

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

I
J
R
C
M



A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

Open J-Gate, India [link of the same is duly available at Inlibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2718 Cities in 161 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

<http://ijrcm.org.in/>

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	IMPACT OF THE URBAN INFORMAL SECTOR IN THE URBAN RESIDENTIAL PROPERTY MARKET <i>MOHAMMED YAHAYA UBALÉ, DAVID MARTIN & DR. SEOW TA WEE</i>	1
2.	COMPARISON OF PCA AND LDA BASED FACE RECOGNITION TECHNIQUE IN NOISY ENVIRONMENT <i>MEETA DUBEY & PRASHANT JAIN</i>	9
3.	A STUDY ON WORKER'S EMOTIONAL INTELLIGENCE IN SIPCOT INDUSTRIAL ESTATE, RANIPET <i>REV. FR. ANGELO JOSEPH, SDB, R. VEERAPPAN, A. STEPHENRAJ, L. MARY EZHILARASI & A. ANTONY MUTHU</i>	14
4.	TERRORISM: A BIG THREAT FOR TELECOM AND INTERNET BASED COMMUNICATION <i>VISHAL KAUSHIK, DR. AVINASH GAUR & DR. ASHISH MANOHAR URKUDE</i>	18
5.	STUDY OF PERCEPTIONS OF INDIVIDUAL INVESTORS TOWARDS INVESTMENT <i>DR. KANCHAN NAIDU & HETAL GAGLANI</i>	23
6.	A STUDY ON TRAINING NEEDS FOR EXECUTIVES IN SMALL AND MEDIUM ENTERPRISES AT SALEM DISTRICT <i>S. SUSENDIRAN, DR. T. VETRIVEL & M. CHRISTOPHER</i>	28
7.	NONFINANCIAL REWARD SYSTEM IN NIGERIAN PUBLIC AND PRIVATE ORGANISATIONS <i>DR. A. M. ABU-ABDISSAMAD</i>	32
8.	WORKING CAPITAL EFFICIENCY AND CORPORATE PROFITABILITY: EMPIRICAL EVIDENCE FROM INDIAN AUTOMOBILE INDUSTRY <i>DR. A. VIJAYAKUMAR</i>	35
9.	EFFECTIVENESS OF RESPONSIBILITY ACCOUNTING SYSTEM OF THE ORGANIZATIONAL STRUCTURE AND MANAGER'S AUTHORITY <i>ALI AMIRI, HOJJATALLAH SALARI, MARYAM OMIDVAR & JACOB THOMAS</i>	44
10.	A STUDY ON APPLICATION OF DATA AND WEB MINING TECHNIQUES TO ENRICH USER EXPERIENCE IN LIBRARIES AND ONLINE BOOK STORES <i>A. PAPPU RAJAN, DR. G. PRAKASH RAJ & ROSARIO VASANTHA KUMAR.P.J</i>	47
11.	IMPACT OF SIX SIGMA IMPLEMENTATION: A CASE STUDY OF A PHARMACEUTICAL COMPANY <i>N. VENKATESH & DR. C. SUMANGALA</i>	51
12.	A STUDY ON EVALUATING THE EFFECTIVENESS OF TUTORIAL PROGRAMS IN QUANTITATIVE TECHNIQUES <i>DR. ROSEMARY VARGHESE & DEEPAK BABU</i>	54
13.	PROFITABILITY ANALYSIS OF REGIONAL RURAL BANKS IN INDIA: WITH SPECIAL REFERENCE TO WESTERN REGION <i>DR. KAUSHAL A. BHATT</i>	59
14.	A SMALL TRIBUTE TO COMPUTER LEGENDS WHO MADE AN IMPACT ON THE COMPUTER INDUSTRY AND PASSED AWAY IN THE YEAR 2011 <i>PRITIKA MEHRA</i>	65
15.	A STUDY ON MANAGERIAL EFFECTIVENESS <i>ANITHA R & M.P.SARAVANAN</i>	68
16.	COMPARATIVE STUDY ON TALENT MANAGEMENT PRACTICES <i>DR. D. N. VENKATESH</i>	76
17.	REVIEW AND CLASSIFICATION OF LITERATURE ON RURAL CONSUMERS' BUYING BEHAVIOUR FOR MOBILE PHONE IN INDIA <i>CHIRAG V. ERDA</i>	87
18.	MOBILE BANKING IN INDIA: OPPORTUNITIES & CHALLENGES <i>DR. P. AMARAVENI & K. PRASAD</i>	92
19.	THE STUDY OF RELATIONSHIP BETWEEN REFINED ECONOMIC VALUE ADDED (REVA) AND DIFFERENT CRITERIA OF THE RISK ADJUSTED RETURN <i>MOHAMMAD NOROUZI & MAHMOUD SAMADI</i>	97
20.	ONLINE SHOPPING: A NEW TREND OF SHOPPING BEHAVIOUR <i>SANTHOSH J & ANU VARGHESE</i>	101
21.	IMPLEMENTATION OF PCA WITH SVD TO REDUCE PRECISION LOSS <i>AMITPREET KOUR & RAMANDEEP KAUR</i>	104
22.	AN ASSESSMENT OF UNIVERSITY-INDUSTRY RELATIONS FOR COLLABORATIVE TECHNOLOGY TRANSFER: THE CASE OF INSTITUTE OF TECHNOLOGY OF BAHIR DAR AND TECHNOLOGY FACULTY OF GONDAR UNIVERSITY <i>TADESSE MENGISTIE</i>	108
23.	DEMARKETING: A CREATIVE THINKING <i>ANITA KUMARI PANIGRAHI</i>	113
24.	A REVIEW OF ISLAMIC BANKING AND CURRENT ISSUES AND CHALLENGES FACED BY ISLAMIC BANKS ON THE WAY TO GLOBALIZATION <i>UZMA FAZAL, SALMA TARIQ, MUHAMMAD MUMTAZ, MUHAMMAD NAEEM, JUNAID ABBAS & MADIHA LATIF</i>	118
25.	THE IMPACTS OF PRODUCTIVE MARKETING COMMUNICATION ON EMERGING MARKET <i>LOO LAE SYEE, TAN KAI HUN, VIVIAN LEONG & RASHAD YAZDANIFARD</i>	124
26.	HP SUSTAINABILITY AS COMPETITIVE ADVANTAGE <i>RIDHI GUPTA</i>	129
27.	ELECTRONIC HEALTH RECORD IMPLEMENTATIONS AROUND THE WORLD <i>DIANA LÓPEZ-ROBLEDO & SANDRA SANTOS-NIEVES</i>	132
28.	FOREIGN DIRECT INVESTMENT (FDI): AN OBSERVATION ABOUT TOURISM INDUSTRY IN INDIA <i>SANDEEP KUMAR, RAJEEV SHARMA & NAVEEN AGGARWAL</i>	137
29.	A SYSTEMATIC APPROACH FOR DETECTION AND COST ESTIMATION OF CLONING IN VARIOUS PROGRAMMING LANGUAGES <i>ANUPAM MITTAL</i>	142
30.	INTELLIGENT SCADA FOR HOME APPLICATION <i>S. R. KATKAR</i>	147
	REQUEST FOR FEEDBACK	151

CHIEF PATRON

PROF. K. K. AGGARWAL

Chairman, Malaviya National Institute of Technology, Jaipur

(An institute of National Importance & fully funded by Ministry of Human Resource Development, Government of India)

Chancellor, K. R. Mangalam University, Gurgaon

Chancellor, Lingaya's University, Faridabad

Founder Vice-Chancellor (1998-2008), Guru Gobind Singh Indraprastha University, Delhi

Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

FOUNDER PATRON

LATE SH. RAM BHAJAN AGGARWAL

Former State Minister for Home & Tourism, Government of Haryana

Former Vice-President, Dadri Education Society, Charkhi Dadri

Former President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

CO-ORDINATOR

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

ADVISORS

DR. PRIYA RANJAN TRIVEDI

Chancellor, The Global Open University, Nagaland

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR

PROF. R. K. SHARMA

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

EDITORIAL ADVISORY BOARD

DR. RAJESH MODI

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. PARVEEN KUMAR

Director, M.C.A., Meerut Institute of Engineering & Technology, Meerut, U. P.

PROF. H. R. SHARMA

Director, Chhatrapati Shivaji Institute of Technology, Durg, C.G.

PROF. MANOHAR LAL

Director & Chairman, School of Information & Computer Sciences, I.G.N.O.U., New Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

PROF. R. K. CHOUDHARY

Director, Asia Pacific Institute of Information Technology, Panipat

DR. ASHWANI KUSH

Head, Computer Science, University College, Kurukshetra University, Kurukshetra

DR. BHARAT BHUSHAN

Head, Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar

DR. VIJAYPAL SINGH DHAKA

Dean (Academics), Rajasthan Institute of Engineering & Technology, Jaipur

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHINDER CHAND

Associate Professor, Kurukshetra University, Kurukshetra

DR. MOHENDER KUMAR GUPTA

Associate Professor, P.J.L.N. Government College, Faridabad

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

DR. BHAVET

Faculty, Shree Ram Institute of Business & Management, Urjani

ASSOCIATE EDITORS

PROF. ABHAY BANSAL

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. NAWAB ALI KHAN

Department of Commerce, Aligarh Muslim University, Aligarh, U.P.

ASHISH CHOPRA

Sr. Lecturer, Doon Valley Institute of Engineering & Technology, Karnal

TECHNICAL ADVISOR

AMITA

Faculty, Government M. S., Mohali

FINANCIAL ADVISORS

DICKIN GOYAL

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS

JITENDER S. CHAHAL

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT

SURENDER KUMAR POONIA

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography; Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript anytime** in **M.S. Word format** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website ([FOR ONLINE SUBMISSION, CLICK HERE](#)).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: SUBMISSION OF MANUSCRIPT IN THE AREA OF

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____ ' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:

Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

- a) The whole manuscript is required to be in **ONE MS WORD FILE** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
- b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
- c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
- d) The total size of the file containing the manuscript is required to be below **500 KB**.
- e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
- f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name, designation, affiliation (s), address, mobile/landline numbers, and email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.
6. **MANUSCRIPT:** Manuscript must be in **BRITISH ENGLISH** prepared on a standard A4 size **PORTRAIT SETTING PAPER**. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.
7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.
9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION**REVIEW OF LITERATURE****NEED/IMPORTANCE OF THE STUDY****STATEMENT OF THE PROBLEM****OBJECTIVES****HYPOTHESES****RESEARCH METHODOLOGY****RESULTS & DISCUSSION****FINDINGS****RECOMMENDATIONS/SUGGESTIONS****CONCLUSIONS****SCOPE FOR FURTHER RESEARCH****ACKNOWLEDGMENTS****REFERENCES****APPENDIX/ANNEXURE**

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed **5000 WORDS**.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure. Sources of data should be mentioned below the table/figure.** It should be ensured that the tables/figures are referred to from the main text.
11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.
12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:
 - All works cited in the text (including sources for tables and figures) should be listed alphabetically.
 - Use (ed.) for one editor, and (ed.s) for multiple editors.
 - When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
 - Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
 - The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
 - For titles in a language other than English, provide an English translation in parentheses.
 - The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:**BOOKS**

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19-22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 <http://epw.in/user/viewabstract.jsp>

TERRORISM: A BIG THREAT FOR TELECOM AND INTERNET BASED COMMUNICATION

VISHAL KAUSHIK
PROGRAMME HEAD
COMPUTER SCIENCE ENGINEERING
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN

DR. AVINASH GAUR
SR. PROFESSOR
RAJKUMAR GOEL INSTITUTE OF TECHNOLOGY
GHAZIABAD

DR. ASHISH MANOHAR URKUDE
SR. PROFESSOR & CEO
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN


ABSTRACT

Modern Information Communication Technology has enabled Human beings to connect faster through various ways; via text mails or messages, voice through telephone or mobile and video calling or image via Facebook, YouTube, and Skype, etc. The antisocial bodies like terrorists are able to connect, command and control (C3) [1] easily just like any normal citizen [2] without even being noticed by any security scanner. The attacks like 9/11 on the World Trade Centre, New York, the planning and brazen execution of 26/11 attacks on Mumbai, Ahmedabad, Pune, Bangalore, and Bodhgaya serial blasts in Bihar [4], India, and the Assam riots based on the false YouTube video clips and the provoking Facebook walls or text messages showcase live examples of how the terrorists are using technology for their desired purpose and there is no way they could be checked during the initial phase of their action plan. Terrorists use technology for provisioning, financing, networking, recruitment, information gathering and for final execution purposes [5]. In every of these attacks, they were much ahead in using these technologies than even best brains in Military could think off. Hence, mostly the activities can be classified under the heads of Activism, Hactivism and Cyberterrorism. [3] The present paper discusses on how the terrorism puts a big threat for telecom and internet based communication technologies those are being used against the civil societies all across the world irrespective of all boundaries, barriers and sections of the society. We conclude on how, such threats could be avoided by implementing GOVI [4] as the Global Communication Technology Policy Framework.

KEYWORDS

GOVI, Cyber Terrorism, Terrorists & Information Communication Technology, video communication, text communication, voice communication, international communication policy framework.

INTRODUCTION

 Globally the most dangerous terror organizations are now using modern ICT tools and services to better organize and coordinate dispersed activities by operating in more flat and decentralized groups tied with common goals. [1] Without technologies such as the web and mobile phone communication, al-Qaeda would have been faded away long time ago. [5] The militant organizations have been availing cyber assistance in order to achieve extremist missions as a regular practice after 9/11. The Al Qaeda executed a series of cyber-attacks against the US government through the threat messages defecation of govt. websites, disruption of internet communication for government and citizens.

The early evidences of Cyber Terrorism include the anti NATO propoganda, denial of Service DoS attacks on e-commerce portals like eBay & yahoo in 1999, and hacking of NATO websites during Kosovo, 2001 the Internet Black Tiger's attacked on Sri Lankan embassy with 800 emails carrying extremist messages to 'disrupt the communications', Sri Lanka, 1997 [6] and cyber-jihad against Israeli and American websites initiated by Pakistan based or Muslim hackers in support of the Palestinian militant forum "al-Aqsa" Intifadah.

India also has seen an emerging phenomenon of cyber terrorism. The 2008 serial blasts in Ahmedabad, Delhi, Jaipur, and Bangalore have showcased strong evidence of cyber terrorism. [7] The November 2008 Mumbai attacks also popularly known as 26/11 have witnessed the exhaustive use of telephone, mobile, satellite phones, GPS and Internet technology during all phases of its execution right from the planning to execution at various target spot in Mumbai. The Muslim Jihadists like the Indian Mujahiddin, SIMI etc. are commonly highlighted to be behind such acts but the surprising fact appearing from the analysis reports on news [8] shows the sharing and spreading of terror messages and announcements claiming to shoulder responsibility for terror attacks had been done by non-Muslim youths as well. This is what has happened during Assam Riots. [9] But the non-Muslim fundamentalist groups and their movements against governments are still least focused. [10]

INFORMATION AND COMMUNICATION TECHNOLOGY

The new communication and computing technologies allow the establishment of networks in three critical ways. [11] First, the telephone reduced transmission/transition time between locations in large corporations and with decentralized operations dispersed across local branches which communicate and coordinate jobs. Second, the networked design significantly reduces cost of communication through easy sharing of vital information and costly resources across the organization. [1] The benefit of IT and the Internet is in the capacity to store, analyse and communicate information instantly, anywhere, at negligible cost. The IT revolution has increased the capacity and speed of communications networks and lowered down the telecommunication costs as well and so the users worldwide has grown to more than 350 million and may reach 1 billion within four years. [12] And third, increased the scope and complexity of the information could be shared, through the integration of computing with communications. Therefore the new phenomenon is now known and termed as ICT (Information Communication Technology). IT and the Internet amplify brain power in the same way that the technologies of the industrial revolution amplified muscle power [13]

TERRORISM AND MODERN TECHNOLOGY

The latest communication technologies enable terrorists the coordination of their operations in networked groups. Other benefits include increase in communication speed, reduced costs, increases in bandwidth, globally expanded presence, and the integration of communication and computing technologies.

[14] The Terrorists make use of information and communication technology to form the voice or data networked groups for planning, command and control their missions. [15]

The presence of the terrorist groups on the net benefits their organization in eight different ways. These are psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination. [16]

INFORMATION PROVISION

It means the secure publicity, propaganda like historical information, profiles of leaders, manifestos, etc. or psychological warfare through disinformation, threat delivery or disseminating horrific images, such as the beheading of American entrepreneur Nick Berg in Iraq and US journalist Terrorist 12 'Use' of the Internet and Fighting Back Daniel Pearl in Pakistan via their Web sites. [16] Earlier else the terrorists had to pass the multistage editorial selection to attract the attention of television, radio, or the print media. But the web is far easier to own by terrorists. Internet provides direct control over the content and extends their ability to shape and manipulate not only their own image, but also the image of their enemies perceived by the different target audiences. The Al-Qaeda 9/11 terrorist team used Internet for various activities such as the flight schedule query, online purchase of tickets, stealing of social security nos. and obtaining fake documents and also gathering information about the flight schools, location maps/ blueprints of targets. [15] The hackers applauded and commended the attacks. They defaced hundreds several web sites and launch Distributed Denial of Service (DoS) attacks against targets.

Islamic Militants have developed various sophisticated ways to spread propaganda via mobile phones and Bluetooth technology to anonymously share provoking and hate information among potential supporters. The information packages usually contain videos, songs, speeches and images etc. [17] The SMS texting has become increasingly popular among the Pro Terrorists just like the non-terrorist audience. In fact certain terror organizations have branded their specific Mobile User Interface like a political party or any other organization has. The following picture showcases a few popular interfaces from Mujahedeen etc.

FIGURE 1: ARMY OF THE MUJAHEDDEEN AND ISLAMIC STATE



INFORMATION GATHERING

The terrorists use the internet to gather information. A lot of dangerous information about fabrication of bomb, explosive and destructive devices etc. is openly available on the internet, bookstores and libraries. [35] [36] There is ready accessibility of the data and technical expertise like CBRN weapons programs documents on the public websites. The hate groups can easily download from the internet. [37] And it is a fact that most of the government and nongovernment web sites around the world contain vital pieces of information openly available for Internet based terrorists.

The information not directly available on the web can be hack attacked from the systems connected to internet. There are kind of open universities teaching hacking techniques via discussion forums, bulletin boards on internet. In 1998, certain classified and unclassified U.S. government software and data from India's BARC (Bhabha Atomic Research Center) was gained by Khalid Ibrahim from hackers over Internet Relay Chat (IRC) [37] using online aliases RahulB and Rama3456. Ibrahim, an Indian citizen and a member of 'Harkat-ul-Ansar', a Kashmiri militant group. [38]

NETWORKING

The Al Qaeda terrorists have been using ICT based technology for communication and coordination purposes of their plans since the very early stage of their existence. The US telecom companies had registered numerous calls in their database between the Ramzi Yousef (1993, World Trade Centre, Bomber) and other terrorists involved in the plan. [18] His computer was found with the data related to flight schedules, future attack plans and various chemical formulae etc. [19] Terrorist websites refer to various existing and some emerging like mobile to web techniques like VoIP, Mobile GPS Mashups and Number Spoofing Techniques etc. for mobile phones. The basic examples cover Pro Terrorist Propaganda Mobile interfaces, Mobile GPS for movements, Ops, Targeting and Exploiting, Mobile Surveillance Tool, Voice Changers for Terrorist Phone Calls, Red Teaming Perspective on the Potential Terrorist Use of Twitter. [20]

Al-Qaeda has alliances with Egypt's Islamic Group, the National Front in the Sudan, the government of Iran, and Hizbollah. There are reports also about its ties with other far-flung Islamic armed groups, such as Abu Sayyaf in the Philippines, as well as with counterparts in Somalia, Chechnya, and Central Asia. [1]

INFORMATION SHARING

The terrorists use the websites for fast sharing of the information. A number of 'Hoe To' web pages are making huge proliferation on to explaining the technicalities of making homemade destructive devices and explosives etc. The otherwise innocuous material in lethal combinations may be used to make such homemade bombs. More dangerously there are several versions of information on Bacteriological weapons attack available on number of sites and in the book format. [39]

Such availability and sharing of the evil information has been playing significant a role in facilitating not only the sophisticated terrorist and other hard core criminal but also by disaffected and raged individuals to showcase their particular agenda. An example A right-wing extremist David Copeland in 1999 learnt from The Terrorist's Handbook and How to Make Bombs and planted nail bombs in three different areas of London by killing three and injuring 139 personals in just three week time. A big thousand paged manual by Al Qaeda, "The Encyclopedia of Jihad", containing complete strategy and plan to establish an underground organization and execute terror attacks is hugely distributed over the Web. [15]

They are present all over and through all sorts for quick sharing and influential penetration of information. Ayaf a prolific contributor to the Islamic Renewal Organization (IRO) website announced on an internet forum about his connection with Al Qaeda US wing led by Abu-Azzam al-Amriki. He further shared the future plans to destroy a nuclear reactor.

The young French Muslims in the suburbs of Paris and some 300 other cities across France were actually misled by some false and fabricated information spread over online French blogs and mobile phone text messaging. The false messages were used to organize, mobilize, and incite the mobs of young French Muslims to violence in the suburbs of Paris and some 300 other cities across France.

Similarly the flooding of falsify information, pictures and morphed videos over the social networking websites like facebook and text SMS spreading through the mobile networks created panic among the people from the northeast India and triggered the uncontrolled migration of Muslims from different corners of the nation to their homeland during the riots in Assam, India. It was so big flood of misleading information that the Government had to ultimately put a ban on SMS

services. [41] Anees Pasha a mobile shop owner "Fonotech" in Koramangala, Bangalore spread rumours through SMSs and uploaded doctored videos to incite hatred against people from the northeast region.

These events clearly show that how the internet has been used as a valuable tool for distorting the debate and disseminating misleading images of reality, as well as fueling emotions with messages of hatred and promotion of violence. This eases the way the passing of operational information and coordination of activities between terrorist cells operating in different geographical spaces.

FUNDING AND RECRUITMENT

Funding is a must for the operations of terrorist network.[51] The internet has global reach and secrecy necessary for the fundraising activities. Al Qaeda and such others depend on donations in the form of charities. They ask for such financial help through websites, chat rooms, forums and blogs containing misleading information for sake of the false religious achievements. They advertise their account numbers and the religious sympathy anonymously support monetarily. Babar Ahmad a mechanical engineer used to run a network of websites for fundraising for Islamic extremists, including Chechen rebels, the Taliban militia and Al Qaeda affiliates. Terrorists also use the modern software tools to identify sympathies for a cause. The individual emails are then sent requesting for donation to organizations with no direct ties to the terrorist organizations.

The recruitment of terrorists has also become easy through the interest of web users surfing their websites. The interested profiles which are felt suitable for a cause are contacted individually by the recruiters roaming online chat rooms or cybercafés. The vulnerable youth are individually contacted with aggressive with religious propaganda encouraged to join global jihad movement. This all process takes place on various secret online chat rooms and software 'Paltalk' which enables users to communicate openly on the internet without fear of being monitored is used for personal counseling or brainwash. [3]

CHARACTERISTICS OF ICT BASED TERRORISM

The information communication age technology and exchanges increase the range, speed and amount of spread of information among the network in an organization. [21] ICT networked terrorist groups may operate under stealth in any part of the world without any governmental protection [22] The communications between al-Qaeda's members is structured like "hub-and-spoke" structure (each terrorist communicate with bin Laden and advisers in Afghanistan) or a wheel structure (nodes in the network communicate with each other without reference to bin Laden). [23]

The terrorists connect to phone (fixed or mobile) and Internet (websites, emails or chat etc.) over public shared infrastructure just like any normal citizen does. Their phone conversation signals are encrypted. They may also use a SIM programmed with stolen phone numbers the phone cloning is very easily possible. A phone number can be stolen with the help of a special scanner is used to "snatch" legitimate phone information from the airwaves i.e., the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) programmed into a single cell phone just before using it. In absence of a well-defined Global policy framework and technology the terrorists may anonymously bulk purchase prepaid phone cards to look them connect like normal citizens and so hide their communications from scanners. They normally discard the phone after using it. [24]

They may use an inbound devised and defined code language to communicate in between their gang. The 9/11 attackers openly communicated using predefined codes. [25] Their emails contained simple conversation words as between normal citizens so were difficult to understand and analyze their plan. Phone calls between the attackers gang used coded conversation too.

The Bin Laden with the help of Egyptian computer expert established a well-defined operative and kind of secure computer and communications network in mountains of Afghanistan. [26] CD ROMs were used for storing information on recruitments, bomb making, heavy weapons and attack plans. Bin Laden himself used satellite phone terminals to communicate and coordinate. His messages were dictated to an assistant and relayed telephonically from a different location. [27]

Indian perspective also witnesses several incidents of terrorists using the modern Information and communication tools. After 26/11 attack, the Indian Ministry of Home affairs, in their annual report (2010), had released a detailed nexus between digital technology and its misuse by extremists. [9] Terrorists were using the mobile phones just like any personnel communication investigations found that the devices like GPS etc. were used to Map the targets and plan, also during the attack the personal communication via cell or satellite phones was used to motivate for massacre. The six handlers & commanders of the Lashkar-e-Taiba including Sajid Mir, an ISI agent were sitting in a control room (a kind of base camp) set up in the VIP area between the Karachi international airport, the Malir cantonment and Quadiabad. [28] They remote-control the ten attackers in Mumbai in a real time fashion as counter strategy of actions by Indian forces and Police after watching and analyzing the Live TV News. [29] And in fact they were even analyzing the Twitter or Facebook posts by common citizens about current status of situations, and / or information about their dears and nears, public alerts for the sensitive areas, and the information for the medical assistance like blood camps etc. for the wounded were lively accessed by the terrorists to regulate the intensity of attacks along with the general websites providing information about Mumbai target areas were surfed during the planning phase. [30] The 2010 Varanasi blast or July 2011, Jhaveri Bazaar, Mumbai blasts were claimed by Indian Mujahiddin through emails while once again witnessing the use of Internet communication. [9]

SUCCESS FACTORS – ICT BASED TERRORISM

The terrorist organizations use Information and Communication Technology such as cell phones, satellite phones, emails, chat rooms, blogs etc. in a manner that becomes almost impossible to trace in the world population almost 7 billion people. Al Qaeda operatives used the internet in public places and communicated using free web-based email accounts to preserve anonymity. The terrorist groups like Hamas are present in chat rooms to discuss and plan operations and the email communication for operation and coordination across Gaza, the West Bank, Lebanon and Israel. Electronic delivery of instruction is coded dialects and the Western intelligence and security services have few or no trained linguists. [3] The Indian Mujahiddin operatives refrained the personal Internet access to shadow the terrorists during the 2010 Varanasi or July 2011, Jhaveri Bazaar, Mumbai blasts. Their terrorists claimed the ownership of blasts through emails accessed through cybercafés. [9]

The Al Qaeda used CD ROMs for information storage. Bin Laden himself used satellite phone terminals to communicate and coordinate but he was refrained from direct use to safeguard him from all sorts of the scanners. His messages were dictated to an assistant, and who then relays it telephonically from a different location. [27]

The 9/11 attackers had defined code words describing the World Trade Center as "Faculty of Urban Planning", the Pentagon as the "Faculty of Fine Arts." [25] Hence they openly communicated and disseminated information. Their emails were difficult understand to belong to Terrorists. Email from Abu Abdul Rahman to Ramzi bin al-Shibh looked like love text between a boy and his girlfriend in Germany –

"The first semester commences in three weeks (the time left for the attacks). Two high schools (referred to the twin towers) and two universities (Pentagon and the Washington DC). This semester will surely be hot19 (no. of hijackers). Certificates for private exams and four exams (no. of planes). Regards to the Professor (Laden) Goodbye".

Phone calls from Mohammad Atta to fellow attacker were also coded into puzzle like [31] –

"Two sticks, a dash and a cake with a stick down".

All this so well planned and managed that even after attacks, hoax email claimed that the string "Q33" was the flight no. and upon changing it to the windings font present in Microsoft Office it revealed the target as " 033".

Online money raising as the case of Lashkar-e-Taiba ("Army of the Pure") from Pakistan and its parent organization, Markaz ad-Da'wa Wal Irshad (Center for Islamic Invitation and Guidance), have raised lot of money mostly from sympathetic Wahhabis in Saudi Arabia, that they are reportedly planning to open their own bank. They benefit financially the Mujahiddins and a normal mujahideen earns 15,000 rupees per month -- more than seven times what the average Pakistani makes. [32]

Electronic exchange of messages and communication can increase the range, amount, and velocity of information flow in a network organization and on the brainwashed terrorists this impacts as face-to-face interaction. [21]

Open Sources of information i.e. the systematic collection of foreign media is an important phenomenon among terrorist groups that use the media and the Internet to communicate leadership guidance through web or other means of networking and sharing. [42] The French Anonymous Society (FAS) website publishes a two-volume Sabotage Handbook that contains sections on planning an assassination and anti-surveillance methods amongst others.

Department of Defence (DoD) websites also host DoD plans, programs and activities would provide more than eighty percent of information. Around 700 gigabytes of such unclassified but harmful material was available for ready downloads on DoD websites. [43] Besides, there is information about the location and operation of nuclear reactors and related facilities available openly on the websites of Nuclear Regulatory Commission (NRC). [44]

The arrest of Al-Qaeda computer expert Muhammad Naem Noor Khan in Pakistan in July 2004 found his computer with photographs and floor diagrams of buildings in the U.S. that might be the potential targets of future attacks and planning. [45] A terrorist charged in Australia visited Australian government Web sites to get maps, data, and satellite images of potential targets. The government of New South Wales decided to restrict the information available on their Web sites. [46]

PREVENTION MEASURES

The 9/11 has alerted the intelligence and security agencies around the world. State intelligence reviewed their online presence. After the 9/11 attacks some U.S. Government agencies took off a lot of information from their sites that could be useful to terrorists planning attacks. Nuclear Regulatory Commission closed its website and pages were removed from the websites of Department of Energy, Interior Department's Geological Survey, Federal Energy Regulatory Commission, Environmental Protection Agency, Federal Aviation Administration, Department of Transportation, National Archives and Records Administration, the NASA Glenn Research Centre, International Nuclear Safety Centre, Los Alamos National Laboratory, Geographic Information Service, National Imagery and Mapping Agency. The information might be useful for the terrorists like chemical industry risk management plans; pipeline mapping information, chemical risk profiles, National Transportation Atlas Databases etc. was removed. [16]

The MI5 (the British Security Service) had appealed for information about potential terrorists on Arab websites. A poignant message in Arabic was posted on sites suspected to be accessed by extremists like Islah.org (a Saudi Arabian opposition site) and Qoqaz.com (Chechen jihad site). [33] [34]

Change of methods and modus operandi of security and intelligence agencies. Try and trust every bit of information available from any source and anywhere. Before 9/11, FBI did not use and their intelligence databases did not register internet based or any public shared information. [47] Starting new facets of intelligence organizations and their presence on the public shared ICT networks to monitor sorts of evil activities or establishments. Internet Haganah, self-described as "an internet counterinsurgency", and the Washington DC based Search for International Terrorist Entities (SITE) Institute have clients including the FBI, Office of Homeland Security, and various media organizations. These agencies focus on the Islamic terror groups. And their operative is not to silence rather to feel them free and let them move and change addresses and communicate this way gathers much information after they make mistakes. [48]

Social propaganda in favour of humanity like Cyber Angels (a computer enthusiasts group) promoted and sponsored television advertisements in US urging hackers to help gather information and intelligence on involved in hacktivism. Dispatchers (hackers group) voiced their rage against terror and they also initiated counter cyber-attacks against the web servers and Internet access in Afghanistan and other terrorism supporting nations. They further defaced hundreds of Web sites and launched Distributed Denial of Service (DoS) attacks against Iranian Ministry of the Interior and the Presidential Palace of Afghanistan. [16] Another group, Young Intelligent Hackers against Terror (YIHAT) founder, Kim Schmitz, to breach two Arabic banks having connections with Osama Bin Laden. Chaos Computer Club, German hacker's organization called for global communication to resolve the conflict. [49]

SECURITY HOLES

Technological Fixes play a big role to monitor, analyze and counter the terrorists making open use of information and communication technology (ICT). The National Security Agency (NSA) was very slow in terms of technology upgrade in telecommunications. They have started to upgrade their technology bases only after the 9/11 conspiracy. FBI's DCS-1000 e-mail packet-sniffer system proved to be less effective and hence has not been employed since 2002 instead commercial monitoring applications have been employed to aid their investigations. Honey Pots the classic spy tactic like hosting bogus websites to attract the target persons should also be deployed. The other technical fronts should be heeded with ample funds availability. [50]

The removal of technical information from public Web sites is no guarantee of safeguarding it. These materials can be stored onto other international Web servers that do not comply cannot the U.S. legislation. [37]

Smarter new terrorists can also use the Internet to learn about antiterrorism activities. This job can be done by simply performing the string of word searching through online newspapers and journals. They may get the complete view of the strategies designed, plans to counter attacks or the potential vulnerabilities. [40]

GOVI STOPS ICT USED BY TERROR

A global policy mandated for the Information and Communication Technology around the world would be a potential solution towards the global problem of terrorists getting multifaceted and tremendous benefits from the wide use of modern Communication technology. All the governments of world nations would share a common technology framework for all faces and all uses of ICT.

The suggested technology framework named as GOVI (Global One Voice ID) would have a direct thread attached to the Government Security and Intelligence Agencies. GOVI has proper technology protocols on every use of each face of technology of Information and Communication Technology. GOVI is a global unique identification number that grants every person an access to connect through any of the communication tool from postal letter, telegraph, Phone, Mobile, PTT, Pager, email, Online chat, website, billboard, net-banking etc.

GOVI protocol suit manages each communication/ call initiated routed and terminated through the single GOVI locally, nationally and internationally. All the communication transactions shall be recorded in the Network Access and Equipment Registration Sheet (NARESH) database clustered nationwide zones and the replica views shared with the service providers. The NARESH database would contain the present entities GOVIs and their locations along with the serving companies/ networks for all kinds of services. The Internet connectivity too would be threaded with GOVI ids. No GOVI can be present at more than one location at one point of time. The duplicate GOVIs found in NARESH database would be automatically logged out of the global ICT network. To increase the security all suspected GOVIs could be monitored easily as there will be no other anonymous identity attached to them globally.

The website would have the national signature globally and one GOVI identity directly attached with them. Therefore all the websites will provide direct link to intelligence databases thus any malicious or dubious website could be easily traced and prevented through domains and hosting.

This way the terrorists would be prevented from the activities like using telephone based mobile communication or internet based e-mail, chat communication and networking, web based fund raising, recruitment and information provisioning etc. Even if they try through hacking or anything else the investigation and security agencies may be able to deduce an easy path to them. Also the people from general population can also oppose the terror based false and hating information. Any one from the general public can trace the actual root cause of such anonymous identities.

CONCLUSION

1. GOVI as a unique communication identity for the voice, data and video communication services provided to each person around the world after personal screening and rigorous verification done by the local intelligence units or security agencies to the local citizens. [4]
2. This data is shared across the global telecom authorities for the valid instance. Hence, the foreign citizens need not apply for GOVI, if they travel in other countries. While travelling, the person just has to take permission via log in to the visiting country's networks, within few seconds time. [49]
3. This will prevent the evil use of the communication network around the world as it refrains the access of any type of communication network and thus stopping the terrorism using the ICT as a medium. [51]

FURTHER SCOPE OF STUDY

1. Designing a policy framework for the global communication ICT networks
2. SIM card obsolescence issue and/ or modifications in the mobile, laptop and other devices.
3. Military personnel security issues
4. Standardization of the framework through ITU, IEEE, IETF, cyber-security, etc. bodies around the world.
5. Feasibility and network updating issues around the globe/ and each and every country.

REFERENCES

1. Michele Zanini and Sean J.A. Edwards, "THE NETWORKING OF TERROR IN THE INFORMATION AGE", *Networks and Netwars: The Future of Terror, Crime, and Militancy* p29-60
2. Richard Clarke, "Terrorists use the Internet just like everybody else", 2004
3. Anonymous, Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, "A Framework for Understanding Terrorist Use of the Internet", *ITAC-CIEM Trends in Terrorism Series*, volume 2006-2
4. Vishal Kaushik, Avinash Gaur, "GOVI – Global One Voice Identity, An Effective Approach to Prevent Malicious Telecom Usage like Terrorism and Other Issues", *CONIAPS XIII*, June 2011
5. "Cataloguing the Materials Put Online by Jihadists", Study report by German researcher Nico Prucha
6. Dorothy E. Denning, "Terror's Web: How the Internet Is Transforming Terrorism", to appear in *Handbook on Internet Crime* (Y. Jewkes and M. Yar, eds.), Willan Publishing, 2009 aka. Denning, 2010
7. "The terror thirteen of Indian Mujahideen", Anuj Dhar, NDTV Correspondent, September 22, 2008
8. "Extreme usage of cyber communications", NDTV News analysis report, 2010
9. Debarati Halder, "Information Technology Act and Cyber Terrorism: A Critical Review", *Social Science Research Network*, Aug, 2011
10. Anonymous, "The Use of the Internet for Terrorist Purposes", United Nations New York, In Collaboration with the United Nations Counter-Terrorism Implementation Task Force, 2012
11. Monge & Fulk, "Communication technology for global network organizations", In G. DeSanctis & J. Fulks (Eds.), "Shaping organizational form: Communication, connection and community", Newbury Park, CA: Sage, 1999, pp. 71-100
12. Pam Woodall, "Untangling e-economics", survey by Survey, *The Economist*, Sep, 2000
13. Bradford DeLong, Pam Woodall, "IT and the Internet amplify brain power in the same way that the technologies of the industrial revolution amplified muscle power", Chapter 1: E-Commerce and the New Economy, *Electronic Commerce: Economics and Strategy*, Draft 1.1, December 19, 2000
14. Beverly H. Burris, "Technocracy at work", Heydebrand, 1989
15. Gabriel Weimann, US Institute of Peace, "How Modern Terrorism Uses the Internet", Volume 31, DIANE Publishing, 2004, ISBN 1437904165, 9781437904161
16. Maura CONWAY, "Terrorist 'Use' of the Internet and Fighting Back", *Information & Security*, An International Journal, Vol.19, 2006, 9-30
17. Anonymous, "Jihadists use mobiles as propaganda tools", BBC Report, 21 April, 2011
18. Video, "Targeted: Volume 1, The Evil Genius (Ramzi Yousef)", Wild Eyes Productions for the History Channel; A&E Networks, 2003
19. Reeve, Simon, "The New Jackals: Ramzi Yousef, Osama Bin Laden and the Future of Terrorism", Boston, Mass. Northeastern University Press, 1999
20. Anonymous, Supplemental to the 304th MI Bn Periodic Newsletter "Al Qaida-Like Mobile Discussions & Potential Creative Uses", 304th MI Bn OSINT Team, October, 2008
21. Nohria N. and R. G. Eccles, "Face-to-Face: Making Network Organizations Work" In *Networks and Organizations: Structure, Form & Action*, Harvard Business School Press, 1992, pp 289-290
22. Soo Hoo, Kevin, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival*, Vol. 39, No. 3, Autumn 1997, pp.135-155
23. Simon and Benjamin, "America and the New Terrorism", *Survival* vol. 42, no. 1 Spring 2000, pp.59-75
24. Denning and Baugh, "Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism", National Strategy Information Center, Washington, DC, July, 1997
25. Anonymous, "Al-Jazeera offers accounts of 9/11 plan", CNN Report, Sep 2002
26. Anonymous, "Tracking Bin Laden's E-mail," *Newsweek*, August 2000
27. Kelley, "U.S. intelligence agencies recently obtained computer-disk copies of a six-volume training manual used by bin Laden to train his recruits", 2000
28. Sebastian Rotella, "On the trail of Pakistani terror group's elusive mastermind behind the Mumbai siege", *Washington Post*, 13 November 2010
29. Neeta Sharma, Surabhi Malik, Shamik Ghosh, "26/11 control room was located in Karachi, says Abu Hamza", *NDTV News*, June 2012
30. Onook Oh, Manish Agrawal, H. Raghav Rao, "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter", *Information Systems Frontiers* March 2011, Volume 13, Issue 1, pp 33-
31. Terry Mcdermott, "Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It", Harper Publications, ISBN 0060584696, 2005
32. Jessica Stern, "Pakistan's Jihad Culture", *Foreign Affairs*, (November/December 2000)
33. Stephanie Gruner and Gautam Naik, "Extremist Sites under Heightened Scrutiny," *The Wall Street Journal Online*, October 2001
34. Richard Norton Taylor, "MI5 Posts Terror Appeal on Arab Websites," *The Guardian*, October 2001
35. Michael E. Conti, "Beyond Pepper Spray: The Complete Guide To Chemical Agents, Delivery Systems, And Protective Masks", Paladin Press, January, 2002
36. Anonymous, United States Department Of Justice, "Report On The Availability Of Bombmaking Information, The Extent To Which Its Dissemination Is Controlled By Federal Law, And The Extent To Which Such Dissemination May Be Subject To Regulation Consistent With The First Amendment To The United States Constitution", April 1997
37. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies", *BiblioScholar*, 2012
38. Niall McKay, "Do Terrorists Troll the Net?" *Wired*, November 1998
39. Jessica Stern, "The Ultimate Terrorists", Harvard University Press, 1999
40. Gabriel Weimann, "Terror on the Internet: The New Arena, The New Challenges", International Studies Association (ISA) Annual Conference, Montreal, Quebec, Canada, 17-20 March 2004
41. Shreya Shah, "India Bans Mass SMS to Counter Panic", *Wall Street Journal*. Aug 17, 2012
42. Dan Verton, "Black Ice: The Invisible Threat of Cyber-Terrorism", McGraw-Hill Osborne, 2003
43. Declan McCullagh, "Military Worried about Web Leaks," *C|Net News*, 16 January 2003
44. Dan Verton and Lucas Mearian, "Online Data a Gold Mine for Terrorists," *Computer World*, Aug 2004
45. Douglas Jehl and David Johnston, "Reports That Led to Terror Alert Were Years Old, Officials Say," *New York Times*, 3 August 2004
46. Australian Broadcasting Corporation, "NSW Considers Limits on Government Website," *ABC Online*, 28 April 2004
47. Staff Statement No. 9 Law Enforcement, Counterterrorism, and Intelligence Collection in the United States prior to 9/11 (Washington DC: 9/11 Commission, 2004)
48. John Lasker, "Watchdogs Sniff Out Terror Sites", *Wired News*, Feb 2005
49. Charles Hauss and Alexandra Samuel, "What's the Internet Got to Do With It? Online Responses to 9/11", *American Political Science Association Annual (APSA) Convention*, Boston, 2002
50. Bernhard Warner, "Experts Comb Web for Terror Clues", *The Washington Post*, November 2003
51. Vishal Kaushik, Avinash Gaur, Ashish Manohar Urkude, et.al., "E-Money: An approach to counter currency crimes through ICT", *IRACST – International Journal of Commerce, Business and Management (IJCBM)*, Vol. 1, No.1, 2012, pp. 8-13
52. Vishal Kaushik, Avinash Gaur, "GOVI: How Does World Communicate With Secure Entities for Personal Communication", *ICETDSMT*, March 2013

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail infoijrcm@gmail.com for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

