huge saving both in time and money.

- **Real-time recording** does not require a VCR for each camera. Up to 16 cameras can be recorded real-time onto a single digital Closed Circuit TV system.

- **Digital Integration** : The digital video can be easily repurposed and integrated into other technologies, including biometric technologies such as Facial Recognition.

- **TCP/IP** : Digital video can be treated as any other data feed over traditional TCP/IP infrastructures. TCP/IP is the protocol fundamental to the internet, and it enables computers to address one another across networks.

- **Storage :** Management of stored images is radically different, for example, easier access, less degradation, greater capacity, and more reliable.

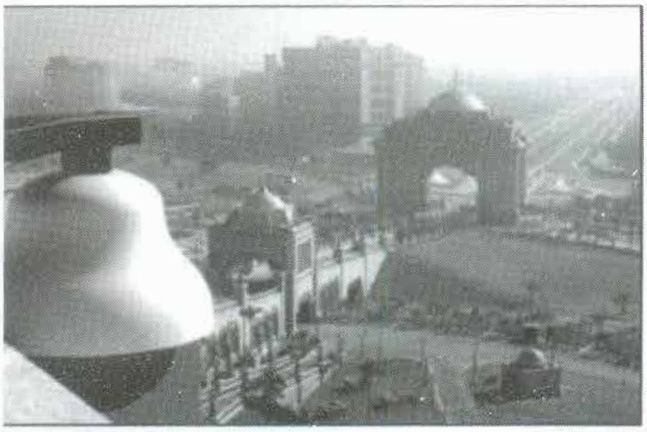
- **Labor Intensity** : The human factor is significant in terms of manually managing the tape, watching the monitors for suspicious incidents, and playback searching – all up to 24 hours per day. Digital surveillance can be an effective substitute for many of the labor intensive activities.

An analog solution cannot provide any analysis of the images that they obtain – they must be manually evaluated to detect any occurrences. With digital technology there are many forms of analysis and processing available. An ideal analog environment requires a considerable number of tapes requiring a large storage space. Plus, the tapes need to be regularly replaced within a recommended usage of 7-10 recording cycles. A requirement to retain video images for an extended length of time will demand even more storage space. The result reveals a higher total cost of ownership.

With the software based image recognition solutions incorporated into a digitally based picture system, the applications for the technology are limited only by one's imagination. For example, automatic real-time facial recognition and remote surveillance of sensitive areas with limited access requirements are all now a possibility.

Best Practices - Integrated Surveillance Solution

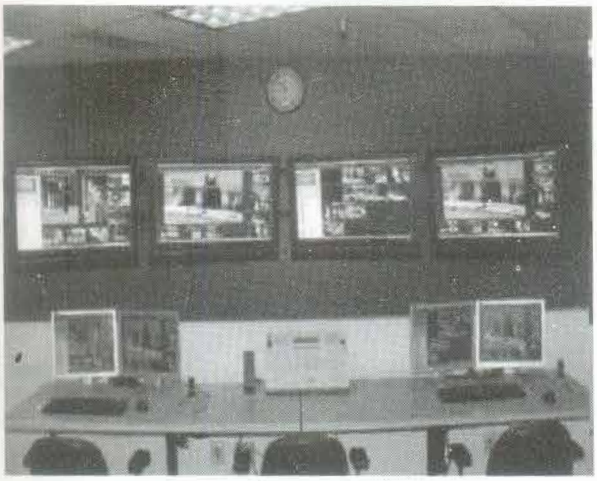
Need of high-tech video surveillance application is must and desirable to counter threats in a real-time. Some of the aspects and best practices need to be considered while designing a surveillance solution.



- **Open Framework VMS**. Any set of cameras; existing, new, or a combination thereof, can be deployed with a digital video management system. Video management system should support open framework architecture

- **Client/server architecture** : The ability to serve a variety of remote demands requires a client/server structure. This permits more than one client to view and control cameras simultaneously and more than one process to access data for more than one purpose, such as automatic remote archiving, searching and/or exporting data.

- **Integrated Command Centre Framework** : Alerts delivered by surveillance application is just a start, application should be well integrated with 3rd party sms gateway, public addressable system and other alerting system.



- **Cross Vendor Integration** : Proposed Command Centre application should be able to integrate with all 3rd party systems from various vendors along with surveillance or leveraging surveillance as a medium. Other applications like facial recognition, license plate recognition, infrared surveillance etc.

- **Workflow Management** : Command & Control application should be able to deliver good workflow management post alerting to do incident response

- **Hardware Independent** : Video Surveillance/ Analytics/Command & Control centre application should be independent of hardware (storage/server)

- **Remote diagnostics and access** :Video servers are network assets that should be managed with network management software. Video surveillance applications must respond to industry standard network management tools.

- **Plug and play on any network** : All video servers should be TCP/IP addresses. All cameras are simply addressable devices from a TCP/IP address.

- **Flexible controls for user level access** : Administrators can establish secure controls to access whatever configuration of cameras to whatever group of users makes sense for the organization.

- **Secured Access** – Secured access using SSL layers to be provide over WAN network

- **Security Framework** : Secured framework to be build from IT Security controls standpoint, it has been observed in most of surveillance or command and control installations security audits or IT security controls and reviewing of these controls on a periodic basis is missing

- **Audit trails.** Consistent with traditional IT guidelines, video surveillance applications should provide managers with complete and reliable usage information.

- **Wired/Wireless** – Wired / Wireless approach to be proposed while designing solution

- **Redundancy** – Redundancy to be planned at network, server, power level

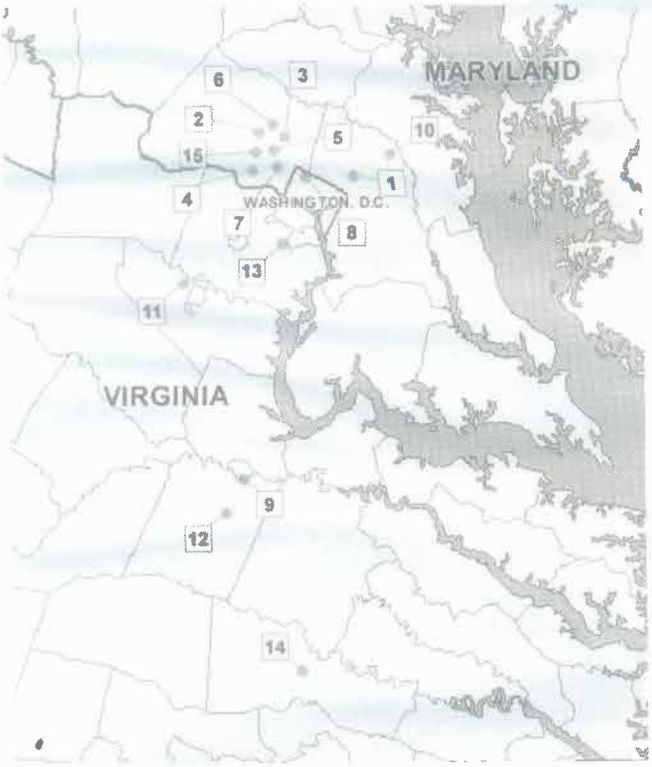
- **Planned Drills** – Planned drills to be carried out to assess the system response and team alertness to counter real incidents

- **Standard Operating Procedures** – SOPs are one of the common elements that are missing in large installations, drafting of SOPs and reviewing of the same should be a common practice

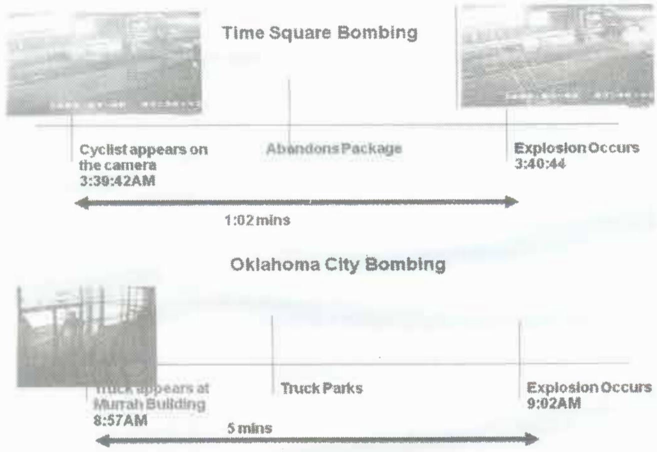
Let's look at one of the city wide surveillance incident and response timelines:

#	Date (2002)	Location	Fatality
1	October 2	Glenmont, MD	1 person
2	Oct 2	MD	No injury
3	Oct 3, 7.41	Rockville, MD	1 person
3	8:12 AM	Aspen Hill, MD	1 person
4	8.37AM	Aspen Hill,MD	1 person
5	9.58AM	Kensington, MD	1 person
6	9.15PM	Kalmia Rd, DC	1 person
6	Oct 4, 2.30PM	Spotsylvania, VA	1 injured
7	Oct 7, 8.09AM	Bowie, MD	1 injured
8	Oct 9, 8.18PM	Pr William Cty, VA	1 person
9	Oct 11, 9.30AM	Spotsylvania, VA	1 person
10	Oct 14, 9.15PM	Fairfax County, VA	1 person
11	Oct 19, 8PM	Ashland, VA	1 person
12	Oct 22, 5.56AM	Aspen Hill, MD	1 person
13	Oct 23	Ballistics Results	
14	Oct 24	Muhammad & Malvo	Arrested

Over a period of 20 days, culprit was killing people one-by-one and surveillance cameras were giving reactive videos for forensic investigation. If there was some real-time assessment it could have saved lives.



Over a span of 3 minutes, incident happened and rest all is reactive assessment.



About Author

Shri Dhruva Khanna having more than 10 years of experience in information technology spanning areas of IT management, IT infrastructure consulting, IT security infrastructure and Physical Security Infrastructure design, project management, practice management & presales. More than 6 years of focused experience on providing consulting services around ISMS, Video Analytics, Speed Detection, Command & Control Centre, security technologies, tools and security architecture. Shri Khanna having experience in Conducting (in a professional capacity) trainings on behalf of British Standard on ISO LI & LA projects. Experience in managing professional services practice, managing functional reporting of people, recruitment (campus and lateral), services development, processes development, setting KRA, etc.

He has spans various industry verticals such as Airports, Government Undertaking, Banking & Financial Services, Insurance, Life Sciences, Oil & Gas, Media and Technology.

He obtained executive Masters in IT from IIM Calcutta, Executive Masters in Planning & Entrepreneurship from IIPM Delhi. He is certified Tutor for ISMS (ISO27001) LI & LA from British Standard post completing transition course. BS7799 Lead Auditor and ISMS Implementation from British Standards Institute - India (2004).

Contact

[1] e-mail : dhruv.khanna@aujas.com
Mobile : 9711133837

[2] e-mail : alok.sardana@aujas.com
Mobile : 9711404321

Role of ICT in War against Terror Surveillance and Sensors

Lt Col Malay Sankar Pal

Abstract

The India centric paranoia of Pakistan based on its geo-political strategic considerations as well as its lack of parity in terms of conventional military force with India will always keep the option open for low intensity conflict. Terrorism is one of the most effective tools that Pakistan has tried to use for over a decade mostly in J&K but now spreading it to other parts of the country as well – the Mumbai carnage on 26/11 being the last such act.

Therefore India as a country must keep up its vigil and take every possible action to thwart any such act in future.

Keeping in view the giant strides taken in the field of ICT there is immense scope to develop effective counter terrorism steps. This paper has endeavoured to explore the scope of realizing an effective surveillance system integrated by an access backbone network which can be made secured, scalable and dynamic enough to cater for fluid situations during an operation. It would be important however to develop an operational doctrine to synergize multiple agencies involved in such operation and a server system to cater for both command and control imperatives as well as access to info on a need to know basis.

Overall the surveillance system should conform to some basic principles and the application of ICT techniques should be congruent to these principles.

Preface

The advent of digital technology induced Information and Communication Technology (ICT) has become a two way tool – on one hand it has shrunk the world to turn it into a global village. Along with proliferation of democracy and market economy world over these tools are becoming extremely powerful to redress various socio-economic ills plaguing the humanity – be it health, education, infrastructure, communication in all its forms etc. But on the other hand these are also falling in wrong hands with malignant minds and thereby posing a serious threat to all the existential ethos and parameters of human being.

The problem is further exacerbated by the fact that some nation states are trying to calibrate their strategic interest with a subjective evaluation of their long term goals. This in turn has two connotations:–

Firstly, it leads to over exploitation of natural resources of the under developed or developing countries by the so called developed ones which in turn puts these countries in a vicious loop of socio economic cesspool. The entire society thereby gets sucked in a spiraling abyss of social anarchy – as is being witnessed in a large number of sub-Saharan countries and banana republics in South America even till date.

Secondly, countries with dogmatic philosophy, as is being witnessed in Middle East theocratic countries, are taking a sovereign position to define their strategic interests. As part of this policy, these countries are increasingly resorting to methods which jeopardize the regional security in short term but have the potential to threaten the world security in long term. The outcome of 9/11 is basically a direct fallout of such policies pursued by USA during cold war era and Afghanistan conflict.

All these developments outlined above are posing serious security threat which is being manifested through various acts of terrorism with, unfortunately, an Islamic tag to it. But in today's time the entire world is getting a taste of this scourge – be it the USA, an Islamic state like Indonesia, a communist country like China or Pakistan itself.

Given this background the necessity of addressing the problem has been well appreciated by all the countries and there are well coordinated moves initiated among the world community which are already showing discernible results. A pinpointed focus has also been put into place by the Obama administration in the form of Af-Pak policy. While Richard Holbrooke is fine tuning the actions taken by Pakistan in its FATA and Waziristan regions the presence of NATO forces in Afghanistan is helping the Karzai government to take on Taliban in a more effective manner.

Obviously there has been a better realization and appreciation of the problems emanating from the terrorist acts by the world community which will definitely scale down the intensity of such acts overall. But India will possibly have to live a bit longer with such scourge. With such a possibility always looming large it would be apt to take all possible actions to thwart repeat of any 26/11 style acts in any part of the country.

The doctrine of counter terrorism is already well developed by the Indian security establishment and is already in practice in J&K and northeastern states. But the use of ICT in this particular area will continue offering unending options since the technology in itself is still evolving exponentially and yet to mature. Keeping this in view this paper endeavours to focus on a specific aspect of counter terrorism tools viz. scope of application of surveillance and sensor grid using ICT.

Surveillance Philosophy

The act of counter terrorism has to begin with area domination which involves surveillance as the most major instrument. It can be easily appreciated that unless the population of the area of interest are not made accountable in terms of their availability and activities it would be impossible to discern the intention of any probable terror act and subsequent build up and execution of such an act. Keeping this in view the philosophy of surveillance has been evolved based on certain principles as enumerated below:-

1. **No gap pattern :** The surveillance grid should be defined in such a manner so that the entire area of interest is covered without any gap. Obviously such a gap will become a chink in the armour which will defeat the very purpose of it being set up.

2. **24 x 7 coverage :** Surveillance is always round the clock – time bound surveillance can be easily defeated by unscrupulous elements.

3. **Multi spectral coverage :** The surveillance grid should cater for all sources of probable intelligence viz. optical, electro-magnetic, radio, infra red, physical characteristics etc.

4. **Overlap :** Every sensor – man or machine – has a limitation of range along with a directional constraint. Therefore the deployment of these sensors should be such that the range and direction of each of these sensors are well coordinated so that there is no gap at the inter se boundaries of these sensors.

5. **Multi layered coverage :** Despite no gap pattern and overlapping of range there is every possibility of existence of blind spots in a given geographical area. The surveillance grid should be deployed in different layers so as to cater for such blind spots.

6. **Redundancy :** The sensor elements – whether man or machine – are always susceptible to failures without any prior notice. Therefore the system should cater for adequate reserve so that any failure can be plugged expeditiously.

7. **Mix of sensors :** As has been mentioned every sensor has its range as well as capability of detecting a particular target. Therefore a thorough appreciation should be done to evaluate the threat perception for a given area which in turn will dictate the selection of the range and depth of the sensors.

8. **Alternate positions :** The appreciation of threat perception will also dictate the location of sensors which may or may not conform to the actual ground condition. It might also be required to redeploy the sensors depending on the progress of certain operation. In any such contingencies there should be alternate positions already earmarked so that the sensors can be relocated without any adverse bearing on the operation.

9. **Secondary task :** While each sensor will be cut out for a primary task but there should be a secondary task defined so as to cater for a contingency situation, particularly during the conduct of a given operation.

10. **Command and control hierarchy :** The information gathered through surveillance is both voluminous as well as fluid. Also the basic intelligence may be laden with a lot of unwanted information which needs to be filtered and collated. Obviously the collation, processing and lateral / vertical communication of the information as operable intelligence is an issue of centralized command and control of the surveillance grid.

Factors influencing surveillance

As can be appreciated from the principles of surveillance outlined above the establishment of a robust and operationally viable surveillance grid is influenced by a mix of technical and tactical factors which can be summarized as below:-

1. **Technical factors :** These factors include intended target and its resolution, distance covered, noise immunity, ability to function in all weather and all terrain condition, output format, compatibility for networking, portability, ECM signature and ECCM capability, power and other administrative requirements, capability of working in unmanned mode, self diagnostics and other smart operational features, requirements of training etc. A balance should be weighed between contradictory requirements viz. long range, low power and weight requirements, ease of detection etc.

2. **Tactical factors :** The appreciation of threat perception is the biggest deciding factor for tactical

considerations. Apart from this other factors e.g. operational objectives, situational awareness, balance of force, enemy activities, availability of local resources, logistics involved will also play significant role in deciding a surveillance grid.

3. **Ground condition :** Essentially this forms part of the tactical considerations outlined above but being mentioned here separately to highlight the important role it plays in influencing a commander's tactical decisions. In case of India our country is endowed with diverse geophysical features which define its borders with its neighbours – a desert, mountainous terrain with thick forest and a long coastal line. As has been demonstrated by the incidents in J&K and North east as well as the act of 26/11 in Mumbai, geographical features are no obstructions for terrorists to infiltrate and mount their attacks. Also the infiltration routes are not direct anymore – in fact a large number of these subversive elements are finding their path through the porous border of Nepal and Bangladesh.

Therefore when one thinks about a surveillance grid it has to be a holistic and all encompassing approach so that the basic principles of the surveillance are preserved in all respect. Keeping this in view an attempt is now made to suggest the components of surveillance to cater for various geo locations.

Components of Surveillance grid

As has already been brought out the selection of the surveillance components i.e. the sensors will be influenced by both technical and tactical considerations which in turn will necessitate selecting these sensors to cater for a given situation. Obviously the solution will involve selecting a mix of sensors which will have to be deployed in an array conforming to the principles of surveillance.

Given this imperative an attempt is now made to enumerate the possible components along with their format of output:-

Sl No.	Component	Output Format
1.	**Humint :** Human intelligence components comprising of spies and moles, border outposts, reconnaissance elements – land, air and water etc.	Radio transcripts, text mails and signals, voice recordings, visual recordings
2.	**Population control measures :** Census, permit based food and drug distribution, license for use of land, identity cards, regulation of movement through check posts, registration of foreigners, periodic cordon and search, random frisking etc.	As above
3.	**Radars :** A slew of radars have been developed to track movement of animals to high speed fighter aircrafts and even locating mortars and artillery. With over the horizon and high resolution capability these radars are offering a tremendous scope of all weather long range surveillance. The AWACS capability extends the scope of surveillance deep into the enemy territory.	Text giving azimuth and elevation information correlating the grid reference of a particular location.
4.	**Cameras :** The most effective and legally acceptable tool, particularly for a given establishment or a localized area. Constrained by ambient light and weather conditions as well as clear field of sight. Susceptible to guises.	Visual recordings with optional audio
5.	**Special cameras :** Thermal imagers and infrared cameras offer excellent options to get over the constraints of normal cameras. These offer images during dark conditions in terrains covered by dense forest and thick foliage as well as through cloudy conditions.	Visual recordings, text giving location information
6.	**GPS :** A matured and stable technology defining own position at any corner of the world. Also can be effectively used for tracking own force	Text giving location information

Sl No.	Component	Output Format
7.	**Electronic warfare :** Most effective tools to track hostile radio activities with pinpoint localization capability. An EW grid can track all sorts of communication and non-communication activities e.g. radar, radio control of UAVs etc. and give localization even upto 12 digit grid reference.	Radio transcripts, voice recording, text giving location information as well as technical parameters of target transmission
8.	**Aerostats :** These are balloons carrying specific sensor e.g. camera etc. which can be deployed for vertical surveillance.	Visual recordings, real time streaming, text
9.	**UAVs and Drones :** Favourite with the NATO forces in its ongoing fight against Al-Qaida and Taliban forces in Afghanistan and Pakistan, these offer excellent scope for both search and destroy missions. Fitted with slew of cameras these can offer excellent opportunity to keep vigil over the target area and track any unusual activity. Capability to carry and launch missiles and bombs adds further teeth to its operational capabilities. However these have some critical constraints in terms of ECM signature and vulnerability to weather conditions.	Both text and visuals through recording and real time streaming with the Ground Control Station.
10.	**Satellites :** The ultimate birds in the sky with high resolution cameras and radars, these are the ultimate tools for area surveillance. Cost and political considerations are the biggest constraints to exploit their capabilities	As above
11.	**Tele logs :** As has been demonstrated during the Mumbai carnage on 26/11 the terrorists are heavily dependent on cellular and satellite telephony for their decision support system during an operation. Therefore tele logs, both pre and post operation, can offer valuable linkage to the perpetrators and master minds, as has been the case in case of Mumbai carnage.	Radio transcripts, voice recordings, text information giving call details
12.	**Sensor array :** Though may sound like a typical James Bond, movie concepts like nano soldiers – robots with specific capability to sniff a target based on parameters e.g. imagery, odour, vibration, texture etc are very much on the anvil. These are now being trial tested to establish operational efficacy. This will in turn force redefining the operational doctrine – both conventional as well as counter terrorism.	Text, visuals, radio transcripts
13.	**Biometric passports :** Already countries like UK has taken concrete steps to introduce these passports and other countries are bound to follow suit. Once the system matures in each country and if finally integrated under the aegis of UN then security agencies can effectively access this information through Interpol.	Text, static graphics

The components enumerated above have mostly been developed and a few e.g. nano robots are in advanced stage of development. Also these have been developed with due compliance to networking and other digital standards and protocols. Of course for the humint there would be a requirement of physically punching the information through a computer interface. Overall these components offer an excellent collection of voluminous information which can be shared, warehoused and processed at various levels of command and control hierarchy – thus making a decision support system on near real time basis. This is where the latest techniques of ICT can be exploited to acquire, share, process and finally give rise to operable intelligence which can be disseminated to the last man in the security pipeline.

Given this potential of ICT the following will be required to fully exploit the information emanating from the sensor components:-

1. A communication network for vertical and lateral transfer of the information.
2. A server system for effective command and control hierarchy to regulate flow of information.
3. A server system for information processing and decision support system.
4. War gaming.
5. Security.

Let's now have a brief overview of each of these components.

Communication network

Given the widely diverse nature of information acquired and its dissemination to a wide variety of users in the form of security agencies involving both military as well as civil – the communication network should have the following major characteristics:-

1. Avoid the bottlenecks of current communication systems viz.

   (a) Poor spectrum utilization.

   (b) Low date transfer rates.

   (c) Pre-defined mission planning.

   (d) Intentional and unintentional jamming environment.

   (e) Lack of coordination among various security and civilian networks.

2. Use an integrated hybrid network which relies on an area based terrestrial network and a satellite based celestial network. The interface for these two networks should be through the Tactical Services Gateways.
3. Use of Next Generation Network (NGN) technology based on IPv6.
4. Must cover the full spectrum of conflict and varying terrain.
5. Ensure high information assurance by making it jam resistant.
6. Adequate ECCM measures to avoid detection, localization and identification by hostile EW means.
7. Adopt the latest techniques e.g. cognitive radio system, software defined radio, bandwidth harvesting, Mobile Adhoc Network (MANET) etc. to optimize the throughput as well as channel utilization.
8. The last mile connectivity should be based on cellular communication techniques to cater for fluid and flexible nature of counter terrorism operations.

Command and control server system : It should be appreciated that any operation – whether conventional or counter terrorism – involves a multi layered hierarchy for effective command and control chain connecting the foot soldier to the highest Commander. The situation is slightly more critical in case of counter terrorism since it may involve agencies of different hues – armed forces i.e. Army, Navy, Air Force, special forces like National Security Guards, central forces e.g. CRPF, BSF or CISF and of course the state police. In such a situation the access to the information and its dissemination has to be based on a defined operational doctrine which has to cater for various contingencies and role of each of these agencies in such situations. Obviously the flow of info and access to it should be based on the need to know. Accordingly the server has to cater for each of such contingencies defined in the operational doctrine.

Decision support server system : Similarly the decision support system for a multi agency operational doctrine is also a critical aspect which the server must cater for.

War gaming : The servers should also make provision for extensive war gaming to hone the state of operational preparedness.

Security : The concerns of security remain the biggest bugbear for all security agencies – particularly with increasing dependence on network centric functional environment and simultaneous increase in cyber terrorism. With the NGN (Next Generation Networks) now a reality there should be a well defined network security strategy in place to synergize the technological advancements with the threat perceptions. A few recommended steps in this regard are as follows:-

1. The strategy should be based on fundamentals of cyber security viz. Authentication, Access control, Secure storage and retrieval, Secure communication, Logging and auditing, Integrity check, Intrusion detection and response, Non repudiation, Physical and General aspects e.g. hardening, SOPs, classification etc.

2. There should be a national level security framework encompassing the following issues:-

(a) Assessment of threats – both internal and external.

(b) Interfacing issues between diverse networks.

(c) Interfacing issues between the media and services.

(d) Solution for end-to-end security.

(e) Key management issues.

(f) QoS and latency requirements for various types of traffic.

3. Cryptographic algorithms should be user upgradable in the field to address compromises.

4. There should be a centralized framework to address issues concerning key change synchronization and accordingly promulgate security policies.

5. Should be platform independent for processing.

6. Judicious mix of security overlay and embedded security.

Keeping in view the above mentioned strategic imperatives the following solutions are suggested:-

1. Communication centres should be secured through mil grade VPN tunnels. Different routes can use different cryptographic engines.

2. Judicious use of conventional tools e.g. intrusion detection and prevention, Firewalls, Antivirus, Anti spam, Bulk encryption units etc.

3. A 'Time server' for time synchronization of all crypto units in the network. Key change operation must be time synchronized across the network.

4. Robust key distribution mechanism to update the keys and crypto algorithm in case of a compromise in security.

5. Strong challenge response based authentication in the subscriber terminals, preferably with multi factor biometrics based access control.

6. Gateways should provide interoperability **only** at the protocol conversion and signaling translation level and **never** at crypto translation levels.

7. Subscriber terminals should implement end-to-end encryption of all payloads viz. voice, video conferencing and data. The following issues assume particular importance in this regard:-

(a) The traffic must not be decrypted and re-encrypted anywhere in the network.

(b) Should work transparently including end-to-end encryption irrespective of the underlying technology deployed e.g. PSTN, GSM, CDMA, IP Broadband, mil network etc.

(c) The convention tools i.e. firewalls or intrusion prevention systems along with a traffic shaper and QoS engine should prioritize various types and grades of traffic on the network.

8. Use militarized VoIP protocol for voice encryption which should originate a pre-designated prioritized packet from the subscriber terminal.

9. Only plain voice calls should be delivered through IP PBX and voice multiplexers.

Conclusion

The ICT techniques concerning info acquisition, collation, processing and sharing in a secured manner have progressed to a very large extent. The scope remains unbounded since the IP based networking has not yet been able to make any progress regarding migration to IPv6 from the existing IPv4 based networking. Once that happens the QoS level will have a paradigm shift – both in terms of service as well as security. The potential of NGN, still mostly at conceptual stage, can only be fully unfurled with such migration to IPv6.

Given this prospect there is a tremendous opportunity to develop a sound counter terrorism operational doctrine and realize it applying ICT tools. A lot of progress in this regard has already been done by the military R&D organizations like DARPA in the form of Battle Field Management system. Similarly there has been a tremendous progress in the field of developing support hardware as well in this regard.

Keeping in view such developments as well as the India centric paranoid obsession of Pakistan, the call of the hour would be an intimately coordinated synergy between the operational planners, R&D organizations and the industry so that a robust counter terrorism system can be realized as expeditiously as possible.

It is definitely not a welcome proposition to have another 26/11 like carnage.

Contact
email : ms_pal267@rediffmail.com
Mobile : 09868385140

ICT and War Against Terror

K M Paul

Abstract

Destructive applications of ICT are as strong as the global ICT is. A strong R&D base in this field is indispensible, which will have continuous knowledge update of the global ICT; assess their possible destructive uses and develop the necessary deservents, by pulling up national resources in the field of communication, broadcasting and software. ITU is engaged in a number of study programmes in the field which will help generation of awareness about the matter; give necessary knowledge of cybercrime, cyber-security, required legal and regulatory frame work and also the details of 'Critical Information Infrastructure Protection, (CIIP) – for all member-nations, specially the developing nations. Since threats of trrorism is a global issue, it needs very close international co-operation in exchanging information and harmonising the legal frameworks for effectively combatting the threats of terrorism.

Background

Information and Communication Technology (ICT) has assumed so much importance in building up the human society that the United Nations (UN) / ITU organized the **'World Summit on Information Society'(WSIS)**, first in Geneva, in December 2003 and later in Tunis, in November 2005. The world convention was attended by - Heads of Member States; Sector Members; Chief Executives of UN Organs as well as the Heads of Media Sectors. The mission of the convention was to explore – How ICT can be used for development of human society, by way of combating – Poverty; Hunger; Disease; Illiteracy; Environmental Degradation; Gender Inequalities; etc.

While on one side the human society is planning to exploit the benefits of the ICT for the development of the human race; on the other side the same strength of ICT is being used by the Negative Forces for the destruction of mankind and its creations on this planet. These two contradictory forces are moving side by side with opposite missions.. The strengths of ICT are all in public domain. So the Negative Forces are as strong as the ICT is. It also appears that such Negative Forces have come to stay. It is therefore necessary that whenever some new strength of ICT is developed, it must be remembered that such strength will be used by the Negative Forces for the destructions also. So along with the ICT developmental activities, we must at the same time give thoughts for developing frameworks for the necessary- **Cyber Security and 'Critical Information Infrastructure Protection (CIIP).** This is a continuous process and is a global issue.

Tele-communications and Tele-control using - internet, satellite, GPS system and computer technology have become common features of today's ICT. Exactly the same ICT facilities are being used by the Negative Forces for Terrorism and all destructive activities throughout the world. It has become the standing responsibility of all national Govts. and their concerned Technical Wings to protect all their strategic areas and Critical Information Infrastructures from these destructive forces by deploying appropriate deterrent ICT systems.

Strengthen RAW R&D

Terrorism is directly linked with the safety and security of the country. Therefore the country's highest intelligence analysis wing like – RAW; FBI; etc. (or any other exclusive and dedicated national establishment) should have one of the strongest R&D Wings particularly in the field of ICT. Apart from the routine operational activities like –monitoring, interception, intelligence analysis, etc. its core R&D Group should be engaged in finding out the latest ICT developments around the world and developing the required deterrents against all possible anti-development usage of those new ICT developments.

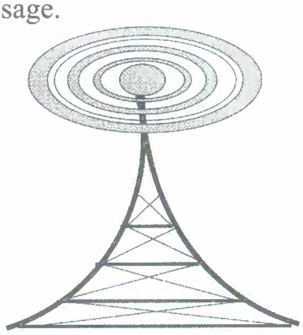
This is obviously a giant task no doubt. But in today's critical terror situations in and outside the country, this is a very important ICT activity in our 'war against terror'. Any matter concerning the Safety & Security of the country is of prime importance. If there is no security of the country , then the very existence of the country is in question. When the implication is so serious then we should never hesitate to attach maximum importance to this matter. In fact country's best scientists and engineers should be engaged in developing these deterrent ICT systems. For finding out the latest ICT developments, the R&D Wing has to have a very close and up-to-date linkage with the concerned agencies of different countries. Likewise for development of deterrent ICT systems as well, they have to maintain similar dynamic global linkages. This R&D is an important part of the activities of the RAW. It must be taken up on priority and results delivered in an objective manner without getting lost and mixed up in the usual routine and bureaucratic process of Govt. departments.

In order to get the services of best scientists and engineers, for this job, Govt. has to make the necessary framework, so that the best people are attracted towards this service. The R&D activities in this field is primarily based on computer software, in which India is a global giant. Therefore India can be a world leader in this field, provided things are mobilized in a planned and objective manner with full political will and determination. Targeted output as per plan must be achieved. It must not be supplanted by - creating only the infrastructures; writing only big reports; holding big meetings / conferences or showing plea for non-performance.

Role of Broadcasting

In the event of some Terrorist attack or Disaster there may often be a need to make urgent communications, sometimes interactive communications with the public in general. For such an urgent mass-communication, there is no substitute of Broadcasting. Interactive Mobile TV (MTV) Broadcasting is poised to be launched in the country in a big way. The system permits Broad Band (BB) operation, allowing delivery of streaming video signal . This MTV will prove to be one of the best mass communications networks in case of emergencies. Being mobile reception, it will instantly draw the attention of the masses by providing audio-video message. Being an interactive system, the peopie also would be able to interact with the broadcast centre and if necessary send in the upstream, multimedia contents from the site wherever they may be. Being a BB wireless media, the Mobile TV B'cast system will be a very useful ICT tool in the fight against 'Terror' and any type of disaster.

A communication control system can be devised by which, in the event of any emergency arising out of Terrorist Event or Disaster, an urgent public message can be instantly disseminated to the masses countrywide using the vast countrywide network of broadcasting. The control system will be so devised that in the event of such exigencies, the normal radio / TV programmes will be bypassed and overridden by the audio / video emergency message.



Broadcasting – Most Powerful Mass Communication Media; Specially in Emergency

If necessary this overriding control can be exercised by the concerned national security administration for all the Radio and Television broadcast transmitters in the country whether private or govt., simultaneously. With this type of mass communication arrangement the whole nation can be addressed / alerted instantly with any emergency message.

Dedicated Communications and Special Surveillance Network

A fail-safe reliable dedicated communications network should be available to the National Security Administration through which any senior official can be contacted any time anywhere throughout the country. The network should be able to connect all stationary or mobile receiving positions throughout the country- including border areas; remote hilly areas and highways.

Such a dedicated BB communication network covering the whole country , will be extremely useful in the event of any urgent need for a countrywide multipoint communications at the time of any unforeseen emergency like – Terror strike or any Disaster –natural or man-made.

In addition to communications, there is need to setup a Special Surveillance Network. All Strategic Areas ; Critical Infrastructures ; Sensitive Data Banks and important Cyber Sections in the country- all should be brought under a special electronic surveillance network with constant electronic as well as manual monitoring. Kargil War reminds us, how devastating can be the results of lack of surveillance in sensitive areas. High Altitude Balloons providing 'Lighter-Than-Air-Surveillance' for – law enforcement, homeland security, facility protection and border security can be

View of earth from a High Altitude Balloon (~30 k.m. high)

The heights of such balloons are generally from 20 km to 30 km. It being at heights above airspace ceiling of 20 km, will not interfere with air traffic. A balloon at a height of 20 km will have a typical footprint diameter of about 800 km.

A Special surveillance network comprising – High Altitude Balloons, Surveillance Satellites as well as Land based Surveillance system is required to be deployed to exercise constant monitoring of the- sensitive border areas; long coastal line as well as all in-land sensitive areas of the country.

Surveillance Satellite on earth orbit

The countrywide network evolved out of this exercise could be a hybrid system having a linkage through – ground based; satellite based as well as high altitude blloon based systems which could be used both for surveillance and emergency communications.

Spectrum ; Legal and Regulatory

In implementing the required ICT infrastructure for the 'war against terror', there may be need for an exclusive RF Spectrum; a new Legal and a Regulatory framework.

National Administration should attach priority to this requirement and act to put them in place on war emergency basis, because **managing terrorism is also a war; may be more serious than the conventional war on the border.** Here the enemy is not visible; neither the time of strike nor the place of strike are known. That is why, this is a more serious war, requiring – Accurate Intelligence, High Technical Competence in the field of ICT and a very good ICT Infrastructure along with the necessary Legal and Regulatory framework.

ITU-D ICT Applications and Cybersecurity Division

The ICT Applications and Cybersecurity Division (CYB) are the focal points of the ITU Telecommunication Development Sector (ITU-D). It is to assist developing countries in bridging the digital divide by advancing the use of ICT-based networks, services, applications and promoting cyber security.

The Division has overall coordination responsibility for 'Programme 3' of the 'Doha Action Plan' adopted at the 2006 'World Tele-communication Development Conference'(WTDC).

ITU-D Study Question- 22/1 was adopted in the conference for surveying, cataloguing, and raising awareness of – (i) Securing information and communication networks: best practices for developing a culture of cyber security (ii) Call for member states and sector members to create a report on best practices in the field of cybersecurity – in a study cycle of four years. Priority activities include promoting cybersecurity, e-Strategies, ICT applications, Internet and IP networks development, multilingualization and community telecentres.

ITU-D Study question 22/1 Draft Report (September 2007) gives 5 key elements to a good national cybersecurity programme : (i) A national strategy (ii) A sound legal foundation to deter cybercrime (iii) A national incident management capability (iv) Collaboration between Govt. and Industry (v) A national awareness of the importance of a culture of cybersecurity.

ITU-D National Cybersecurity/Critical Information Infrastructure Protection(CIIP); Self - Assessment Toolkit

To prepare documents on Framework of Best Practice, based on Study Question 22/1. The activities are to focus on national management and policy level. The activities are intended to assist the national administrations to – (I) understand existing approach (ii) compare to best practices (iii) identify areas for attention (iv) prioritise national efforts.

ITU-T Study Group 17 - Security

ITU-T continues studies in the field of telecommunications security to secure network infrastructure, services and applications. Over seventy standards (Recommendations) concerning 'security' have been published. One of the important standards in wide use today is the ITU-T Recommendation X.509 for electronic authentication over public networks. X.509 is widely used in applications securing connection between a browser and web-server, providing digital signatures that enables e-commerce transactions.

Study Group 17's Recommendation X.805 will enable the telecom. operators to provide an end to end architecture description from a security perspective. The Recommendation will allow operators to pinpoint all vulnerable points in a network and mitigate them.

ITU-R – Disaster Management and Cybersecurity

Telecommunication is critical in all phases of disaster management. In many a disaster situations when the 'wired' telecommunication system is destroyed, the 'wireless' or Radio-communication services (land based or satellite based) become indispensable and can not be supplanted by any other means. ITU-R has two major tasks – (i) to ensure effective use of radio frequency spectrum and (ii) to conduct studies concerning development of Radio-communication systems including systems used in disaster management .The Radio-communication Assembly 2007 (RA-07) approved Resolutions – ITU-R 53 and ITU-R 55 instructing all ITU-R Study Groups (SG's) to carryout studies on the use of radio-communications on 'DISASTER MANAGEMENT'. SECURITY problems are mentioned in the following Series 'S' ITU-R Recommendations:

- S.1250 : Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed satellite service.
- S.1711 : Performance enhancements of transmission control protocol over satellite networks.
- Various other security related Recommen-dations are:
- Recommendation 1078 : security problems for IMT-2000
- Recommendation 1223 : evaluation of security mechanisms for IMT-2000
- Various other texts on systems beyond IMT-2000 and software defined radio also raise the importance of security, e.g. Recommendation M.1645 and Report M.2063.

ITU Cybercrime Lagislation Resources

The purpose of ITU's dedicated 'Cybercrime Legislation Resources' is to assist countries in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks. It addresses the first of the seven strategic goals of the **ITU Global Cybersecurity Agenda (GCA)** which calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.

The adoption by all countries of appropriate legislation against the misuse of information and communication technologies for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation. The ITU 'Cybercrime Legislation Resources' include two separate components: a publication on **Understanding Cybercrime: A Guide for Developing Countries** and a **Toolkit for Cybercrime Legislation**.This is the need of the day. The terrorism appears to have come to stay. The society has to survive with this menace and therefore always keep ready to face this undeclared war. For doing so, the Govt. must place a strong ICT Infrastructure in position, backed by competent technical manpower. The Infrastructure will need continuous updating and the supporting manpower will require continuous alertness and refreshing the knowledge with the latest ICT .

CONCLUSION

Number of seminar, symposium and conference on the subject will continue to be held. But at the same time Govt. should immediately act on framing the action plan to exploit all the benefits of ICT in fighting the Terrorism and to ensure the maximum possible safety and security of the country – its people, its critical infrastructures and other national assets. Though the safety-security of the critical Information infrastructures and cyber security are the shared responsibility of - Govt., corporate sector other organizations and indivisuals; it remains that Govt.must establish the necessary framework to – (i) assign the specific responsibilities (ii) bring up the required legislations and clear regulatory guidelines (iii) do the overall system planning and monitoring. All the action plans are required to be implemented in a strictly time bound manner avoiding bureaucratic clutches of the Govt machinery. Nothing should be considered only as a ritual and limited only to a report making activity like many of our R&D projects in the country.All activities have long term importance and hence should be time bound; sustainable and forward compatible.

About the author

Shri K.M. Paul is the former Engineer-In-Chief and Acting Director General, ALL INDIA RADIO (AIR). He served the Public Broadcaster for 35 years for the development of broadcasting in India He served-International Telecommunication Union (ITU)-Study Group 6 (for Broadcasting) as its Vice-Chairman; European Broadcasting Union (EBU) as member of DAB 'Specialists 'Group'; Asia-Pacific Tele-community (APT) as its 'Mission Expert' and the Asia-Pacific Broadcasting Union (ABU) in implementing its various projects. Shri Paul obtained his Bachelor's Degree & Master's Degree in Electronics & Telecommunication Engg. from Jadavpur University, Kolkata in 1967&1969 respectively. He is- the Member PAC of the DST; Member ICA; Sr. Adviser Broadcast Engg. and the Life Fellow of the IETE and the BES(I).

Contact

e-mail : kmpaul_2000rediffmail.com
Mobile : 09968927338

Modern Communication Networks TETRA to counter Terrorist Activities in India

Dr V Gunasekhar Reddy

Abstract

Terrorism is a modern ware fare. India has been affected by several terrorists attacks over the past several years, causing huge devastation and loss to Human lives, property and infrastructure and thus posing severe threat to internal and external security. Recent attacks on Parliament ,Mumbai attacks, Jaipur attacks, Hyderabad Gokulchat bomb blasts are some major devastations. The terrorists acts are from internal or external agencies. The domestic threats from internal agencies which are arising due to separatists movements, ethnic, socioeconomic differences. The domestic threat agencies are often supported by external agencies in providing funding, weapons, explosives and training. External terrorists threats like Jihadi terrorism are more predominant. Terrorists and terrorism are two different entities. we need to severely curb terrorists but terrorism can be fought only based on the mind set of the people who are encouraging terrorist activities. Religious fanatics need to be isolated then only the terrorism is bound to suffer and can be brought under control.

Science and technology for countering terrorism includes ensuring premature detonation of explosives or of inhibiting the triggering of explosives. Most Science and Technology counterterrorism tools are highly useful for public health, law enforcement, or general intelligence purposes. Much science and technology now useful for counterterrorism is embodied in systems in general use, such as the media of mass and selective and secure communications. Science and Technology cannot eliminate the problems of terrorism, but they can help in opposing it. There is a need for communications and information security. It is also predicted that ICT (Information and communications Technology), Biotechnology and Nano technology together could be more effective than ICT alone.ICT will be one of the several critical factors for the economic security in India. Increasing use of computers, Mobile phones are posing information and identity security threats.

There must be an efficient surveillance system with fast and secure communications networks. Public panic has to be controlled by providing appropriate and accurate information to the Media. The tactical communications interceptions applied against AlQueda operations in Afghanistan and Pakistan provided fruitful results to the US Govt. The extensive communications interceptions carried out by Andhara Pradesh Police on Naxalite movements helped in curbing their activities effectively. Emergency response communications is affected by different isolated communications links used by various agencies involved in antiterrorists activities. This hampers prompt command-and-control operations during intensive high impact terrorist outbreaks-wherein the situation demands many resources and personnel to be pooled effectively on very short notice.

This paper describes the latest UHF Digital trunking communication network-TETRA (Terrestrial Trunked Radio) which provides challenging communications tasks and applications like high secure communications, simultaneous voice and data transmission, Broadcast call , Priority channel over ride, GPS and GIS applications for Vehicle tracking, Picture and video applications. This also provides integration with existing VHF and land line communication links. Andhra Pradesh Police is the first Police Organization to induct this latest technology for Cyberabad Commissionarate and installation is being completed during 2009. Most of the Govt. Organizations in India are in the process of inducting this latest networks to provide effective communications systems to fight Terrorist activities.

India has been affected by several Terrorist attacks and attempts, for the past several years causing heavy loss of human life, devastation and destruction and posing threat to internal security.Few of them are attacks on Parliament, Mumbai Taj Mahal hotel, Attack on Gokul chat Hyderabad bomb blasts, Jaipur blasts etc. Terrorist acts may be by internal agencies or external agencies. The domestic threats (Internal) arising due to separatist movements, ethnic, religious, socio-economic differences. The domestic threat agencies are often supported by external agencies in providing weapons, explosives and training in extremist activities. External terrorist threats like Jihadi Terrorism is of great concern now a days.

Science and Technology will have to play a crucial role in the future in attacking terrorism as terrorism causes huge devastation and destruction. One important area to counter terrorism is communications. For Terrorist activities communication interception, the tactical communication interception adopted in USA against Alqueda operation in Afganistan and Pakistan provided fruitful results. The communication interception of Naxalites in A.P. yielded better results in curbing their activities. As there is more tendency by the terrorist to use science and Technology, they are more vulnerable for detection and elimination.

There is a need for highly secure communication and information security. It is also predicted that ICT, bio-technologies and nano technologies together could be more perilous than ICT along. In future IT will be one of several critical factors for the economic security in India, Mobile phones which are increasingly used can pose information, identity security threats. Information security is decisive to India as it is connected with economic security. In the area of information warefare-defensive, offensive and monitoring are the components. The defensive components are encryption/description devices, firewalls, secure protocols. The offensive components are scanners, sniffers, viruses, hard-ware, software bugs.

The monitoring component consists of communication interception, traffic analyzers, intrusion detection systems, communication intelligence, passive detection. Emergency response communications is affected by different isolated communication links between various Govt. organizations. This hamper prompt command and control operation during intense high impact terrorist out breaks where in many recourses and personnel to be pooled effectively on very short notice. Better intelligence is a more effective tool.

Terrorist and Terrorism are two different entities. We need to severely curb terrorist but terrorism can be fought and reduced only based on the mind set of the people and the society, who are encouraging terrorist activities. Religious formations need to be isolated, then only the terrorism is bound to suffer and can be bought under control.

Devices such as electronic interceptors, and jammers are crucial and can play vital role in fighting terrorism in India. Surveillance for counter terrorism - for movement of people. Authentication & Identified terrorism is a modern warefare. There must be an efficient surveillance system with rapid communication system. Public panic has to be controlled by providing appropriate and accurate information to the needy.

Science and Technology specific to countering terrorism includes the means of ensuring premature detonation of explosives or of inhibiting the triggering of explosives. Most Science and Technology counter terrorism tools are highly useful for public health, law enforcement or general intelligence purpose. Much Science and Technology now useful for counter terrorism is embodied in systems in general use, such as media of mass and selective communication. Science and technology cannot eliminate the problem of terrorism but they can help in opposing it.

This paper describes the latest communication networks needed for effective, quick and integrated secure communication inter connecting various Govt. and private agencies involved in handling anti terrorist activities.

The Modern digital UHF communications systems – TETRA provide these challenging tasks of unified communication channel, with broad cast facility, priority over ride GPS & GIS Automatic vehicle tracking, Voice, data, picture and video with high security. During 2008-09 A.P. Police, Cyberabad Commissionarate is the first Govt. agency to acquire and install this modern communication network. The advantages of TETRA Digital communication network is explained in detail in this paper as an effective communication back bone in extremist attacks.

TETRA (Terrestrial Trunked Radio) Trunking System

What is Radio Trunking

Trunking stands for sharing. Whenever resources are in short supply, they will have to be shared. In Radio Communications Trunking System a fixed number radio frequencies are used and are shared by large number of remote/ mobile subscribers. The frequency spectrum is a Scare resource. This is commonly known as Radio Trunking System.

Advantage of Digital Trunking System over Analogue Trunking System:

More reliable, flexible with low noise and provides internet connectivity.

Disadvantages of Digital Trunking System over Analogue Trunking System:

Only disadvantage is that they have low coverage range as compared with Analogue Trunking System. This can be overcome by more repeaters.

What is TETRA

Terrestrial Trunked Radio (TETRA) comprises a suite of open digital trunked radio standards used by Private Mobile Radio users such as Public Safety, Transportation, Utilities, Government, Commercial &

Industrial, Oil & Gas and Military etc. TETRA is an Interoperability standard that allows equipment from multiple vendors to interoperate with each other.

Frequency Range:

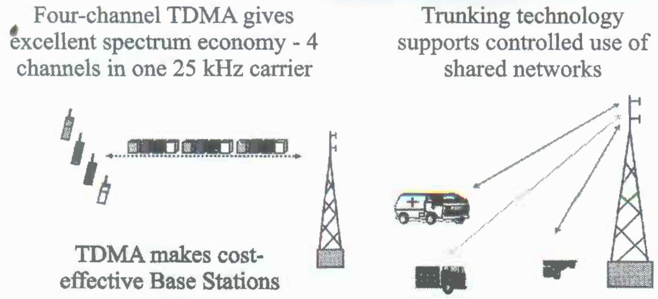
380 - 400 MHz for public safety systems,410 - 430 MHz & 800 MHz for commercial applications.

TETRA is superior PMR (Public Mobile Radio) technology

Provides individual, group and direct mode communications between radios, Packet data and fast data transfer services, Over-the-air programming of radios Frequency economy, Fast call set-up time, Security features & Encryption TETRA provides Voice and Data Services.

TETRA TDMA

One carrier with 24 kHz spacing provides 4 channels using TDMA (Time Division Multiple Access).Digital modulation, p/4 DQPSK at 36 kbits/s, Speech calls use one channel.Data calls can use up to 4 channels (Data transfer rates up to 7.2 kbit/ s per channel)


Four-channel TDMA gives excellent spectrum economy - 4 channels in one 25 kHz carrier
Trunking technology supports controlled use of shared networks
TDMA makes cost-effective Base Stations

Fi g:1 TETRA is the Cost - Effective Technology

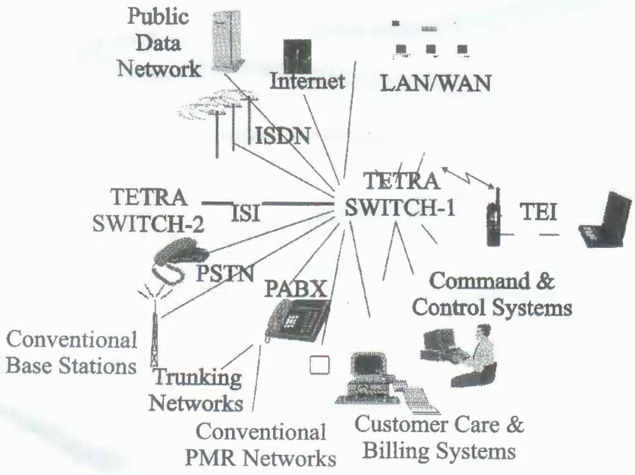

Public Data Network
Internet
LAN/WAN
ISDN
TETRA SWITCH-2
ISI
TETRA SWITCH-1
TEI
PSTN
PABX
Command & Control Systems
Conventional Base Stations
Trunking Networks
Conventional PMR Networks
Customer Care & Billing Systems

Fig:2 TETRA Connectivity

TETRA Call Types

Private call (individual call),Phone call (PSTN or PABX call),Group call, Emergency call, Any of the above types can be an emergency call Highest level of call priority, may pre-empt other users Call type and called party are pre-programmed Operated by pressing dedicated red emergency button, Broadcast calls.

Simplex Calls

Radio is either transmitting or receiving, Requires operation of PTT switch (Push To Talk),Talk time is usually limited, typically 1 minute maximum, Group calls are always simplex.

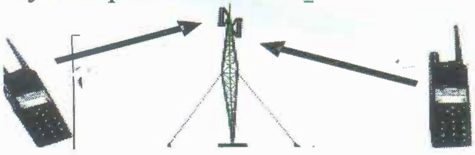


Fig:3 TETRA Traffic case - simplex calls

Duplex Calls

Radio is transmitting and receiving (like GSM phone call) Does not require holding PTT to continue transmission.

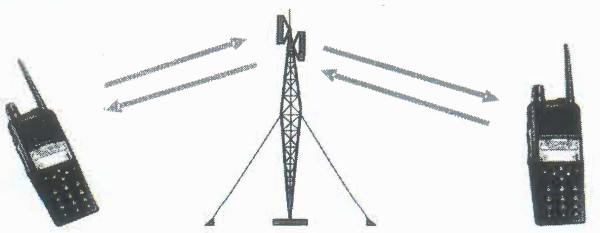


Fig4 TETRA Traffic case - duplex calls

TETRA Traffic case - Trunking options

Trunking options only apply to simplex calls, Applies to private simplex calls and group calls, Trunking type is controlled by the Base Station, Message trunking ,Transmission trunking

Advantages of TETRA Over IP

Future technology: Industry Standard IP Hardware and Software. Multimedia technology, combining voice, data and images. Continuous performance improvements driven by IP market.

Efficiency: Call processing is very efficient.

Flexibility: Any combination of Star or Mesh network topology is allowed in order to balance traffic handling

Resilience: Network elements and links can be duplicated for extra resilience.

Difference between GSM and TETRA System

GSM Systems

Designed for public cellular telephony. Based on Frequency Division Multiplication Access (FDMA), Not suitable for emergency services (Call set up time ~ a few seconds). Do not maintain privacy and mutual security. Direct Mode Operation (DMO) is not possible.

TETRA System

Designed for professional mobile radio applications. Based on Time Division Multiplication Access (TDMA) - Economy on frequency spectrum. Suitable for emergency services due to very fast call set up time (300 ms). Maintain privacy and mutual security. Direct Mode Operation (DMO) is possible, which supports voice and data transmission without a Base Station between Radio Terminals. Provides broadcast call service.

Summary:

In order to tackle terrorism, all the user agencies of Govt. and Private Organizations need to upgrade and integrate their communication infrastructure for secure, faster, reliable communications. This integrated network should be capable of providing unified command and control channels for voice, data and video applications in future.

About Author

Dr V Gunasekhar Reddy is Deputy Inspector General of Police & Addl. Director (Police Commns. Orgn.). He obtained Ph.D. in Physics (Mobile Communications); Master of Science – Physics (Electronics); Post Graduate Diploma in Business Management. He is fellow of Institution of Electronics & Telecommunication Engineers (India).

Presently he is Chairman IETE Hyderabad Centre for 2008-10; Fellow of IETE for the last 15 years. He is Actively participated in the activities of IETE Hyd. Centre for the last 15 years serving as Executive Committee Member & Treasurer for two Terms.

He has published & presented several papers.

Contact

e-mail : gelered@hotmail.com
Mobile : 09440627261

ICT in Crisis Management

Lt Col T Ravi Kumar Reddy

Abstract

Improving the quality of information and the use of information and communications systems in the field are not aims themselves but means to support the achievement of the political objectives, to rebuild institutions and infrastructure within a country to create conditions conducive to peace and development.

In this paper the role of information technology in crisis management will be discussed from two different perspectives. First, how we can use ICT to support the work of the international community in crisis areas and second, how we can support the recovery of local government in post-conflict countries with information technology. Finally the paper will bring out the key principles and recommendations on how to improve both the sharing of information in crisis situations and the tools to do that in a more secure and speedy manner.

The challenge

Over the past decade, the international community has responded to an increasing number of major political conflicts. The interventions have become ever more complex and multifaceted, extending from peace-enforcement to peace-keeping, from policing to nation-building, from humanitarian relief to reconstruction and development. Because of the width of this challenge, the crisis scene is crowded with multiple mediators, civilian agencies, military crisis management forces, development agencies, individuals, hundreds of NGOs, the media and private businesses, all seeking to make a change.In many cases, organisational relations and responsibilities are not necessarily clearly delineated – such as in the relations between military and civilian operators in both national and international emergencies. And as no single authority exists that can manage the various responders to crises, international peace-building efforts are often confused, difficult and even chaotic in the field.

In this chaos, the international community has a shared objective to stabilise and rebuild a country after a conflict. The aim of the international community is to leave behind a country with sustainable democratic structures, civil society, functioning rule of law and economy. Accomplishment of this objective requires efficient coordination of activities and sharing of information between organisations working in the field as well as access to new data and databases, such as images, maps, and geographical, building and infrastructure information. On the other hand the conflict often leaves the country devastated. In many cases in civil wars and ethnic conflicts it is a deliberate target to destroy both government infrastructure and databases and information. Particular targets are land and citizens registers – warring parties want to humiliate people by taking away their identity and property.

Improving the work of the international community

Information does play a vital role in humanitarian assistance and crisis management. The use of ICT can improve the effectiveness of the work of the international community in several different areas such as:

(a) Decision-making

(b) Institutional memory and knowledge management

(c) Coordination

(d) Situational awareness

Decision-making

Proper management of information and the resulting analysis of crisis situations are crucial for informed decision-making and the effective use of resources. In any crisis management situation, the critical factor in making timely, appropriate decisions is to have the benefit of the optimum amount of quality information. This information may come from a variety of sources that need to be integrated in an information system that is appropriate for the environment in which it is used. The situations on the ground are often extremely complex and volatile and can change rapidly without warning. A coherent and coordinated reaction can only be based on accurate information that must be produced and transmitted with speed and precision.

The reasons for the lack of good information during the post-conflict reconstruction phase according to the NGOs in Kabul, ranged from the sheer danger of being seen to possess technological equipment—*which made them targets of attacks to steal the equipment, resulting in their not taking equipment outside of Kabul or using it visibly inside the city*—to ignorance about the difference between agricultural and demographic maps and how the information they contain is not interchangeable and tantamount to misinformation, to the inability to receive current security information because of the firewall between classified and unclassified information among the civilian and military actors in the field. The outcome of all these short falls of information was poor security for the workers and thus poor service for the people inadequately served by the NGOs who lack critical information on which to act. A perilous situation for all concerned is the ultimate outcome of the lack of information interoperability.

Better use of ICT would provide access to critical, real-time decision-making information – getting information to people in a timely manner to save lives, limit damage and accelerate recovery. It has to be noted that no significant technical problems exist in the field of crisis management— only organizational obstacles and unwillingness to share information. These largely stem from policy and management issues inherent in the nature of organisations and bureaucracies. Resolving them is a gradual and fitful process, which naturally frustrates those attempting to introduce efficiencies through ICT practices and procedures.

Institutional memory – knowledge management : Crisis management operations are charaterised by a rapid turnover of staff. People are often working on the basis of a six month contract. Sometimes they are renewed, sometimes six months in crisis environment is more than enough for international civil servants. Often there is no handover period at all – the new officer arrives after the predecessor has departed. It is easy to imagine what kind of challenges this creates for information management and institutional memory in the organisations. And the effectiveness of the work suffers tremendously.

Institutional memory is related to the issue of "lessons learned," which organisations assemble from their last activity during a crisis as a review of their performance and what did or did not work. Although drawing up "lessons learned" by organisations from the military to the humanitarians has received universal support, to date few lessons have been systematically reviewed or institutionalised.

There is already more than enough capacity, and infrastructure is relatively inexpensive. However institutions still operate through business processes established before the information age. Vast amounts of information are stored on electronic media and exchanged over the Internet or intranets. But the main point is that the processes which allow this to be turned into useful information and intelligence are still very much in their infancy – most organisations do not know what they know. The technology to share information is there, but business drivers of knowledge sharing are still immature. Purchasing goods or paying people is relatively easy these days, but transforming data into intelligence is a business function that is much more complex, qualitative and requiring a high degree of sophisticated human thinking. The challenge is of information management, not of technology.

In addition to internal institutional memory, there is a lack of global institutional memory in crisis management. Past mistakes are repeated and lessons too often not learned. The particular role and function that the LLA fulfils is one that is becoming increasing important; that of critical policy input and analysis. For these purposes this ad hoc operation should be fully integrated into the institutional and operational structures of an operation. The temptation is to see interoperability only in terms of management of operational units (humanitarian, medical, etc) however the LLA illustrates the need for policy functions to be integrated and fully interoperable so that key decision makers at all levels are appraised of the necessary information.

Coordination : Crisis management involves the activities of a great number of agents confronting the same problems but lacking shared or consistent knowledge, coordination or communications technology or a common user culture. As a consequence, different organizations work wastefully on the same problems, plan and take decisions without consulting other organisations and without access to up-to-date or adequate knowledge. ICT would facilitate sharing of information and communication amongst multiple organisations and agencies. It would help to identify and reduce redundant efforts quickly. There are many examples of duplicate efforts going on in parallel, usually with the best of intentions. It is often required to develop manual systems in the first instance – simpler is better in most cases, especially in real-time situations. It should be recognised that nothing can be relied upon to work in emergency situations – what if there is no power, no Internet and so on. If there is power and water and other supplies, it may be possible to use ICT but in a non-connected manner. The number and diversity of actors and networks involved in crisis management creates multiple coordination challenges. Organisations working in crisis management at any level, whether governmental, intergovernmental or nongovernmental, are competing for resources. One implication of this state of affairs is that organisations will not invest in initiatives that do not deliver concrete returns to them.

Information sharing and coordination requires connectivity and interoperability. Each of the institutions is governed by specific information sharing policies and operates a range of technologies to implement those policies. In the absence of investment in interoperability, many such systems are likely to be incompatible between (and sometimes even within) organisations. This can become a particular obstacle for the effective coordination of crisis management within national governments – for example, in the area of response to flooding, which may require the mobilisation of resources from the military, civilian emergency services, government agencies responsible for preparedness, response and reconstruction, as well as non-governmental community groups and charity organisations.

There are three major barriers to establishing interoperability in this sense. The first is that between the different levels of crisis management – whether political, organisational, operational or technical – there are genuine issues of coherence in policy and practice, even within organisations. The second is that, within each of those different levels, for a number of reasons, there is frequently competition rather than co-operation. Crisis management is seen as a zero-sum game, where one actor's loss is another's gain – as opposed to an environment in which the value of resources can be multiplied by combining them. The third and final barrier is simply that the operational environment for organisations involved in crisis management works against longer term partnership and planning. During crises there is little time to allocate resources to this type of development; between crises there is plenty of time but few resources to invest in such preparation. In such instances, interoperability and information sharing 'problems' are often rooted in political, management and resource issues, rather than in significant technical obstacles. Organisational behavior based on these issues tends to subscribe to more traditional ways of thinking about information. Such attitudes reinforce the position that information is more valuable if it is restricted rather than shared – rather than recognising it as an asset whose value increases in direct relation to its distribution – and fails to realise the potential of information sharing as a route to building the organisation.

In many organisations, however, the recognition of information as a key organisational resource has begun to change this type of approach. It is actually in the self-interest of organisations to share information and to create systems that facilitate that sharing – for instance, for governments to ensure that their systems are in step with those of their regional neighbours and international partners. In this case, information sharing adds value to their existing resources (by combination with the information resources of other organisations) and thus increases their status as a key information resource for others. The value of sharing and combining information resources outweighs the transaction costs involved in working with other organisations.

Situational awareness : Proper use of ICT would also have great impact in improving situational awareness in crisis environment where dozens of actors work without knowing enough about each other's activities. The lack of information sharing and their associated tools have been noted as key contributing factor in some of the recent incidents resulting in death or injury of international personnel. The concerted use of ICT in crisis management can improve the safety and security of all crisis management personnel in crisis areas. Functioning information sharing between organizations improves situational awareness and creates opportunities for early-warning on threats and prevention of conflicts.

Support of the local governments and civil society in post-conflict countries

The final objectives in peace support operations and in crisis management are to restore and enhance local capacities and build sustainable and democratic societies. ICT used in international field operations could be transferred to the local authorities of the host country. The use of information technology is a feature of all societies, and a peaceful, modern, open and democratic society certainly should include constructive use of the potential of ICT both by the government and by civil society for the process of construction of good governance.

Crises are often a consequence of the failure of systems of governance and representation and natural disasters. The resolution of a crisis often lies in restoring domestic governance capacity. This may include the capacity to organise elections or the ability to deliver humanitarian aid in the event of a natural disaster. The implementation of ICT solutions to crisis management situations should be inclusive in their design to enable a transfer of governance capacities to domestic authorities, delivering governance and sustainability.

Today's new information and communication technologies would make it possible to develop new tools for peace-building that would allow people to take charge of their own destiny much sooner than is currently evident in the case of traditional assistance programmes. To develop such new tools would require an active partnership with the private sector to help international organizations to re-think peace-building operations, to improve its delivery mechanisms and to provide a better service to those we ultimately work for, people in post-conflict countries and failed states. Peace-keeping operations must first and foremost concentrate on creating an environment that enables local communities to mobilize local talent and respond quickly to basic local needs. These aspects make peace-building operations around the world similar enough to develop ready-made tools that would help provide such an enabling environment.

Modern ICT can help making these tools possible. These new technologies can provide readymade modules for managing and administering specific areas of activities such as managing local basic health administrations or local civil registrations. Those modules could be made easy-to handle so that local administrators could be trained relatively fast in using them. At the same time, they would allow central monitoring of activities by producing real-time reports. I would consider local ownership the most important aspect and a new civilian intervention tool must help handing-back of responsibility to local entities. There will simply be no peace-building without local people feeling that they are in charge and that they will have a stake in their own future. No number of international organisations, no quantities of international expertise and no size of external funding could compensate for a lack in local participation and ownership.

Key recommendations

I would like to make some recommendations how to improve the use of ICT in crisis management. At the political level, clearly understood frameworks for co-operation need to be put in place in order both to agree on policies for information-sharing and implement ICT standards to ensure that those policies can be acted on. ICT initiatives need to look at the commonalities between previous operations to predict what shape future demands might take and develop appropriate solutions based on those predictions.

The most important factor in the success of ICT implementation within organisations is investment – not just financial and human resources, but also in terms of management support based on recognition of the strategic importance of it. User involvement in the ICT development processes is a fundamental necessity. The most basic requirement for achieving good internal communication practices and interoperability among crisis managers is the need for the organisations to recognise, understand and communicate their needs to ICT solution. ICT projects must, in the final analysis, be based on needs. Only on the basis of *actual* needs can technology solve *actual* problems.

There are a number of key factors that will contribute to the successful introduction of ICT into the field. Amongst them are the following:

(a) Portability. Mobility is frequently vital for aid workers in the field, who cannot afford to be tied to an office-based system, and so ICT must be easy to transfer between locations.

(b) Durability. The rigours of a harsh working environment – during a natural disaster, or a conflict situation – mean that standard products may not be suitable.

(c) Flexibility. Proprietary software represents a dilemma to many organisations. Off-the shelf packages meet most of the needs of most organisations, but are limited when used by nontechnical staff.

(d) Simplicity. Products and services cannot afford to place additional learning burdens on field workers, and should minimise the need for training and support.

(e) Affordability. Funding constraints are a constant in field operations, and interventions must be low cost. Partnership with business is a precondition for secure, sustainable and up-dated ICT solutions for crisis management. The cost of developing own ICT systems is enormous and this forces organisations to look very hard at what is commercially available right from the start. In ICT, the private sector has a lot to offer to governments, international organisations and NGOs, and one key aspect of introducing ICT to crisis management is building relations with the private sector. ICT solutions for crisis management should be based on open standards and commercially available solutions and not tied to a certain provider.

(f) Standardisation: Information systems depend on standards – not just in terms of hardware and software, but also in terms of staff capacity – and the international community needs to move towards standardisation if it is to take advantage of ICT. Only standardisation at every stage in the information cycle will allow information to be integrated and compared across different organisations.

Conclusions

Improving the quality of information and the use of information and communications systems in the field are not aims themselves but means to support the achievement of the political objectives, to rebuild institutions and infrastructure within a
country to create conditions conducive to peace and development.

Contact : e-mail : majravi@gmail.com
Mobile : 0919717808408

Cyber Terrorism: Current Threats and Challenges

S S Sarma

Abstract

The Information infrastructure has become a critical asset of the organizations, businesses and the country. The cyber space is witnessing computer security threats such as virus, worms, website defacements and identity theft during past decade. The cyber security threat landscape is changing and cyber threats are now originating in an organized fashion from cyber criminals. Such acts of cyber terrorism are a growing threat to the cyber space and critical information infrastructure of nations. This paper examines current threats of cyber terrorism and methods of cyber criminals. The challenges in combating the cyber threats and possible solutions are highlighted from the technical and social perspective.

1. Introduction

The Information infrastructure has become a critical asset of the organizations. The Information Technology and Internet are now considered as an essential element of economic growth. As such, threats to information security and has adverse impact on the economic well being of the country. The cyber space comprising of interconnected networks and systems is becoming an essential medium for communication and flow of business information. Hence threats to information in the cyber space can be termed as cyber security threats. The impact of threats in physical world and cyber world are similar but the nature of these threats varies. Cyber terrorism has two aspects. One is the use of cyber space for the purpose of terrorist activities and second is attacks launched by cyber criminals on essential information infrastructure. The following sections examine the current trends in cyber security threats and methods used by cyber criminals to attack the information infrastructure.

2. Current Cyber Threats

The information infrastructure and cyber space comprise information, computer systems, telecommunication systems, operating systems, applications, websites, databases and network of computer systems. The information technology is developing rapidly and phenomenal changes are taking place in the way information is delivered to user's systems. As the information technology has developed rapidly, the threat landscape is also changing dynamically.

Significant threats to information security or computer security incidents that transpired over a period of last three decades are:

- Unauthorized access into computers/networks
- Website defacements/intrusions
- Malicious code such as virus, worm, Trojans, Bots and spyware
- Denial of service attacks
- Identity theft and phishing
- Spam

The computer security incidents are caused by hackers by exploiting vulnerabilities in operating systems, applications and protocols such as TCP/IP, DNS, FTP used for delivering different services etc. The trends of these computer security incidents are to be seen from three perspectives.

(i) The attackers
(ii) The motive
(iii) The attack methodology and vulnerabilities exploited

(i) The attackers : computer security incidents are caused by attackers such as malicious users or hackers or organized criminal gangs

(ii) The motive of the attackers are fun and curiosity i.e, to prove their technical ability, stealing sensitive information and gaining financial benefits, gaining popularity or sending messages pertaining to political or ideological purposes, hactivism, or to cause disruption of services

(iii) The attack methodologies are such as exploiting vulnerability in operating system or application, creating and spreading malicious code such as worms or Bots, enticing users to disclose sensitive information such as passwords, credit card PINs etc through social engineering and phishing etc.

Cyber space has witnessed significant changes in the attacks and attack methodologies over a period of time. Various types of threats are existing targeting different systems, services and aiming organizations, service providers and end users. Significant trends to be noted and threat elements that can affect the information infrastructure at the national level are briefly described in the following sections.

2.1 Malicious code threats

The malicious code is evolved from simple virus that causes annoyance to more destructive worms such as SQL Slammer [1], Blaster [2], Mydoom [3], Conficker [4] etc. Latest worms are equipped with multiple infection vectors such as emails, network shares, removable drives etc, and perform various malicious functions such as spamming and Denial of Service. The malicious code is now crafted for stealing sensitive information from user's computer system and conducting financial frauds. Information stealing Trojans such as Nethell [5], Bzub [6] etc are rising.

2.2 Botnets

Botnet is a network of large number of compromised systems called as Bots. Botnets are created and owned by bot herders and cyber criminals use these botnets for various malicious activities such as

- Spam
- Phishing
- Malware propagation
- Distributed Denial of Service attacks

The Storm Botnet [7] that emerged in January 2007 propagated through context based Spam such as latest news events and spread across millions of systems during first half of year 2007. The Asprox Botnet [8, 9] evolved from a Trojan in the year 2005 to large scale Botnet during 2008 and launched large scale SQL injection attacks on to the websites and infected large number of websites during the year 2008. Figure 1 shows number of Bot infected systems tracked by CERT-In during 2008-09. As shown in the figure, large number Bots were reported in April 2009 due to propagation of Conficker worm which propagated by exploiting Microsoft Windows server service vulnerability and through removable drives [10].

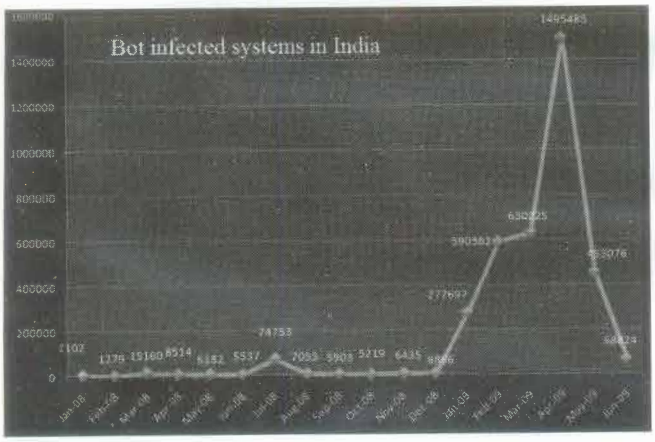


Fig 1. Bot infected systems in India

3. Financial frauds through Identity theft, phishing and crimeware

With advent of e-Commerce and online banking, incidents of phishing and identity theft are rising. The users are being enticed to disclose sensitive information such as passwords and PIN through Phishing sites and emails with social engineering. Stealing of data from users system through key loggers and information stealing Trojans called crimeware is also on the rise. These attacks are facilitating financial frauds and promoting online underground economy.

3.1 Attack Toolkits

Significant development in the attack methodology during last couple of years is usage of attack toolkits. The attack toolkit such as Mpack [11, 12] facilitate hosting of wide range of exploits for specific vulnerabilities and have ability to choose a particular exploit based on configuration of target system. In a typical scenario innocent user is redirected to malicious websites hosted by the toolkit. The HTTP Request header is analysed by the toolkit to determine the configuration of user's system. Based on this, suitable exploit for vulnerability in the target system is used to compromise users' system or deliver malware. Various series of attacks analysed by CERT-In reveal that primary goal of these attacks is to install malware such as Trojan or Bot on end user's system. Similarly Neosploit tool kit [13, 14] used exploits for vulnerabilities in popular applications and even used to steal FTP credentials which are then used by cyber criminals to compromise legitimate websites. Several such toolkits and exploit packs are available which facilitate even unskilled cyber criminal to launch an effective mass scale attack.

3.2 Organised cyber criminals

As described in the previous section, while the attack methodologies are becoming innovative and sophisticated, the profile of cyber criminals is also changing. More number of attacks on websites are now performed by automated toolkits under control of organized gangs rather than individual hackers or script kiddies. Cyber crimes are more organized now. Analysis of different attacks reported during last year reveals that these are launched through combined efforts of malware authors, spammers and bot herders. Cyber underground economy is growing. Similar to real world, the cyber arms (toolkits, botnets etc.) are available for sale [15].

4. Affects of cyber threats on National Information Infrastructure

After examining the current trends of cyber threats as mention above, it is to be seen how these threats affect the assets of information infrastructure at the national level.

Distributed Denial of Service attacks (DDoS) on websites of important government organizations, industry, financial institutions and media can cause disruption of essential services. It is to be recalled that a series of such DDoS attacks were launched on websites of Estonia in April-May 2007 [16, 17]. Similarly websites of USA and South Korea were flooded with requests (DDoS) in July 2009 with help of systems infected with variant of Mydoom worm [18, 19]. The websites targeted by these attacks belonged to Government, Financial Institutions and Service providers.

DDoS attacks may also deplete the bandwidth and disrupt availability of connectivity to critical services and businesses. Attack toolkits available today can compromise or infect websites on large scale. Similarly intrusion into sensitive databases and altering/stealing of important information may create confusion among the public. Critical information infrastructure of the nation may also be affected by unathorised access by cyber criminals.

5. Challenges in combating the cyber threats

The cyber space has no geographical boundaries. The uniqueness of cyber crimes and transnational issues pertaining to cyber laws in various countries demands greater understanding of issues and cooperation at international level. The sophistication of attacks coupled with affective social engineering techniques used by the cyber criminals target end users to steal sensitive information leading to financial frauds and other attacks. Creating awareness among users about latest threats within a reasonable time is a challenge.

Keeping in view the technological complexity involved in the attack methodologies, prevention, detection and mitigation of these cyber attacks demands knowledge and skills among the users and system administrators. Further, cyber attacks such as denial of service or identity theft can only be mitigated with combined efforts and cooperation between users, organizations, service providers and security agencies located in different countries.

6. Technological and Social measures required

Based on examination of different threats and challenges mentioned in the previous sections, the solutions and initiatives in the area of cyber security existing currently and developing need to be looked into. Various initiatives are taken by Government, Academia and Industry over a period of time on administrative and technological fronts.

Information security best practices and standards are being developed and followed worldwide to protect information and secure cyber space. Computer Emergency Response Teams (CERT) are operational in different countries that work together through forums such as Forum of Incident Response and Security Teams (FIRST) [20] to share information related to cyber threats and act together to respond to cyber security incidents affecting respective constituencies. Collaborative forums such as Anti Phishing Working Group (APWG) [21] are working to tackle with specific threats.

Cyber security measures require affective formulation of appropriate security policies, procedures and adherence to information security standards and implementation of best practices. Particularly cyber crime prevention is to be supported by appropriate cyber laws and regulation. Government of India has enacted the Information Technology Act 2000 and amendments to the same have been notified through Information Technology (Amendment) Act 2008 covering different forms of computer crimes.

Investigation of cyber crimes involves appropriate collection, analysis and maintenance of electronic evidence and demands skills in the area of computer/cyber forensics. Accordingly the Law Enforcement need to be equipped with appropriate tools and techniques to collect and analyze the electronic evidence and investigate the cyber crimes. Development of cyber forensic centres and capabilities is essential to facilitate affective cyber crime investigation.

Keeping in view the dynamically changing threat landscape and sophistication of attack methodologies such as obfuscation of malicious code, usage of encrypted communications for Botnet Command & Control, unauthorized usage of wireless networks through MAC spoofing etc., research and analysis of attack methodologies as well as development of appropriate tools and techniques for detection and prevention of these attacks is required. Government, Academia and Industry has to work together to conduct appropriate Research and Development in the areas of Information Security such as Intrusion Prevention for Wireless networks, Cryptanalysis, Botnet detection particularly for P2P & HTTP Botnets and mitigation of DDoS attacks.

7. Conclusion

Considering the challenges posed by cyber threats to the national information infrastructure, efforts in cooperation and collaboration between Government, Industry and Academia are required to proactively prevent these threats and ensure well being of information assets.

8. References

1. http://en.wikipedia.org/wiki/SQL_slammer_(computer_worm)
2. CERT-In Incident Note CIIN-2003-02 http://www.cert-in.org.in/incident/ciin-2003-02.htm
3. CERT-In Advisory CIAD-2004-02 http://www.cert-in.org.in/advisory/ciad-2004-02.htm
4. CERT-In Virus alert: Worm:Win32/Conficker http://www.cert-in.org.in/virus/win32_conficker.htm
5. CERT-In Virus alert: Nethell Trojan http://www.cert-in.org.in/virus/Nethell_Trojan.htm
6. CERT-In Virus alert: BZub Trojan http://www.cert-in.org.in/virus/BZub-Trojan.htm
7. CERT-In Virus alert: Storm Botnet http://www.cert-in.org.in/virus/Storm_Botnet.htm
8. CERT-In Virus alert: Asprox Botnet http://www.cert-in.org.in/virus/Asprox_Botnet.htm
9. http://www.secureworks.com/research/threats/danmecasprox/?threat=danmecasprox
10. http://www.confickerworkinggroup.org/wiki/
11. http://www.securityfocus.com/brief/529
12. http://www.symantec.com/connect/blogs/mpack-packed-full-badness
13. http://www.aladdin.com/AircBlog/?tag=/neosploit
14. http://explabs.blogspot.com/2008/01/neosploit-january-2008.html
15. http://finjan.com/Pressrelease.aspx?id=2280&PressLan=2139&lan=3
16. http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/
17. http://www.zdnet.com.au/insight/security/soa/How-Estonia-s-attacks-shook-the-world/0,139023764,339288625,00.htm
18. http://www.guardian.co.uk/technology/2009/jul/08/cyber-war-mydoom-virus-attack
19. http://en.wikipedia.org/wiki/July_2009_cyber_attacks
20. http://www.first.org/
21. http://www.antiphishing.org/

About Author

Shri Sarma is working as Scientist 'E' in the Indian Computer Emergency Response Team (CERT-In) since 2003. He is handling computer security incidents reported to CERT-In. Currently he is looking after activities of CERT-In relating to tracking of malicious code, Botnets, analysis of vulnerabilities and exploits, Vulnerability Assessment and Penetration Testing and issuance of advisories, security alerts and vulnerability notes. He has over seven years of experience in Information Security. He has overall experience of 17 years in the area computer communications and broadcasting.

He is a CISSP (from ISC2, USA) and a Certified Ethical Hacker from EC Council, USA. He received training in Information Security and Computer Forensics at CERT/CC, Carnegie Mellon University.

Contact

e-mail: sarma@cert-in.org.in; ss.sarma@nic.in
Ph. : 91-11-24368551

A Conceptual System for War Against Terror

Brig A P Sharangpani (Retd)

Abstract

Apropos to the theme "Technology and Terror – Role of ICT in War against Terror", the paper briefly covers the technology available worldwide; in ICT domain, exploited by the terrorist organizations to disrupt economy of the country and cause damage to life and property besides gaining psychological victory. The paper later covers challenge for ICT professionals in denying and frustrating terrorists in effecting their ghastly acts. A conceptual system that could be in place/considered for development to combat terrorism is proposed. It covers some recommendation on integration of IT infrastructure already in place and proposed systems coming up under National e-governance program (NeGP). War against terror cannot be fought in pockets. Issues required to be considered jointly by stakeholders in Government, public and private sector are briefly mentioned.

Introduction

Technology at the hands Terrorist Organizations and Anti National Elements

- **Cyberspace**

  ❖ **Information Repository:** Cyberspace is replete with range and depth of information, being misused by terrorists. Critical ones are Google-Earth™, Wikimapia™ and host of similar packages which provide vector maps, satellite maps and their hybrid in browser. Some provide three dimensional views, with facility of viewing objects at different angles and zoom. No doubt GIS technology is being misused for planning and executing the operations, unchecked.

  ❖ **Information On the Move**

  ➢ ***High Speed USB ROM (Data card) :*** GSM service providers enable wireless data communication with data cards.

  ➢ ***Wi-Fi :*** Data connectivity is available in the vicinity of hot spots. Hijacking/Intruding wireless connections is routine to avoid detection/spoofing.

  ➢ ***3G Enabled Data Services, Wi-Max :*** These services for high speed data communication are not far away.

  ❖ **Cyberspace Attack:** Hacking, denial of service, degrading QoS, Phishing and many more methods are in use by these organizations to attack Government/Private sector portals/e-services.

- **Telecommunication**

  ❖ Mobile (GSM/CDMA): It is well known that 26/11 attackers had procured around 35 SIM cards for communication. Two important weaknesses exploited were **firstly** anonymity and **secondly** difficult detection as fifteen GSM/CDMA operators in the country, servicing user base of around 320 million users do not converge at a common database.

  ❖ Satellite Phones and Smart Phones: In the 26/11 incident, terrorists communicated with their masters on Sat phones during sea journey.

- **Remotely Operated Explosive Devices:** Over many years, massive damage to life and property has been caused by radio remote explosions. It's a regular feature in North and East. Timed devices have been used in Metros (Mumbai, Delhi etc). Radio operation of devices is constantly under update. Terrorists have been using DTMF for remotely detonating the explosive devices. Even DTMF operations have varying combinations of 3-Digit Code / 4-digit code for pre-arming, arming and exploding the device. Mobile phones also have been used to remotely detonate explosives.

- **Remotely Controlled Toy Air Crafts:** A recent report of import of 3000 radio-controlled aircrafts imported from China, Taiwan and Korea is a case in point. Incidentally these are permitted to be operated in 27 MHz band (Spot frequencies already in National Frequency allocation Table). In general Terrorist organizations look out for all available technologies to execute their nefarious acts.

- **RFID:** Though there are no reports till date on use of these cards, RFID must be taken as a potential powerful tool assisting contraband consignment tracking/ personnel tracking. Long range (vicinity) Track and Trace applications are commercially available and can be exploited.

Challenge for ICT Professionals

As we see a total convergence between electronics, telecommunication and IT, the challenges enumerated below are applicable to all ICT professionals.

- **Cyberspace:** Websites, e-business, e-commerce portals for financial transactions, on line banking are always vulnerable to Cyberspace attack. Developing tools guarantying security to computer networks, web contents, business portals, systems on networks should be dynamic and capable of frustrating the ever eager hacker. Internet connectivity on move must be fully exploited.

- **Telecommunication:**

  ❖ Mobile (GSM/CDMA): The technology of measuring power levels, antenna patterns and vicinity of handset to towers needs to be exploited to locate suspected handsets. Similarly, conversation recording facility at the service providers' infrastructure premises need be explored. It is well known that mobile phones have been used in the form of electronic surveillance in U.S. by remotely activating mobile phone's microphone and using it to eavesdrop on nearby conversations. Privacy however, is the major issue in such activities, particularly recording the conversations and locating handsets.

  ❖ Sat Phones: Developing ability to locate hostile satellite phones, recording conversations on Sat phones even if the conversation is encrypted is a challenge ICT professionals need to take on.

- **Neutralizing Remotely Operated Explosive Devices:** This calls for grass root level designs since such neutralizers have to be effective as pre-detonator for the armed explosive devices. R & D for deactivators/jammers for such remotely operated devices should be a continuous process. The designs need to be catering following features:

  ❖ Cover entire frequency band in which Walkie-Talkie sets would operate, generally in 27 MHz, 138 to 172 MHz and 350-400 MHz.

  ❖ Generate optimum RF power to neutralize the remote at right time and sequence.

- **RC Toy Air Crafts and RFID:** Appropriate plans need be developed to neutralize their misuse.

- **Electronic Warfare**: Involves actions to use our own Electromagnetic Spectrum effectively and direct energies to deny the use of Electromagnetic Spectrum by terrorist organizations. This may feature the following:

  ❖ Communication Surveillance

  ❖ Jamming

  ❖ Snooping

  ❖ Sniffing

- **Hyper Spectral Imaging (HSI), SAR & ISAR:** Surveillance from space, either from the airborne systems or satellites has received new dimensions with HIS, SAR and ISAR. These technologies circumvent the limitation of optical surveillance due to cloud cover, darkness and camouflage. Detecting and processing the spectral image data in real time is possible. SAR uses echo from terrestrial Metallic objects/targets thereby nullifying the effect of camouflage or concealment. The combination of HSI and SAR as a pay load can provide excellent results as HSI would provide spectral images of illuminated objects during daytime while SAR would pick up objects during nights. In daylight hours the data collected by both would augment each other. We have already achieved capabilities of launching Israeli satellite with SAR capabilities (TechSAR in LEO launched in Jan 2008[1]) with object resolution capability ranging from 1 M to 10 Cm.

- **GIS:** Representation of Earth's natural and man-made features (called spatial data) has come a long way. GIS facilitates collection, storage, processing and analyzing of spatial data. Geospatial technologies have excellent potential to nail the activities of non-state actors terrorizing the country and the citizens. Virtual Reality GIS is high end application allowing creation, manipulation and exploration of geo-referenced virtual environments, using VRML (Virtual Reality Modeling Language). Virtual Reality GIS can be ported on web, for users to get reality feel and training. Web-based applications can include 3D simulation for planning, rehearsing, executing missions (experimenting with different scenarios).

- **Network Based Surveillance:** Mass surveillance has become a routine practice in UK, US and other countries. IP based surveillance must be considered in following domain. Technology must take care of non-repudiation.

- ❖ IP Phones: **Internet telephony** should be seriously looked into. Skype^{TM} and other freely available Voice & Video IP service are favorites amongst terrorists. Ability to tap conversations on these services over Indian Territory needs to be developed. In the absence of this, we can consider selectively jamming these virtual circuits. Needless to say, legal issues, privacy violation must be weighed against national interest.

- ❖ IP Cameras: Monitoring/surveillance of entry/escape routes at transport Hubs' (Airports, sea ports, Railway Stations, Bus Terminus) can be effected with IP devices connected to net. Real time data can be auto-analyzed for operational intelligence. The technology can be extended to important buildings, energy centers, hospitals and education centers. (Already such project has taken off with private partnership in Bangalore[2]).

- ❖ Capability of e-mail monitoring/snooping by security agencies need be considered.

- **GPS assisted Automotive Navigation System/ Portable (Personal) Navigation Assistant:** These systems use hand held/ vehicle attached devices to acquire position data from GPS satellites and locate the user on a road/ground in the map stored in device database. Using the road database, the unit can give directions to other locations along roads also in its database. Devices are capable of sensing distance from sensors attached and using distance data for providing a reliable location of the user. As these devices operate on mobile OS (J2ME, Windows Mobile, Android etc), ICT professionals may consider working in this domain to enhance the inherent strength of such devices.

An Integrated System to Combat Terrorism

Issues discussed in preceding paragraphs indicate the necessity of "Enterprise Class"[3] system (Combination of hardware and software providing high speed and high reliability) that should be capable of dealing with high volume of data in a fault tolerant, distributed environment. The system can adopt DIKW (Data-to-Information-to-Knowledge-to-Wisdom) Model[4] for inference and decision-making. This calls for conceptual system development termed as **Intelligent Knowledge Management System (IKMS).**

- **IKMS as an Enterprise Information system:** Conceptually IKMS will provide a technology platform that will enable security organizations, ministries and other relevant organizations to integrate and co-ordinate their processes. IKMS will provide sharing of information across all functional levels and management hierarchy. The problem of information fragmentation caused by multiple information systems in the organization can be eliminated. IKMS may conceptually have more than one data center and have applications functioning in cross organizational structure. A conceptual view of IKMS is provided below. System integration may consider following features on merits, keeping legal, privacy, human rights issues in mind. The list is suggestive and not exhaustive :

- ❖ GIS encompassing geo-data of the entire country, greater details of sensitive areas, Indian water limits and international waters. Areas from the neighboring environment nurturing terrorism also can be considered in database.

- ❖ Build Stream database platform for online/ offline analysis of streamed data from IP cameras at transport hubs. Integrate face/object recognition system with these.

- ❖ Image analysis, image synthesis, auto-conflation with GIS database need be developed in space imagery domain (images acquired from sat, aircrafts, air drones etc).

- ❖ Integration with entire range of database systems in the country for linking up & locating an individual and/or device. Suggestive list given below may not be exhaustive:

  - ➢ KYC database (banks, financial institutions, Mobile service providers)
  - ➢ City RTO
  - ➢ Crime and Criminal Information System (CCIS), fingerprints, DNA
  - ➢ Voter ID
  - ➢ Passport
  - ➢ Foreigners' entry/exit/Visa etc.
  - ➢ Unique ID (Proposed)

- ❖ Telepresence solutions be implemented for online decisions.

- **Network bandwidth capacity: Should cater for multimedia transmission and upward scalability, NGN protocols.**

- **Network enabled Capability (NEC):** It is a terminology adapted from UK MoD, looking forward to "right information, at right time and right place" achieved by optimum use of information system. To achieve NEC, all activities are focused for coherent integration of sensors, decision makers and other support capabilities to achieve he flexible and effective response. IKMS needs to be developed with this concept in view.

- **Storage Management:** The proposed system will be continuously collecting huge volume of data every day. Expected data size may be in the range of Terabyte/Petabytes. Managing the rapid growth in data will be challenging storage management issue. Data reduction and/or de-duplication will ensure manageable storage. Risk of data loss, data retention, backup and recovery, availability will have to be taken care.

- **High Availability:** Since the proposed system will be providing net centric information capabilities, system needs to be designed with high availability. It should provide fault tolerant operational continuity. The system should also cater for future load.

- **Data Management**

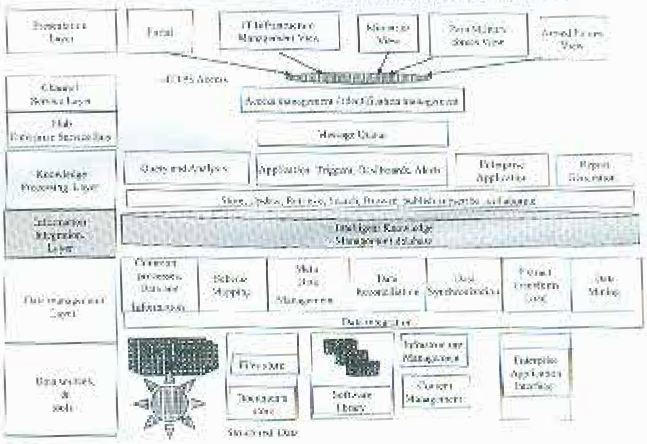
  - ❖ Taming Raw Data: It can be quickly discerned that the volume of data generated every day will be very large. This data needs to be cooked without loss of time for converting it into information for decision making, lest it would become garbage in and garbage out.

  - ❖ Data ware House and Data Mining: Data mining is discovering previously unknown, valid patterns and relationships within data sets/Very Large Data Base (VLDB) using sophisticated data analysis tools. In general the tools are statistical models, mathematical algorithms, and machine learning methods, such as neural networks or decision trees and are required to be selectively deployed.

Stake Holders

Multiple and complex threats and challenges to our security from the land, sea and air at international borders are tackled by Armed Forces and *Defence Ministry*. *Home Ministry* takes on internal security, through its Para-military forces. National Security Council (NSC) looks into strategic security. *Joint Intelligence Committee* (JIC) analyzes intelligence data from the IB, R&AW and from Armed Forces. Organizations and departments within these ministries have inherent resources to capture and consume data for decision making (D-I-K-W model). Ministry of C & IT has resources to build up Network & IT infrastructure. Independent Department of Space has ISRO and NRSA under its roof.

CONCEPTUAL INTELLIGENT KNOWLEDGE MANAGEMENT SYSTEM



It's time the country demanded long-term strategic vision for war against terrorism from aforesaid stakeholders. War against terrorism is to be fought jointly and hence each and every organization involved should come to a common platform. Private sector's contributory efforts could be coordinated through CII & FICCI.

Conclusion

Unrestricted access to technology facilitates terrorists to create panic, cause loss of life and property at their will. A sustainable model, with the platform adaptable to ever changing underlying ICT environment has to be built to fight this battle. Rapid progress in ICT domain, miniaturization and unpredictable approach of terrorists presents a challenge for ICT professionals. They have to keep the stakeholders' efforts at an upper edge. As the stakeholders comprise of several ministries, independent departments, policy makers, security forces, service providers with different responsibilities, it is important for them to put their heads together to focus in this domain and arrive at a common consensus.

References:

1. http://en.wikipedia.org/wiki/TecSAR

2. Business Line News Article Dated 13 Feb 09.

3. http://www.pcmag.com/encyclopedia_term

4. "Understanding Data, Information, Knowledge and Their Inter-Relationships", *Journal of Knowledge http://www.tlainc.com/articl134.htm*

5. "A Roadmap for Enterprise System Implementation" By **Diane M. Strong**, Worcester Polytechnic Institute & **Olga Volkoff**, Worcester Polytechnic Institute **doi.ieeecomputersociety.org/ 10.1109/MC.2004.3**

About Author

Brig (Retd) AP Sharangpani is currently providing consultancy and training services in IT services Management and IT Infrastructure. He has been handling ICT Infrastructure of Army over 34 years. Post retirement, he was in Tokyo as Principal Consultant over an year, for IT infrastructure in BFSI domain.

Contact

e-mail:sharang1951@gmail.com
Mobile : 09422300450

Cyber Terrorism

Brig Lakshman Singh, VSM (Retd)

Abstract

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

Business, government and industry have all become addicted to information. Their reliance on information creates opportunities for terrorism. Imagine a day without the Internet. What would the impact be? Computer networks do more than systems --they run the business of daily life the nature of cyber security threats pose not only to critical infrastructures but ultimately to the economy and the citizens.

If one looks at the projected e-Commerce number, with a projected e-Commerce purchase volume expected to reach over $355 Billion in North America alone over the next three years, the Internet being down for just one day could disrupt a mind boggling worth of transactions.

More than just e-Commerce transactions flow over the Internet .e Mail, voice communications, some banking machines, credit card authorizations for physical stores and the list goes on and on. Information is the life blood of commerce, regulatory oversight and even social status. The importance of the information and the ability to access it, transfer it and act upon it has increased to the point that it is unfathomable for all but the smallest of businesses to operate without computers or networks. As the value of the computing infrastructure increases so to does the value of disruption. The financial implications are one thing, but the psychological impact of the Internet disruption could be even more damaging.

How likely is this to happen? *It is not, if it will happen, but when.* The likelihood of a cyber terrorism attack disrupting the Internet increases every day. The increased reliance on the Internet by business, government and society has made it a prime target for terrorist intent on disrupting our economy and way of life.

Security professionals have expressed their increasing concern over not only the increase in frequency of attacks against the Internet, but also the increase in the level of sophistication of these attacks. While the complexity of the attacks is increasing, the skill level of the intruder that launched the attack is decreasing. This is a very troubling trend. As the terrorists learn from every attack what works and what doesn't, where the vulnerabilities are, how we respond, and the methods we use to detect these attacks, they gain the knowledge that will increase their odds for success.

What is the current state of attack?

Despite significant investment in technology and infrastructure, cyber terrorism represents one of the greatest challenges in combating terrorism. Every day the Internet and countless other computer systems are under attack.

Most studies to date have shown that critical information infrastructures are potentially vulnerable to a cyber terrorist attack. The increasing complexity of information systems creates new vulnerabilities and challenges for IT management. Even if the technology is armour plated, insiders acting alone or in concert with other terrorists may be able to exploit their access capabilities to wreak considerable harm.

What would the impact be of Terrorism attack?

The intention of a cyber terrorism attack could range from economic disruption through the interruption of financial networks and systems or used in support of a physical attack to cause further confusion and possible delays in proper response. Although cyber attacks have caused billions of dollars in damage and affected the lives of millions, we have yet witness the implications of a truly catastrophic cyber terrorism attack. What would some of the implications be?

Direct Cost Implications

- Loss of sales during the disruption
- Staff time, network delays, intermittent access for business users
- Increased insurance costs due to litigation
- Loss of intellectual property - research, pricing, etc.
- Costs of forensics for recovery and litigation

- Loss of critical communications in time of emergency

Indirect Cost Implications

- Loss of confidence and credibility in our financial systems
- Tarnished relationships& public image globally
- Strained business partner relationships - domestic and internationally
- Loss of future customer revenues for an individual or group of companies
- Loss of trust in the government and computer industry

When will it happen?

As discussed earlier as the value of our information infrastructure further increases and the capabilities of the cyber terrorists' increase, the likelihood of a significant incident increases.

Thwarting Cyber Terrorism "Critical" Infrastructure and "Key Resources"

The growing threat of international terrorism in the mid-1990s renewed federal Government interest in infrastructure issues. On July 15, 1996, President Clinton signed Executive establishing the President's Commission on Critical Infrastructure Protection (PCCIP). The Directive's goal was to establish a national capability within five years to protect "Critical" infrastructure from intentional disruption. To help achieve its goal, it directed certain federal agencies to lead the government's security efforts and identify private sector liaisons in specific critical infrastructure sectors.

Following the terror attacks of September 11, 2001, President Bush signed new Executive Orders relating to critical infrastructure protection.

The Executive Order signed October 8, 2001, established the Office of Homeland Security and the Homeland Security Council. Among the duties assigned the Office was to coordinate efforts to protect: energy production, transmission, and distribution services and critical facilities and other utilities, telecommunications, facilities that produce, use, store, or dispose of nuclear material, public and privately owned information systems, special events of national significance, transportation, including railways, highways, shipping ports and waterways, airports and civilian aircraft, livestock, agriculture, and systems for the provision of water and food for human use and consumption. In response to the terror attacks of September 11, 2001, Congress passed the USA PATRIOT Act of 2001 The PATRIOT Act was intended to "deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."

- Congress Research Service Report for Congress October 1 2004

The Obama administration is finalizing plans for a new Pentagon command to coordinate the security of military computer networks and to develop new offensive cyber-weapons, sources said last night. Planning for the reorganization of Defense Department and intelligence agencies is underway, and a decision is imminent, according to a person familiar with the White House plans. The new command would affect U.S. Strategic Command, whose mission includes ensuring U.S. "freedom of action" in space and cyberspace, and the National Security Agency, which shares Pentagon cyber security responsibilities with the Defense Information Systems Agency. The Pentagon plans do not involve the Department of Homeland Security, which has responsibility for securing the government's non-military computer domain.

-Washington Post April 22 2009

Indian Scene

The Indian Express dated February 6th reported of the setting up of the National Security Board (NIB) consisting of the three defence chiefs, the Cabinet secretary, the It secretary and the RAW chief and draw on the expertise of all intelligence agencies.. The NIB will be the nodal agency for the interception of SMS, e-mail:, this has come on the heels of the setting up of the Cyber Emergency Response Team (CERT) a nodal agency for tracking cyber crime across the country and digging their origins.

What needs to be done by Corporates

Corporates must be forced to wage an all-out war against cyber terrorism. Securing the information infrastructures will require a substantial effort on everyone's part. Close collaboration between government and the private sector is critical. Even more critical is the close collaboration within the computer, networking and software industries. These industries must work closely and continue efforts to enhance technology security capabilities. Security is designed in, not added on. Until the weakest links in the network are protected we all are vulnerable and may be impacted. The government sector must institute tougher penalties for cyber crimes and increased funding for law enforcement efforts to fight it., though easier said than done. This must be accomplished with a high degree of collaboration globally. Getting countries to agree on anything these days seems to be an almost unachievable task. Is cyber terrorism the shape of future conflict? Is a digital underground developing right now? Will our scientists, software engineers, and technical resources be able to stay one step ahead of these faceless terrorists? Only time will tell!

Computer and information security, data protection, and privacy are all growing problems. No single technology or product will eliminate threats and risk. One wonders if we have even begun to think of the social and economic implications of a considerable cyber terrorism attack against our infrastructure. Securing our computers, information, and communications networks secure our economy and our country. A global strategy and policy for combating this type of terrorism is need now.

CYBER TERRORISM PREVENTION CHECKLIST

Find out whether your IT, security, and human resource personnel have put in place the necessary security precautions to protect you from becoming an unwitting collaborator.

Intelligence Gathering

This area includes three possible security lapses that allow for penetration of systems with the goal of stealing information or sensitive data. The key here is to get your organization, company, or institution on a wartime footing and control access to your building, personnel, and information systems.

Identity Impersonation and/or Identity Theft

Many organizations—businesses especially—fall down on this simple yet effective threat Prevention.

Spyware

Spyware is software that sits on your system and tries to be invisible while collecting as much information as possible to be sent offsite.

Internal Threats

This area is often overlooked by organizations, but employees can be a great source of information-gathering for unauthorized use.

Systems Damage

This area includes four possible security lapses that allow for the disruption or damage of data and your information infrastructure

Breakdowns in the Human Firewall

People are the weakest link in a security plan. Proper training can prevent a majority of security lapses.

System/Browser Vulnerabilities

Bugs or other code flaws can allow an unauthorized user to execute arbitrary code.

Wireless Insecurity

Wireless networks are bringing installed by organizations at a rapid rate, opening their networks to "drive-by hacking."

Denial-of-Service (DoS) Attacks

These attacks are becoming more and more sophisticated, and in some cases initiated as a side effect of some other attack.

System Hijacking

In this area, three possible security lapses allow the use of established communications vehicles for clandestine operatives to secretly communicate with others.

Steganography

Steganography is the art and science of hiding the fact that communication is happening

It involves hiding messages inside text, images, sounds, or other binary files for clandestine communications.

Tunneling

Tunneling allows communication in an environment where communication may not be possible due to firewalls or proxies that limit traffic. For example, an application called HTTP-Tunnel allows people behind a firewall (which allows only web surfing) to use *any* Internet application. HTTP-Tunnel runs as a SOCKS server or via port mapping and can tunnel both TCP and UDP.

Worms, Trojan Horses, and Viruses

These attacks are becoming more prevalent and much more sophisticated. Next generation worms, Trojan horses, and viruses will be more intelligent and attack through multiple methods of distribution.

Disinformation

This area includes two possible security lapses that allow for the dissemination of propaganda such as the following:

- Spreading false rumors electronically that are picked up by the media as true
- Cracking into news servers to plant false or misleading stories
- Entering false or misleading information in databases, thus undermining the effectiveness of organizations relying on that information

DNS Poisoning and Domain Hijacking

DNS poisoning is convincing a name server that a domain has a different IP address. *Domain hijacking* involves stealing a domain at the registrar level.

Changing Web Site Contents

Web site defacement is widespread and has evolved to being used as a method of distributing propaganda, rumors, and misinformation (as opposed to just plain vandalism).

-Frank Fiore and Jean Francois

The problem

The resource to launch a cyber attack are common place:-a computer and an internet connection is all that is needed to wreck havoc, added to this is public and private sectors are relatively ignorant to there dependence on computers and the venerability of these computers.

THE NEXT GENERATIO OF TRANSNATIONAL CYBER TERRORISTS UNDERSTANDS THAT A HAND ON MOUSE CAN BE MORE LETHAL THAN A FINGER ON TRIGGER

About Author

Brig Lakshman Singh VSM (Retd), MSc, PTSC, LDMC, FIET, FNTF, MSEMCE (I), Dip AAFT has more than 30 years experience in the field of Electronics and Telecommunication, setting up and maintenance of Defence Communication & Electronic Warfare system, Defence R&D and Electromagnetic Emission & Compatibility. He was Member Secretary Joint Electromagnetic Interference & Compatibility Board; Faculty Commander of Comm & Elec Engg of MCTE, Mhow; Advisor to Electronic Corporation of India Ltd (ECIL) and Director in R&AW. He has authored two books and specializes in Soft Skills, Cyber Security and Computer related Injuries (CRI).

Actively associated with IETE for more than two decades, Founder Member and Vice Chairman of IETE Noida Centre, set up Noida Centre IETE Examination Centre, Computer Lab, Guidance Classes for IETE Grad/Dip students and computer literacy program for seniors & others. He was the Council Member (2003-06), represented in various Committees of the Council and Chairman, Board of Elan (e-learning & Local Area Network). He played a keyrole in developing Portal (iete-elan.ac.in) to facilitate IETE students to get access to course material and lectures on the web for IETE Grad and Dip courses.

Contact

e-mail : lakshman31@gmail.com
Mobile : 09871044560

Role of Counter Remotely Controlled Improvised Explosive Device (RCIED) Equipment in War against Terror

Brig Yashwant Singh

Abstract

Improvised Explosive Device (IEDs) is a locally fabricated unconventional mine with explosive of any type that can weigh few grams to hundreds of kgs, packed in any shape/ size. Detonator placed in the explosive pack initiates the blast. IEDs are also used to distract, disrupt, or delay an opposite force.

IEDs may be used in terrorist actions or in unconventional warfare by guerrillas or commando forces in a theater of operation. IEDs have been used extensively by cadres of the rebel Tamil Tiger (LTTE) organization against military and civilian targets in Sri Lanka and by various militant outfits in India.

IEDs are extremely diverse in design and triggend by various methods. In same cases multiple IEDs are used.

Latest, IEDs are no longer made by inexperienced designers or with substandard materials. They have developed into sophisticated devices that are constructed with components scavanged from conventional munitions and standard electronic components, such as mobile phones, pagers, garage door openers etc.

A Vehicle Borne IED (VBIED) is a military term for a car bomb or truck bomb. These are typically employed by suicide bombers, and can carry a relatively large payload. They can also be detonated from a remote location. VBIEDs can create additional shrapnel through the destruction of the vehicle itself, as well as using vehicle fuel as an incendiary weapon.

Historical Back ground

(a) **World War II :** Used by Belarusian Guerillas aginst Nazis to derail thousand of German trains.

(b) **Northern Ireland :** Used by IRA against British Army, from simple petrol bomb to remote controlled IEDs.

(c) **Vietnam :** Used by Vietcong against US Troops and land/river borne vehicles. Approx 33% of US casualty were due to IEDs.

(d) **Afghanistan :** Used by Afghan Mujahideen against Russian troops and vehicles and also used by Taliban against US Troops, ISAF, Afghan civil and military vehicles.

(e) **Labanon :** Used by Hezobullah against Israel forces and vehicles.

(f) **Chechnya :** Used by Chechan rebels against Russian troops and vehicles.

(g) **India :** Being extremely used by terroist/ extremist in Jammu and Kashmir, North East, Jharkhand, Orissa, Chattisgarh, Andhra Pradesh etc.

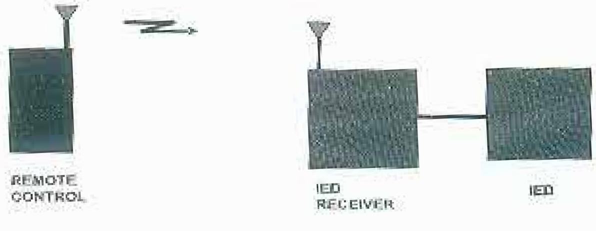
AIM

The aim of this paper is to bring out the trends in IEDs and role of counter RCIED equipments in defeating these IEDs, in war against terror.

Remotely Controlled Improvised Explosive Device (RCIED)

Technological Aspects

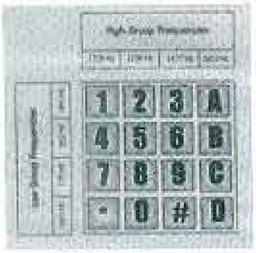
A typical Remotely Controlled IED will consist of a handheld commercially available transmitter, a matching receiver usually buried/concealed and an explosive pack which is electrically wired to the receiver. The receiver is a hardwired electronic device operating in the frequency range of handheld transmission.



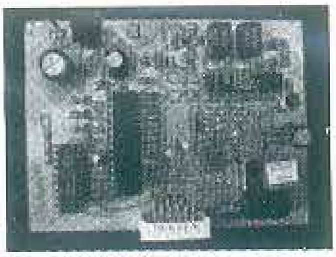
Remotely controlled IED is characterized by three unknown factors viz frequency of operation, 2 or 3 digit DTMF codes and exact loc of planting of IED. Any receiver can be tuned within a band width of 10 kHz, hence there are 4,000 frequencies that are possible in the band width of 135 to 175 MHz. Considering 2 digit codes, a combination of 72 possible codes may be used by an ANE. Similarly there are 504 such codes possible in a 3 digit RCIED.

Citizen Band (VHF) : In the VHF band the citizen band of frequencies span from 135MHz to 175 MHz. The frequencies below 135 MHz are being constantly monitored by Air Traffic Control (ATC) and above 175 MHz are in range of TV Audio frequencies, hence these frequencies are not likely to be used.

DTMF Codes : Dual Tone Multiple Frequency (DTMF) is a unique audio frequency generated by time domain mixing of two frequencies which is the vector addition of two frequencies. Commercial DTMF coders and decoders Integrated Circuits (IC) are readily available in the market.

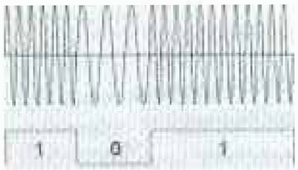


DTMF Generator



DTMF Coder/Decoder

Modulation : The DTMF codes are frequency modulated on the RF frequency ie any of the 4000 frequencies between 135 to 175 MHz. This modulation is done by the transmitter. The receiver demodulates these codes and operates gate circuits to activate the IEDs.



Modulation

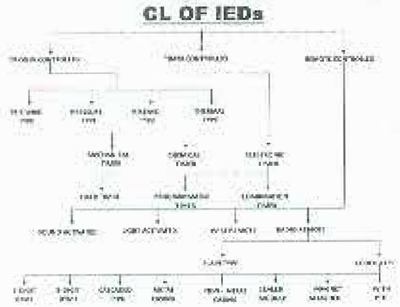
Receiver : The receiver consists of the following circuits:-

(a) Antenna Tuning Network.

(b) FM IF Amplifier.

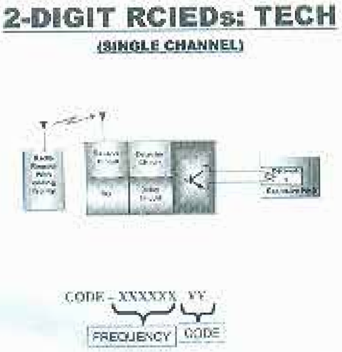
(c) Final Gate Circuit.

Classification of IEDs

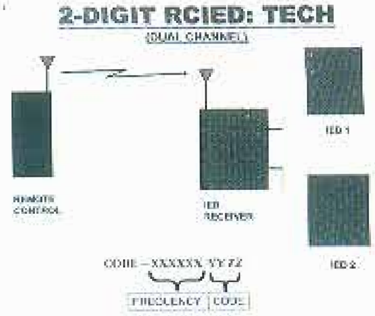


IED Technologies

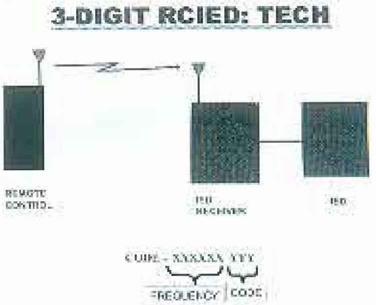
(a) 2 Digit RCIED (SINGLE CHANNEL)



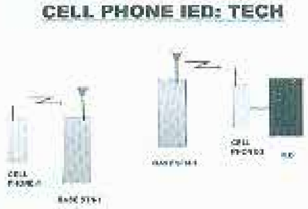
(b) 2 Digit RCIED (DOUBLE CHANNEL)



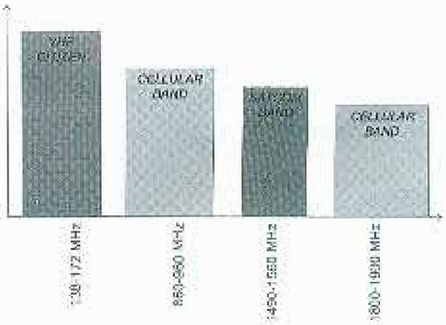
(c) 3 Digit RCIED



(d) Cell Phone IED



Frequency Bands



Characteristic of RCIED

(a) **Explosive Charge :** High explosives like TNT, RDX etc are most frequently used in sophisticated IEDs. However, locally manufactured explosives are more commonly used by Anti National Elements (ANEs) in J&K. Some of the more popular local explosives are :-

(i) Ammonium Nitrate Mixture.

(ii) Potassium Chlorate Mixture.

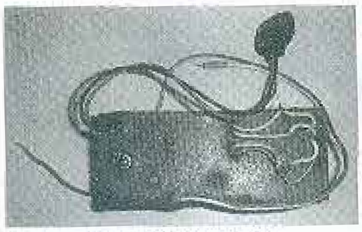
(iii) Sodium Chlorate Mixture.

(iv) Urea mixed with gun powder and diesel

(v) Prepared Charges.

(b) **Control Mechanisms :** While a variety of innovative control mechanisms have been evidenced, the more commonly used control mechanisms fall under one of the following two categories :-

(i) **Ambient Condition Mechanisms :** These mechanisms use any of the ambient conditions, such as sunlight, day temperature, etc for initiating the IED. A commonly used Ambient Condition Control mechanisms is the Light Dependant Device (LDD) which consists of a photosensitive Light Dependent Resistor (LDR).



Temperature Device

LDR Mechanism

(ii) **Command Actuated Mechanisms :** These mechanisms are more sophisticated and actuated by a pre-decided command given at the most opportune moment by the ANE. Since actuation can be accurately controlled by the ANE, such mechanisms are normally used for precise and critical disruptive activities. There are two basic types of Command Actuated mechanisms :-

(aa) Wire Controlled Remote Mechanism.

(ab) Radio Controlled Remote Mechanism.

Modus Operandi of Anti National Elements

(a) Selection of site.

(b) Selection of explosive and explosive containers.

(c) Use of Tandems IEDs.

(d) Use of Anti Lifting Devices (ALDs)

(e) Dummy IEDs.

(f) Use of Aiming Mark.

(g) Use of Rehearsed IED Attack drills.

Countering The Remotely Controlled Improvised Explosive Device (RCIED)

A counter RCIED equipment must have the following essential features for it to be effective:-

(a) Must have sufficient radius of influence. This feature will ensure that knowledge of exact location of the IED is no longer important.

(b) The equipment must be capable of generating all frequencies in the citizen band.

(c) For jamming of RC IED, sufficiently high radiated power is desired so as to create a 'barrage' effect.

(d) For pre-detonation of the RC IED, the counter-IED equipment must generate all possible DTMF codes and super-impose these codes on all possible transmitted frequencies.

(e) The above actions must be accomplished in the minimum possible time so as to make the counter RCIED tactically viable.

Typically, RCIED counter measures entail one or more of the following methods:-

(a) **Jamming :** Generation of all frequencies within the citizen band at sufficient power levels so as to cause a 'barrage' jamming effect on the RC IED receiver rendering it insensitive to the coded frequency transmitted by the ANE. The types of Jammers are :-

(i) Barrage Jammer

(ii) Selective Jammer

(iii) Responsive Jammer

(iv) IF Jammer

(b) **Pre-Detonating :** Transmitting the exact preset frequency along with the correct DTMF code to the RC IED receiver so as to detonate the IED at the time and under the conditions of our choosing, thereby depriving the ANE of the use of the IED. The major features of Pre-Detonating are :-

(i) Most effective countermeasure equipment.

(ii) Transmits Radio-Remote Simulated Signal Frequencies and Codes.

(iii) Blasts the RCIED at a convenient time, during Area Sanitization.

(iv) Generates all frequencies and DTMF codes required.

(v) Covers the frequency band in reasonable time.

(c) **Neutralising :** Continuous transmission of a set of DTMF codes in sequential manner to reset the transmitter thereby rendering the detonation impossible.

(d) **Responsive Jammer / Responsive Pre-initiator :** In this system a broad band receiver or a set of receivers are tuned to receive any transmission of DTMF in Citizen band. All receiver out puts are analysed for DTMF code. In case code is present it is assumed that a receiver is being operated by the ANE. By this approach the frequency and one of the code is known. The system can then send 504 codes of three digits to pre-initiate the IED.

Latest Trends in Counter RCIED Technology.

(a) **Cell Phone Jammers :** Cellular jammer is a transmitting device meant to interfere/jam the operation of cell phone in the near vicinity. Cell Jammer can be used to block Hand Set/Cell towers. It is an active jamming device, which can counter the threat of Cellular Triggered Bombs. The jammer interferes the linkage between cellular handset and cellular base station by very low output power radio signals. The jammer may cover areas as large as 2 square miles or it can be used in an area as small as 5 sq ft. These can neutralise/jam all types of GSM and CDMA cellular IEDs. The jammers currently available off the shelf are :-

(i) **SH 066 BM :** Advanced Cell Jammer covering 30 m radius. The cell user does not come to know, he only gets 'no network coverage' in his set. Suitable for big conference halls, library, hospital OTs, Operation rooms etc.

(ii) **Celljam 1000/5000 :** The Cell jam 5000 is a sophisticated and flexible rack mount jamming system. The jammer transmits RF signals at various bandwidths to jam wireless communications. The complete system consists of a cased exciter, power amplifier, as well as an antenna for jamming in various cellular bands.

(iii) **High Power Jammer :** High power cell Jammer of static range of 1 Km have been developed to secure installations from cell based IED threats. The code name used for products is "C-guard "developed by Netline technologies Ltd , Tel Aviv Israel. The cell users get "No service " or "Signal not available" or "No Network coverage" in their cells.

Satellite Phone Jammer : It jams/neutralises the signals of Transmitter Satellite phone used to remotely activate explosive devices and bombs connected to Receiver Satellite Phone. These use advanced DSP technology.

Counter IED Strategy : USA

(a) **Threat Analysis**

(i) In Iraq alone, there are 160 groups of IED users. These groups are hierarchical, connected to other countries and the street gangs.

(ii) High threat level.

(iii) IED designs change rapidly.

(iv) Technological solutions are neither sufficient nor effective.

(v) RF devices used to trigger the IEDs are commercially available from retail/ industrial electronics.

(vi) Greater diversity of IED triggers, with more reliance on diverse RF triggers as well as land wire and pressure devices. Trigger capability has improved from simple detonation to an arming and detonation system.

(vii) Changing delivery methods – Roadside and vehicle underbelly IEDs have been supplemented by vehicle born IEDs and suicide bombs.

(b) **Combat Strategy**

(i) A dedicated and specialist organization 'Joint IED Defeat Organisation (JIEDDO)' has been created whose long term task is rendering the strategic influence of IEDs as NULL, which would automatically reduce their tactical effect.

(ii) Counter IED efforts largely focus on mitigating the effects of devices, preventing their use or stopping the groups that use them.

(iii) Greater reliance is on disrupting terrorist networks and training allied troops in finding IEDs using RF counter measures, collecting information about terrorist groups and their Networks.

(iv) Increased deployment of protection afforded military vehicles as well as better discipline in use of personal protective equipment.

(v) Use of Human Intelligence (HUMINT) as a significant tool at all levels of Counter IED activity. Integration of intelligence has resulted in major success, due to degradation of Networks.

(vi) Industrial Control to prevent proliferation of RF triggers.

(vii) Constant feedback from Afghanistan and Iraq for reorienting the training as well as material counter measures.

(viii) Allotment of fairly large budget for training, developing counter measures and attacking Networks.

(ix) Building robust infrastructure, redevelopment of peoples' commercial livelihood and enforcing low of land terrorist affected areas.

(x) Design and development of ideal jamming systems that would allow troops to communicate while jamming terrorists' threat devices.

(xi) Working in close partnership with industry to develop solutions to IED Challenges.

Conclusion

Anti National Elements (ANEs) are increasingly resorting to the use of RCIEDs and continuously upgrading RCIEDs to stay ahead of developed counter RCIED equipments. The extensive usage of RCIEDs by terrorists/extremists in most parts of India warrants extensive deployment and usage of counter RCIED equipment to counter this threat. It should be the endeavour of the Engineers to continuously upgrade/design and develop new counter RCIED equipments to defeat the emerging IEDs. Communications are playing a vital role in helping defeat IEDs. Indian Security forces should rely on communications amongst themselves and leading IED experts to jointly defeat these weapons and their terrorist users.

Contact

e-mail – yash35167h@yahoo.com
Mobile : 09410226271

Programme for 52nd ATC-2009

Saturday, 26 Sept 2009

Technical Session – I – ICT in Crisis Management

	Name	Topics
irman:	Lt Gen A K S Chandele, AVSM DGEME & Sr Col Comdt Dte	
aker(s)	1. Col Alok Sardhana	Role of ICT in War against Terror : An integrated approach to security of an Installation
	2. Rear Admiral Karve	Role of ICT in Crisis Management : Maritime Aspects
	3. Brig X P Adriyanwala	ICT in Crisis Management and Technology bridging the gap
	4. Lt Col Malay Shankar Pal	Role of ICT in War against Terror Surveillance and Sensors
	5. Mrs S Mohanalakshmi	Identifying the Terrorist & Handicap their movement Entering through Sea : An Intelligent Approach
	6. D B Alaspure & D G Badshe	Technology: For National Security & Better Development of Society

Technical Session – II – Cyber Terrorism

	Name	Topics
irman:	Dr Gulshan Rai	
aker(s)	1. S S Sarma	Cyber Terrorism : Current Threats and Challenges
	2. Brig A P Sharangapani (Retd)	A Conceptual System for War against Terror
	3. Brig Lakshman Singh VSM (Retd)	Cyber Terrorism
	4. Shri Kiran Bhandari	Cybercrime : A Growing Threat
	5. Shri Vijay Mukhe	Cyber Terrorism is our response adequate after 26/11
	6. Ms Rachna P Narkhede	Cyber Terrorism

Technical Session – III – Broadcasting in Emergency

	Name	Topics
irman:	Shri S R Agarwal	
aker(s)	1. Shri S C Khasgiwala	
	2. Shri S N Gupta	
	3. Shri Suresh Nayak	Broadcasting in Natural Calamity in Emergency situation
	4. Shri R K Mittal	NGN and Security

Kavi Sammelen

ef Comments by Technical Session Chairpersons

Lt Gen A K Chandele, AVSM

Dr Gulshan Rai

Shri S R Agarwal

Shri J Gopal

Dr Sathish Kumar

Sunday, 27 Sept 2009

31st Ram Lal Wadhwa Memorial Lecture
on *'Morphological Algorithms for Image Processing'*
by Shri Nnarinder Kumar Malik

Best Papers Awards Ceremony

Technical Session – IV – NGN for Public Security

	Name	Topics
Chairman:	Shri J Gopal	
Speaker(s)	1. Shri Himanshu Shah	Vessel Monitoring System using INSAT MSS Terminal
	2. Shri Deepak Mukherjee	
	3. Shri S N Gupta	NGN Ecosystems-Regulatory and Security Issues
	4. Shri M Muthusamy Shri S Sivanathan	Wireless Network Security

Technical Session –V– Surveillance, Network Security and Sensors

	Name	Topics
Chairman:	Dr Sathish Kumar	
Speaker(s)	1. Dr Pawan Kapur	ICT in Combating Terrorism- Role of Sensors and Devices
	2. Dr V Gunasekhar Reddy	Modern Communication Networks-TETRA to Counter Terrorist Activities in India
	3. Prof S R Jog, Mukund Bhople, Gautam Hardikar, Pramod Chavan & Vishwesh Saraf	Wireless Bomb Detection System
	4. Shri Neeraj Sinha	Nuclear Base terrorism
	5. Shri Ganesh Manza Pravin Yannawar Madhav Karbhari S C Mehrotra	Criminal Information Analysis using Facial Expression with ICT
	6. Gp Capt H Kaushal (Retd)	Role of ICT in War against Terror

Valedictory Session / Panel Discussion

Chief Guest	:	Shri Shekhar Dutt
Guest of Honour	:	Shri D Sivanandan
Presided over by	:	Lt Gen A K Agarwal, PVSM (Retd) President, IETE

Overview of Technical Sessions

Shri P N Chopra,DIG,BSF(Retd)
Chairman,Technical Programmes Committee

Interactive Session

Address
Shri D Sivanandan
Police Commissioner,Mumbai

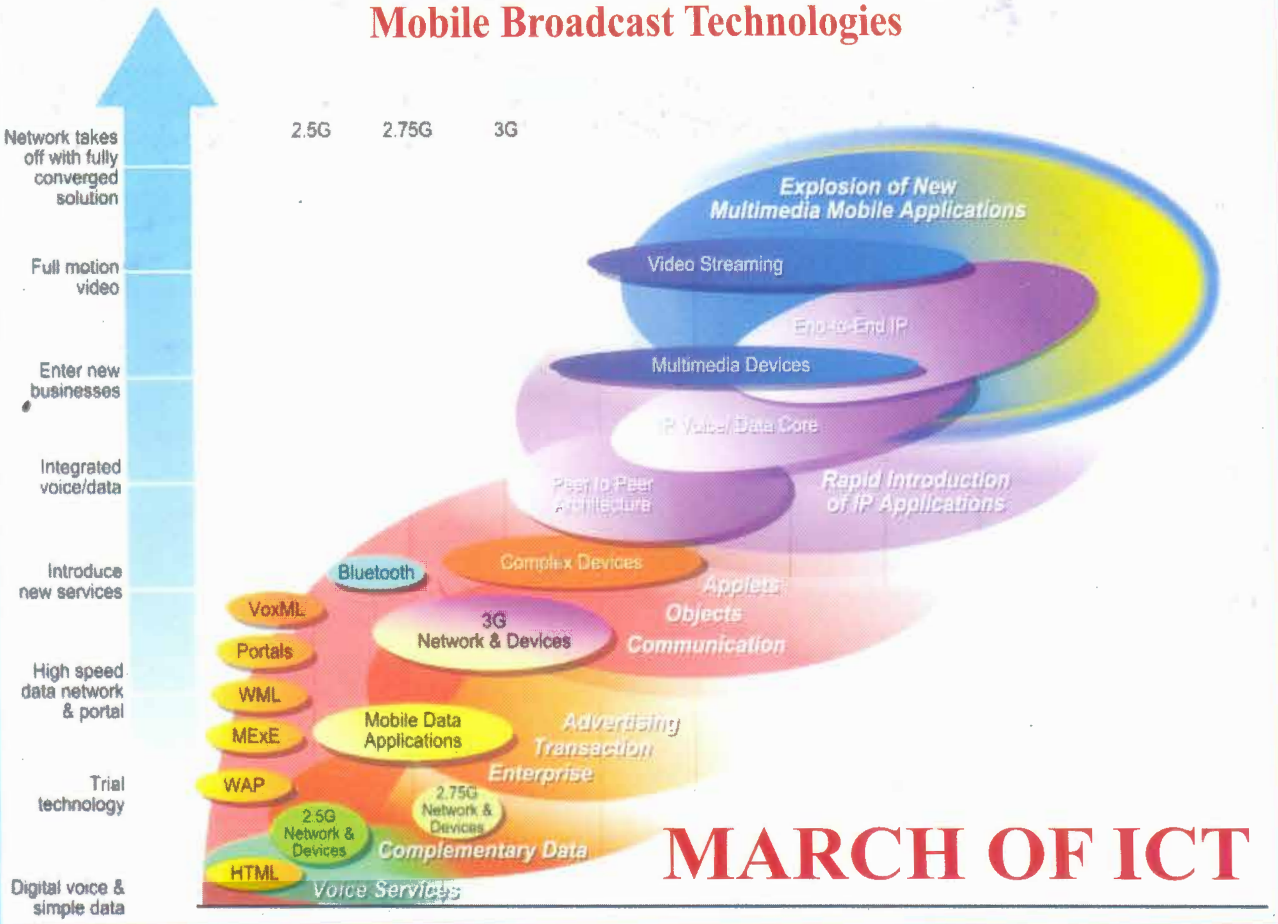
Address
Shri Shekhar Dutt
Dy NSA,NSCS, New Delhi

Presentation of Mementoes

Vote of Thanks

The Institution of Electronics and Telecommunication Engineers (IETE)

Two Key Technology Streams are Evolving Towards Mobile Multimedia
Mobile Cellular Broadband Technologies
Mobile Broadcast Technologies



MARCH OF ICT

Printed and Published by Brig (Retd) V K Panday, for the Institution of Electronics and
Telecommunication Engineers, 2, Institutional Area Lodi Road, New Delhi 110 003 (India)
printed at **Grover Printing Press**, 82, Khanna Market, Lodi Colony, New Delhi 110 003.
Ph. : 9810194345, 9811015523