Society & Change
Vol. X, No.2, April-June 2016
ISSN :1997-1052 (Print), 227-202X (Online)

Analyzing the Challenges of Cybercrime in the Global Context: Need for A Cross –Border Response

Tariq Bin Sarwar[1]

Abstract

Cybercrime is a relatively new phenomenon. The technical aspect of this crime has distinguished it from the conventional crimes. Therefore, there have been dialogues globally over the challenges posed by cybercrime and the possible means of preventing it. It has been a much talked issue in the last few decades and the discussion continues since the cybercriminals are persistent. The article tries to understand the nature and feature of cybercrime along with its dimensions. There have been attempts to prevent cybercrime in different legal systems of the world. The research makes a comparative analysis regarding the issues of cybercrime which includes the challenges posed by cybercrimes for both the developed and developing countries and the implications of those crimes. The article evaluates both international and national initiatives challenging cybercrime in a globalized world where technology has deleted all the borders between and amongst the states and criminal activities have emerged as a global phenomenon. It is seen that in combating cybercrimes greater responsibility lies upon the business groups and the technologists.

Keywords: Cybercrime, Cybercriminals, Cross-Border Response, Cyber Security Strategy, Challenges in Combating Cybercrime.

Introduction

Former Secretary General of Interpol Ronald K. Noble observed "Cybercrime is emerging as a very concrete threat. …Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats we will ever face."[2] It demonstrates that combating cybercrime has not been easy. The objective of the research is to identify the challenges posed by cybercrime and find the best possible means of

[1] Lecturer, Department of Law, Northern University Bangladesh, e-mail: tariqsarwarman@gmail.com

[2] Issues Monitor**,** Cyber Crime – A Growing Challenge for Governments, July 2011, Volume Eight, KPMG INTERNATIONAL, p. 6, available at https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf, last accessed on 11.02.15.

overcoming those. Crime is an age old phenomenon but cybercrime is a recent development. Needless to say less than hundred years ago people of the world never heard of anything like cybercrime. It is a special species of crime like white collar crime; corporate crime etc. The crux of the problem is to define and categorize cybercrime. This is a cumbersome task to be performed by the state through legislation since cybercrime is a changing and evolving thing. Generally, crimes are defined in terms of the end result and not how that result was brought about.[3] However, cybercrime is necessarily an exception to this general rule since here the tools of committing the crime is the determining factor to bring that act within the definition of crime. Some conventional crimes become cybercrimes if those are committed by using computer technology. Cybercrime is a major concern for the global community as the introduction, growth, and utilization of information and communication technologies have increased the criminal activities.[4] It is an obvious form of international crime that has been affected by the global revolution in ICTs.[5] The peculiarity of this crime is it can be committed in a jurisdiction without being physically present in it.[6] This necessitates the existence of effective supranational as well as domestic mechanisms that monitor the utilization of ICTs for criminal activities in cyberspace.[7] The cross-national nature of most computer related crimes have rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective even in advanced nations, while the 'digital divide' provides 'safe havens' for cyber-criminals. In response to the threat of cyber-crime there is an urgent need to reform methods of mutual legal assistance and to develop trans-national policing capability.[8]

Cybercrime: An Overview

The history of cybercrime begins with the development of computer. The first published accounts of computer manipulation, sabotage, espionage, and

---

3 Craig J. Balkeley, Combating Cybercrime: the Legal (&Practical) Challenges, Alliance Law Group, available at http://www.alliancelawgroup.com/cybercrime.pdf, last accessed on 27.01.2015.

4 Parker, D. (1998), Fighting Computer Crime: For Protecting Information, John Wiley, USA, p. 10.

5 Barr, R. & Pease, K. (1990), Crime Placement, Displacement, and Deflection", in: M. Tonry & N. Morris (eds), Crime and Justice: A Review of Research, 12(3), p. 12, University of Chicago Press, Chicago.

6 Levi, M. (1998), Organized Plastic Fraud: Enterprise Criminals and the Side-Stepping of Fraud Prevention, The Howard Journal, 37(4), p.423.

7 Kundi, Ghulam Muhammad, Nawaz, Allah, Akhtar, Robina (2014), Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries, Journal of Information Engineering and Applications, Vol.4, No.4, p. 61.

8 Broadhurst, Roderic (2006), Developments in the Global Law Enforcement of Cyber-crime, Policing: An International Journal of Police Strategies and Management 29(2), p.2.

the illegal use of computer systems date back to the published press and scientific literature of the 1960s.[9] However, the first major instance of cybercrime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide.[10] The term Cyberspace was first used by William Gibson in his 1984 novel "Neuromancer", which is now used to describe the entire spectrum of computer networks and associated activities that take place over computers and their interconnected networks which is their largest manifestation form the internet.[11] So it is the virtual place without jurisdictional boundaries in which people interacts through network of hundreds of thousands if not millions of computers and users at the same time, thus, this cyberspace paved ways for cybercrimes.[12] There is no universal definition of cybercrime. It is understood with reference to its different occurrences. Cybercrime involves activities in which computers and other technological devices are used for illicit purposes. Cybercriminals can cross international boundaries without the use of passports or official documentation. There is no question regarding the cyber wrongs being crime since it is recognized as crime under international law. The Budapest Convention on Cybercrime, 2001 describes as such.[13] There is an Additional Protocol to the Convention, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[14]

Computer Itself is Victim

The best-known type of crime involving computers as targets is hacking. Hacking involves breaking into a computer system. Hackers operate in virtually every country at a high economic cost to the global marketplace.

---

9 Goodman, Marc D. (2002), Brenner, Susan W., The Emerging Consensus on Criminal Conduct in Cyberspace**,** 10 Int'l J.L. & Info. Tech. 139, p. 31.

10 Message Labs Intelligence: 2010 Annual Security Report, Symantec, available at https://www.symantec.com/about/newsroom, last accessed on 12.02.15.

11 Jamil, Z. (2006), Cyber Law, Presented at the 50th Anniversary Celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, 2006, Jamil and Jamil Law Associates, Islamabad, Pakistan, available at: http:// jamilandjamil.com/wp- content/uploads/2010/11/article_for_scp_50_anniv_v5 .0.pdf, last accessed on 27.01.15.

12 Marvin, C. (1988), When Old Technologies were New: Thinking about Electric Communication in the Late Nineteenth Century, The Journal of Law and Lawyers, 4(1), p. 88.

13 Articles 2-10 provide different cybercrime.

14 The Convention was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of September 2015, 47 states have ratified the convention, while a further seven states had signed the convention but not ratified it. On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia.

Computer viruses can destroy thousands of computers within short time. Cyber terrorism is engaging in unlawful attacks or threats of attack against computer networks and the information contained within them to intimidate or coerce a government or its people to further a political objective. Cyberstalking is gaining online access to information about a target for the purpose of intimidation or physical harm. Cyberstalking can result in assault, kidnapping, or murder. Web-page 'jacking' is an effective way to steal a customer's identification.[15] Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. There are many other crimes in which computer itself is target and victim.

Use of Computer to Commit Crime

In addition to being targets of crime, computers are used as a means to commit traditional forms of crime such as theft, fraud, terrorism, phony stock trading, stalking, and sex offenses. In these cases, the computer is simply a hi-tech tool to commit a traditional type of crime. Criminal offenses in all categories can be committed through the use of the computer. The computer can be used as a tool to commit theft through sophisticated Internet scams. A wide range of Internet fraud scams include phishing. Cybercrimes are in numerous forms. Those vary in different legal systems. The list of cybercrimes cannot be circumscribed.

Implications of Cybercrime

As never before and at little cost a single offender can inflict catastrophic loss or damage on individuals, companies, and governments from the other side of the world.[16] There are national, economic, social and individual aspects of the implications of cybercrime.

Economic Loss

Financial loss caused by the cybercrimes is too great. Some are reported and some are not which is even greater. A report of Reuters on 2014-06-09 says Cyber crime costs global economy $445 billion a year.[17] Although it is difficult to quantify the total costs, evidence from operational agencies suggests that economic costs of cybercrime are substantial.[18] The cost of

[15] Supra note 8, p. 4. Too often one category of crime can target the computer itself as well as may cause effects of ordinary crimes in which case it is said that computer is both target and tool of crime.

[16] Ibid.

[17] See http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609, last accessed on 12.02.15.

[18] National Plan to Combat Cybercrime, Australian Government, Business and Information Law Branch, Attorney-General's Department, Commonwealth of Australia 2013, p.4, available at https://www.ag.gov.au/CrimeAndCorruption/

cybercrime in Australia, for example, is as high as $2 billion annually.[19] The costs to maintain, protect and restore cyber infrastructure have increased rapidly.[20] In the UK, the annual cost resulting from cybercrime is estimated at GBP27 billion (US$43 billion).[21] The Indian film 'Jai Ho' suffered losses from piracy, as a pirated print of the film was uploaded on YouTube by a Dubai-based user on January 28, 2014. A better print of the film was uploaded on February 2.[22] IP theft costs US organizations nearly US$200–250 billion annually, according to estimates from the US Commerce Department.[23] Moreover, the cost of combating cybercrime is enormous.

National Security Threat

Cybercrimes may threaten a nation's security. Stuxnet worm was launched with the intention of damaging utilities companies and nuclear facilities in Iran and other countries. The program reportedly destroyed a fifth of Iran's nuclear centrifuges.[24] Estonia and Georgia witnessed the Web War I. In 2009, computer hackers broke into the Pentagon's US$300 billion Joint Strike Fighter project, F-35 Lightning II. As hackers carefully encrypted the stolen data, investigators were unable to determine the amount or nature of the lost data.[25] In 2008, the US military's classified computer network was hacked by an unidentified intelligence agency, which inserted a malicious code into the system through a flash drive.[26] In June 2007, the Pentagon was forced to disable up to 1,500 computers, as hackers breached an email system at the Office of the Secretary of Defence.[27] Canada has also been a

---

Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, last accessed on 11.02.15.

19 Ibid.

20 The Cost of Cybercrime, Detica, February 2011, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf, last accessed on 12.02.15.

21 Ibid.

22 Jai Ho Online Leak: Business Worth Rs 10-12 crore hit?, Hindustan Times, available at https://en.wikipedia.org/wiki/Jai_Ho_%28film%29#cite_note-24, last accessed on 18.1.16.

23 Computer Crime & Intellectual Property Section, Department of Justice, The United States, available at http://www.justice.gov/criminal-ccips, last accessed on 12.02.15.

24 Broad, William J., Markoff, John and Sanger, David E. , Israeli Test on Worm Called Crucial in Iran Nuclear Delay, NYTimes, January 15, 2011, available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0, last accessed on 12.02.15.

25 Gorman, Siobhan, Cole, August and Dreazen, Yochi, Computer Spies Breach Fighter-Jet Project, WSJ, April 21, 2009, available at http://www.wsj.com/articles/SB124027491029837401, last accessed on 12.02.15.

26 Pentagon Official Says Flash Drive Used in Classified Cyberattack, AoL News, August 25, 2010.

27 Pentagon Target of Cyber Attack, Betanews, June 21, 2007.

victim of a cyber attack.[28] Director, Centre for Strategic and International Studies, Jim Lewis observed "Cyber-espionage is the biggest intelligence disaster since the loss of the nuclear secrets (in the late 1940s)."[29]

Combating Cybercrime: A National, Regional and Trans-National Agenda

There have been numerous attempts nationally, regionally and internationally up to now to address the issue of cybercrime with a view to prevent it. But the prospect of the developed and developing countries in this regard does not warrant an equal picture. Many countries have enacted national legislation relating to cybercrime. However, there is no international convention regarding cybercrime up to now. The Council of Europe, the European Union, the United Nations and Interpol have played leading and important roles in building international awareness and cooperation in combating cybercrimes.[30] The Council of Europe Convention, popularly known as the Budapest Convention, is the first multilateral treaty on cybercrime. Efforts of G8 to combat cybercrime have been maintained on a row. It concluded that there must be no safe havens for those who abuse information technologies. Many UN general assembly resolutions have addressed the issue of cybercrime and adopted measures to prevent and control it. Interpol helps the national authorities in operations against the cybercrimes in many places with technical and operational assistance.[31] However, the responses of the Interpol are disproportionate to the extent of the crimes committed.[32] It has been seen that developed nations provide funds to fight cybercrime. Different countries, both developed and developing, have taken numerous initiatives to prevent cybercrime. In efforts to combat it, government spending on cyber security has increased significantly.[33]

In Bangladesh, cybercrime was addressed for the first time by The Information and Communication Technology Act, 2006. This Act established special Court namely Cyber Tribunal to try and punish the cyberoffenders. The law provides for extra territorial jurisdiction in section

---

[28] Austen, Ian, Canada Hit by Cyberattack, NYTimes, February 17, 2011, available at http://www.nytimes.com/2011/02/18/world/americas/18canada.html, last accessed on 12.06.15.

[29] War in the Fifth Domain, Cyberwar, Are the Mouse and Keyboard the New Weapons of Conflict?, Economist, July 1, 2010, available at http://www.economist.com/node/16478792, last accessed on 12.02.15.

[30] Supra note 9, pp. 36-37.

[31] Interpol, available at http://www.interpol.int/About-INTERPOL/Vision-and-mission, last accessed on 18.01.2015.

[32] Levi, M. and D. Wall, 2004, 'Technologies, Security, and Privacy in the Post –9/11 European Information Society', Journal of Law and Society, 31, p.194.

[33] Supra note 2, p.6.

4 for offences committed outside Bangladesh targeting computers within Bangladesh. It also provides for different cyberoffences like hacking, spreading viruses, changing the computer source codes etc. and the penalties for committing such offences in sections 54, 55, 56. However, the law does not provide for the admissibility of the digital evidence which is a setback for trying the offenders. Moreover, the investigators and the tribunal follow the code of criminal procedure in investigation and trial of the offender which make the proceedings lengthy.

Challenges in Combating Cybercrime

Cybercrime presents the nations of the world with a problem they have never before had to address, i.e., the permeability of national borders.[34] Europol says cybercrime presents a major challenge for law enforcement.[35] Such challenges are of different dimensions. There are legal and technical challenges in combating cybercrime. The nature of the crime itself poses some unique challenges which are not available in ordinary crimes. The biggest challenge of cybercrime is that it can be committed from any place of the world targeting any computer of the world. The cyberspace is generally wide open for everybody which facilitates the offenders to infiltrate into the network. However, if it is done from a distant place apprehension of the offenders is a great difficulty. Here in this chapter it is discussed the challenges in combating cybercrime.

Legal Challenges

There is either absence or inadequacy of cyber legislation; the laws are ambiguous in many places. It is difficult to define the cybercrimes clearly and comprehensively. In many cases, no exemplary punishment is awarded. The enormous growth of cybercrimes due to its intrinsic features is itself a challenge for the justice system. It turns the combat into a tougher one. It is difficult to trace the cybercriminals. They are anonymous phantoms. Due to the technicality of the crime proper legal interpretation and application of the existing law in a given situation is a difficulty. Incapacity of the investigating authorities and the prosecutors in terms of technical knowledge, skill and instruments has made the cybercriminals persistent. Many legal challenges faced by police and prosecutors in pursuit of cybercriminals can be illustrated by the brief yet destructive career of the "Love Bug" virus.[36] However, the culprit could not be tried since there was no law as such in Phillipines. Before the forces get to the offenders, potential evidences were destroyed. However, he was arrested but

[34] Supra note 9, p. 89.
[35] See,https://www.europol.europa.eu/content/press/cybercrime-presents-major challenge-law-enforcement-523, last accessed on 12.02.15.
[36] Supra note 9, p. 4.

discharged finally. As extradition treaties with the affected countries require double criminality he could not be extradited for prosecution as well. Therefore, "Love Bug" havoc ended up with no legal consequences for these loopholes despite having caused billions of dollars in damage to thousands of victims in numerous nations.[37] Traditional procedural law is not instrumental in combating cybercrime as it entertains the tangible evidence only. Therefore modernization of both the substantive and procedural laws is essential. Moreover, as multiple jurisdictions may be involved in cybercrime it is difficult to determine the place where the offence was committed and which law should apply. There are associated problems of finding evidence since it can be more easily hidden, changed or destroyed and presenting the evidence as well.[38]

Technical Challenges

Forensic specialists tasked with investigating computer-related crime face new challenges. The greater use of encryption and access protection also poses a growing challenge of extracting evidence from computers, and servers.[39] Online, criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Law enforcement and the courts face investigative and legal challenges unique to cybercrime—in particular, the investigative challenge of locating an offender who is not physically present at the crime scene.[40]

Digital evidence is fragile therefore its preservation is a difficulty. The rapid transfer of data leaves little time for law-enforcement agencies to investigate or collect evidence. Traditional investigations take much longer period.[41] The expansion of wireless internet access in developing countries is an opportunity as well as a challenge for law-enforcement agencies. If offenders use wireless access points that do not require registration, it is more challenging for law enforcement agencies to trace offenders, as investigations lead only to access points. Cybercriminals do anonymous communications. Determining the origin of communication is very often a key component of cybercrime investigation. However, the distributed nature of the network, as well the availability of certain Internet services, which create uncertainty of origin, make it difficult to identify offenders.

---

[37] Ibid, pp. 6-7.
[38] Supra note 3.
[39] Supra note 8, p. 5.
[40] Helfgott, J. B. (2008), The Influence of Technology, Media, and Popular Culture on Criminal Behavior, Copycat Crime and Cybercrime, in Criminal Behaviour: Theories, Typologies and Criminal Justice, Thousand Oaks, CA: SAGE Publications, p. 376.
[41] Gercke, Marco (2006), The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, No.5, p. 142.

General Challenges

Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow.[42] Because of a lack of consensus as to definitions of cybercrime police cannot keep accurate track of it.[43] Moreover, combating cybercrime is expensive. With the growing number of people connected to the internet, the number of targets and offenders increases. The increasing number of internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. The more advanced technologies are coming bringing more cyber risks. New developments of computer and internet related technology brings new dimension and speed of crimes harder to prevent. Use of pirated software is a major challenge for the state agencies. Rob Wainwright, Director of Europol, observed, identifying and tracking the origin of cybercrime is not only complex but sometime impossible due to its borderless nature, which is one of the great challenges for the developing world, who are already technology deficient.[44] Ronald Noble, Former Secretary General of Interpol, observed,

"An effective cyber-attack does not require an army; it needs just one individual. However, there is a severe shortage of skills and expertise to fight this type of crime; not only at Interpol, but in law enforcement everywhere".[45]

Major Findings of the Research

Combating cybercrime has been and will be an uneven journey. Due to the transnational nature of cybercrime it is not possible for a state to fight the cybercriminals alone. The major findings of the research are given below.

- International agreement and cooperation are essential due to the worldwide nature of the internet. Mutual assistance and information sharing in investigation of cybercrimes are critically important.

---

[42] Cyber Crime and Punishment? Archaic Laws Threaten Global Information, Mcconnell International (December 2000), available at: http://www.mcconnellinternational.com/services/cybercrime.htm, last accessed on 13.01.15.

[43] See, e.g., Goodman, Marc D., Making Computer Crime Count, FBI Law Enforcement Bulletin (July 2001), available at https://leb.fbi.gov/2001-pdfs/leb-august-2001, last accessed on 13.02.15.

[44] Council of Europe (2003), Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of A Racist and Xenophobic Nature Committed Through Computer Systems (ETS 189), available at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, last accessed on 13.02.15.

[45] Grabosky, P.N., & Smith, R.G. (1998), Crime in the digital Age: Controlling telecommunications and cyberspace illegalities, Federation Press, Sydney/Transaction publishers, New Brunswick, p.220, available at http://trove.nla.gov.au/version/46410671, last accessed on 13.02.15.

- Special national law is to be enacted to prevent cybercrime and it has to be updated time to time. The law must clearly define and categorize cybercrimes. There should be more research in this field.
- Digital evidence should be admissible. In order for cybercrime offences to be prosecuted effectively, prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence.
- Special training and skill of the members of the law enforcing agencies are required. Separate specialized department should be established to investigate cybercrimes.
- National sovereignty should not be hindrance in the investigation of cybercrimes by an international or regional agency.
- Cooperation between the government and private sectors are essential. Network owners or internet-service providers can take more responsibility to help identify cyber attacks and attackers on user computers, and take the necessary steps to counter such attacks.
- Preventive measures like cyber security strategies are more appropriate than the measures taken after the occurrence.
- Strong political will is required to combat cybercrime both nationally and internationally.
- Harmonization of law and cross border coordination is essential to fight cybercrime. National law can greatly benefit from the experience of other countries and international expert legal advice. Countries must work together to devise a set of core consensus crimes that can be used to pursue cybercriminals wherever they may operate.
- New technologies are to be developed in a way that will facilitate law enforcement action against cyber-criminals.

Concluding Remarks

Individual awareness can be effective in preventing cyber attacks but only to a certain extent. Without cross-border response in combating cybercrime the threat remains ever growing. The fight against cybercrime either is a global one or it makes no sense.[46] Cyber attacks become more widespread with the advancement of technologies like automation. It requires a long term, sustained response from the governments. Developed countries are far ahead in combating cybercrime than the developing countries. The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is crucial.[47]

[46] Esposito, G. 2004, The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument? In Broadhurst, R. (ed), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, p. 34.

[47] Supra note 8, p. 6.

Governments and industry need to be proactive in anticipating where new threats might emerge.[48] Internet service providers have major role to play in combating cybercrime. Some countries use filter technology to restrict access to websites that address political topics. Expedited preservation and disclosure of stored computer data (Quick freeze procedure) is required. The identification of an offender who has committed a cybercrime often requires the analysis of traffic data. The IP address, in particular, can help law-enforcement agencies to trace the offender.[49] Time is therefore a critical aspect of Internet investigations. A data-retention obligation forces the provider of Internet services to save traffic data for a certain period of time. The implementation of a data retention obligation is an approach to avoid the abovementioned difficulties of gaining access to traffic data before they are deleted. An example for such an approach is the European Union Directive on Data Retention.[50] Exchange of intelligence among law-enforcement agencies in different countries is needed. If neither a multilateral nor a bilateral agreement is applicable, international cooperation generally needs to be founded on international courtesy, based on reciprocity. This remains the key thing in the combat against cybercrime in which all the nations are needed to work together to eliminate this globalized threat.

References:

Austen, Ian, Canada Hit by Cyberattack, NYTimes, February 17, 2011, available at http://www.nytimes.com/2011/02/18/world/americas/18canada.html,last accessed on 12.06.15.

Barr, R. & Pease, K. (1990), Crime Placement, Displacement, and Deflection, in: M. Tonry & N. Morris (eds), Crime and Justice: A Review of Research, 12(3), University of Chicago Press, Chicago.

Broadhurst, Roderic (2006), Developments in the global Law Enforcement of Cyber-crime, Policing: An International Journal of Police Strategies and Management 29(2).

Broad, William J., Markoff, John and Sanger, David E. , Israeli Test on Worm Called Crucial in Iran Nuclear Delay, NYTimes, January 15, 2011, available at

[48] Supra note 18, p. 7.

[49] Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, September 2012, Telecommunication Development Sector, p.246, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, last accessed on 27.01.15.

[50] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0, last accessed on 12.02.15.

Computer Crime & Intellectual Property Section, Department of Justice, The United States, available at http://www.justice.gov/criminal-ccips, last accessed on 12.02.15.

Craig J. Balkeley, Combating Cybercrime: the Legal (&Practical) Challenges, Alliance Law Group, available at http://www.alliancelawgroup.com/cybercrime.pdf, last accessed on 27.01.2015.

Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information, Mcconnell International (December 2000), available at: http://www.mcconnellinternational.com/services/cybercrime.htm, last accessed on 13.01.15.

Esposito, G. 2004, The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument? in Broadhurst, R. (ed), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong.

Gercke, Marco (2006), The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, No.5.

Gercke, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, September 2012, Telecommunication Development Sector, p.246, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, last accessed on 27.01.15.

Goodman, Marc D. (2002), Brenner, Susan W., The Emerging Consensus on Criminal Conduct in Cyberspace**,** 10 Int'l J.L. & Info. Tech. 139.

Gorman, Siobhan, Cole, August and Dreazen, Yochi, Computer Spies Breach Fighter-Jet Project, WSJ, April 21, 2009, available at http://www.wsj.com/articles/ SB124027491029837401, last accessed on 12.02.15.

Grabosky, P.N., & Smith, R.G. (1998), Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Federation Press, Sydney/Transaction publishers, New Brunswick, p.220, available at http://trove.nla.gov.au/version/46410671, last accessed on 13.02.15.

Gros, J. 2003, Trouble in Paradise: Crime and Collapsed States in the Age of Globalization, British Journal of Criminology, 43.

Helfgott, J. B. (2008), The Influence of Technology, Media, and Popular Culture on Criminal Behavior, Copycat Crime and Cybercrime, in Criminal Behaviour: Theories, Typologies and Criminal Justice, Thousand Oaks, CA: SAGE Publications.

https://www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law enforcement-523, last accessed on 12.02.15.

http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609, last accessed on 12.02.15.

Interpol, available at http://www.interpol.int/About-INTERPOL/Vision-and-mission, last accessed on 18.01.2015.

Issues Monitor**,** Cyber Crime – A Growing Challenge for Governments, July 2011, Volume Eight, KPMG INTERNATIONAL, available at https://www.kpmg.com/ Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf, last accessed on 11.02.15.

Jai Ho Online Leak: Business Worth Rs 10-12 Crore Hit?, Hindustan Times, available at https://en.wikipedia.org/wiki/Jai_Ho_%28film%29#cite_note-24, last accessed on 18.1.15.

Jamil, Z. (2006), Cyber Law, Presented at the 50th Anniversary Celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, 2006, Jamil and Jamil Law Associates, Islamabad, Pakistan, available at: http://jamilandjamil.com/wp content/uploads/2010/11/article_for_scp_50_anniv_ v5 .0.pdf, last accessed on 27.01.15.

Kundi, Ghulam Muhammad, Nawaz, Allah, Akhtar, Robina (2014), Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries, Journal of Information Engineering and Applications, Vol.4, No.4.

Levi, M. (1998), Organized Plastic Fraud: Enterprise Criminals and the Side-Stepping of Fraud Prevention, The Howard Journal, 37(4), p. 423.

Levi, M. and D. Wall, 2004, 'Technologies, Security, and Privacy in the Post –9/11 European Information Society', Journal of Law and Society, 31.

Marvin, C. (1988), When Old Technologies were New: Thinking about Electric Communication in the Late Nineteenth Century, The Journal of Law and Lawyers, 4(1).

Message Labs Intelligence: 2010 Annual Security Report, Symantec, available at https://www.symantec.com/about/newsroom, last accessed on 12.02.15.

National Plan to Combat Cybercrime, Australian Government, Business and Information Law Branch, Attorney-General's Department, Commonwealth of Australia 2013, available at https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National% 20Plan%20to%20Combat%20Cybercrime.pdf, last accessed on 11.02.15.

The Cost of Cybercrime, Detica, February 2011, available at https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf, last accessed on 12.02.15.

White, Aoife, EU Headquarters under Cyber Attack before EU Leaders' Meeting, Bloomberg, March 24, 2011, available at http://www.bloomberg.com/news/ articles/2011-03-24/eu-headquarters-under-cyber-attack-before-eu-leaders-meeting, last accessed on 12.02.15.

War in the Fifth Domain, Cyberwar, Are the mouse and keyboard the new weapons of conflict?, Economist, July 1, 2010, available at http://www.economist.com/node/ 16478792, last accessed on 12.02.15.