Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Review of International Legal Framework to Combat Cybercrime

Sandeep Mittal, IPS
Director
LNJN National Institute of Criminology & Forensic Science
Ministry of Home Affairs, New Delhi, India

Prof. Priyanka Sharma
Professor & Head
Information Technology & Telecommunication,
Raksha Shakti University, Ahmedabad, India

Abstract: Cyberspace is under perceived and real threat from various state and non-state actors. This scenario is further complicated by distinct characteristic of cyberspace, manifested in its anonymity in space and time, geographical indeterminacy and non-attribution of acts to a tangible source. The transnational dimension of cybercrime brings forth the issue of sovereignty, jurisdiction, trans-national investigation and extra territorial evidence necessitates international cooperation. This requires and international convention on cybercrime which is missing till date. Council of Europe Convention of Cybercrime is the lone instrument available. Though it is a regional instrument, non-members state like US, Australia, Canada, Israel, Japan etc. have also signed and ratified and remains the most important and acceptable international instruments in global fight to combat cybercrime. In this paper, authors have argued that Council of Europe Convention on Cybercrime should be the baseline for framing an International Convention on Cybercrime.

Keywords: Cybercrime, International Convention on Cybercrime, Cyber Law, Cyber Criminology, International Cooperation on Cybercrime, Internet Governance, Transnational Crimes.

I. INTRODUCTION

Information Societies have high dependency on the availability of information technology which is proportional to security of cyber space [1] [2]. The availability of information technology is under continuous real and perceived threat from various state and non-state actors [3]. The cyber-attack on availability of information technology sits on a thin line to be classified as cybercrime or cyber war having devastating effects in the physical world. The discovery of 'cyber-attack vectors' like Stuxnet, Duqu, Flame, Careto, Heart Bleed etc. in the recent past only demonstrates the vulnerability of the confidentiality, integrity and availability of information technology resources [4] [5]. The scenario is further complicated by the very nature of cyber space manifested in anonymity in space and time, rapidity of actions resulting in asymmetric results disproportionate to the resources deployed, non-attribution of actions and absence of international borders [6]. By virtue of these features, 'the transnational dimension of cybercrime offence arises where an element or substantial effect of the offence or where part of the modus operandi of the offence is in another territory', bringing forth the issues of 'sovereignty, jurisdiction, transnational investigations and extraterritorial evidence'; thus necessitating international cooperation [7]. In this essay, international efforts and their efficacy in combating cybercrimes would be analysed.

II. INTERNATIONAL LEGAL FRAMEWORKS

Although several bilateral and multilateral efforts have been attempted to combat cybercrime, the European Union remains at the forefront in creating a framework on cybercrime [8] [9] [10] [11]. Going beyond the European Union by inviting even non-member States, incorporating substantial criminal law provisions and procedural instruments, the Council of Europe Convention on Cybercrime (the Convention) [12] puts forth 'instruments to improve international cooperation' [13]. The Convention makes clear its belief 'that an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters' [14]. As on December 2016, 52 States have ratified the Convention and 4 States have signed but not ratified. As of July 2016, the non-member States of Council of Europe that have ratified the treaty are Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and US. The Convention is today the most important and acceptable international instrument in global fight to combat cybercrime [15] [16] [17] thereby limiting the scope of discussion to the Convention for the purpose of this essay.

The Convention seeks to harmonise the substantive criminal law by defining 'offences against the confidentiality, integrity and availability of computer data and systems' [18], 'computer related offences' [19], 'content related offences' [20], 'offences related to infringement of copyright and related rights'[21] and 'ancillary liability and sanctions' [22]. The convention also seek to harmonise the procedural law by providing scope, conditions and safeguards to procedures [23], expedited preservation of stored computer data, traffic data and partial disclosure of traffic data [24]; the search and seizure of stored computer data [25] and collection of real time data [26]. The jurisdiction over the offences established by the Convention is also sought to be harmonized [27]. However the strength of the Convention is the details in which general and specific principles relating to international co-operation including extradition and mutual assistance are enumerated [28]. To sum up, the Convention intends to provide 'a swift and efficient system of international cooperation, which duly takes into account the specific requirements of fight against cybercrime' [29]. However, a few scholars [30] have raised doubts about the effectiveness of the Convention, in improving the international co-operation thus enabling law enforcement agencies to fight cybercrime, and thereby terming it merely a symbolic instrument. The Convention 'is an important step in right direction' [31] and remains as 'the most significant treaty to address cybercrimes' [32].

III. EFFICACY, FUNCTIONING AND LIMITATION

A number of contentious legal and procedural issues generally arise while investigating cybercrimes involving transnational dimension, thus acting as impediment to the very process of investigation [33] [34] [35]. The cyber space has evolved exponentially since the Convention was drafted. The deployment of 'military-grade precision-vectors' and the advanced persistent threats (APTs) to attack infrastructure in virtual and real world are the order of the day. The internet of things has beginning to become botnet of things. The Nation-states also have realised that the cyber-space has almost become the fifth domain of war.[36] In view of this escalated scenario, while the formal channels like extradition and mutual assistance are delayed to the extent of killing the investigation, the informal requests between law enforcement agencies (LEAs) are viewed with suspicion.

The Convention only seeks to harmonize the domestic law but many nation-states have no cybercrime legislation. This combined with heterogeneity of skills, capacity, technology access and sub-culture of LEAs, cybercriminals and victims forms a 'vicious circle of cybercrime' [37]. The role of consent, having cognitive and cultural limitations, for accessing stored computer data in accordance with Article 32 of the Convention, is not well defined and therefore open to the interpretation of courts making this provision rather an instrument of international non-cooperation. Moreover, EU Primary Law viz., Charter of Fundamental Rights (CFR) of the European Union of 2000 [38], Treaty on European Union [39] and the jurisprudence of the CJEU [40], now recognise data protection as a fundamental right. The shield of human rights is very effectively used to prevent international co-operation. The domestic laws of some nation-states, e.g., Section 230, CDA [41] in US, have become judicial oak in hampering international co-operation in cybercrime investigations as it provides blanket immunity to search engines like Google.

The very nature of the internet-governance structure, tilted heavily toward private players, leaves very little in the hands of the States. The efforts for strengthening international co-operation to combat cybercrime, including the Convention, have miserably failed to tap this private element of the governance mainly due to conflict of private and public interests.

IV. CONCLUSION

As cyber space is rapidly evolving with the advent of new technologies, the cybercrime is assuming new dimensions in space and time impeding its investigation in ways never before contemplated. The law and the capacity building of LEAs are not able to keep pace with these new developments. While the cyber space has no borders for the cybercriminals, the law enforcement agencies would have to respect the sovereignty of other nations. The national disparities in 'law', 'legal systems' and 'capacity' to combat cybercrimes are so wide that the international co-operation remains the only hope to combat crime. The Convention on Cybercrime is, though symbolic, a great effort to identify issues and provide solution to the existing legal and procedural gaps in fighting cybercrime. As the laws were and would always remain inadequate for enforcement, it would only be a concerted effort to achieve international co-operation to make cybercrime a very high cost and high risk proposition. The UN has recently woken up to the situation [42] and would do well to take the Convention on Cybercrime as the baseline to frame an International Convention on Cybercrime.

V. REFERENCES

[1] M. Gercke, "Europe's legal approaches to cybercrime," in *ERA forum*, 2009, pp. 409-420.

[2] M. Gercke, "Understanding cybercrime: a guide for developing countries," *International Telecommunication Union (Draft)*, vol. 89, p. 93, 2011.

[3] D. L. Speer, "Redefining borders: The challenges of cybercrime," *Crime, law and social change*, vol. 34, pp. 259-273, 2000.

[4] S. Mittal, "Perspectives in Cyber Security, the future of cyber malware," *The Indian Journal of Criminology*, vol. 41, p. 18, 2013.

[5] S. Mittal, "The Issues in Cyber- Defense and Cyber Forensics of the SCADA Systems," *Indian Police Journal*, vol. 62, pp. 29- 41, 2015.

[6] S. Mittal, "A Strategic Road-map for Prevention of Drug Trafficking through Internet," *Indian Journal of Criminology and Criminalistics*, vol. 33, pp. 86- 95, 2012.

[7] O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.

[8] "COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime," ed, 2001.

[9] "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final - not published in the Official Journal]."

[10] "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems," vol. OJ L 69, 16.3.2005, p. 67–71, ed.

[11] *Council of Europe, Convention on Cybercrime, 23 November 2001, available at: http://www.refworld.org/docid/47fdfb202.html [accessed 26 February 2017]*.

[12] ibid.

[13] ibid.. Articles 23-35

[14] ibid. Preamble

[15] "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890 final - not published in the Official Journal]."

[16] O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.

[17] "United Nations, UN General Assembly Resolution 55/63: Combating the Criminal Misuse of Information Technologies (Jan. 22, 2001)," ed.

[18] *Council of Europe, Convention on Cybercrime, 23 November 2001, available at: http://www.refworld.org/docid/47fdfb202.html [accessed 26 February 2017]*.. Articles 2 - 6.

[19] ibid.. Articles 7, 8.

[20] ibid.. Article 9.
[21] ibid.. Article 10.
[22] ibid.. Articles 11, 13.
[23] ibid.. Articles 14, 15.
[24] ibid.. Articles 16, 17.
[25] ibid.. Article 19
[26] ibid.. Articles 20, 21.
[27] ibid.. Article 22.
[28] ibid.. Articles 23- 35.
[29] ibid.. Preamble
[30] N. E. Marion, "The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation," *International Journal of Cyber Criminology,* vol. 4, p. 699, 2010.
[31] I. Walden, "Harmonising computer crime laws in Europe," *European Journal of Crime, Criminal Law and Criminal Justice,* vol. 12, pp. 321-336, 2004.
[32] S.-J. Wang, "Measures of retaining digital evidence to prosecute computer-based cyber-crimes," *Computer Standards & Interfaces,* vol. 29, pp. 216-223, 2007.
[33] "United States v. Gorshkov," in *WL 1024026, U.S. Dist. LEXIS 26306 (W.D. Wash. 2001).* ed, 2001.
[34] R. Power and R. Foreword By-Farrow, *Tangled Web: Tales of digital crime from the shadows of cyberspace*: Macmillan Press Ltd., 2000.
[35] B.-J. Koops, "Police investigations in Internet open sources: Procedural-law issues," *Computer Law & Security Review,* vol. 29, pp. 654-665, 12// 2013.
[36] S. Mittal, "Perspectives in Cyber Security, the future of cyber malware," *The Indian Journal of Criminology,* vol. 41, p. 18, 2013.
[37] N. Kshetri, "The simple economics of cybercrimes," *IEEE Security & Privacy,* vol. 4, pp. 33-39, 2006.
[38] Article 8
[39] Article 6(1)
[40] Law Commission, "Reforming Bribery," 2008.
[41] "Communications Decency Act 1996," ed, 1996.
[42] O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.

