International Cooperation in Cyber Space to combat Cyber crime and terrorism

Manmohan Chaturvedi[1] , Aynur Unal[2],Preeti Aggarwal[3], Shilpa Bahl[4], Sapna Malik [5], ,

[1]mmchaturvedi@ansalunivesity.edu.in, [2]aynurunal@ansaluniversity.edu.in,
[3]preetaggarwal@gmail.com, [4]gerashilpa@gmail.com, [5]sapnadhankhar@gmail.com

Abstract

Cyber crime and terrorism is an international problem which does not respect national borders. Cyber criminals operate from relatively safe territories beyond the easy reach of the law enforcement agencies of the countries in which their victims reside. Collaboration between governments, intelligence agencies and law enforcement officers is critical to prosecuting cybercrime, and new organizations have been created to enable this. However, this co-operation seems to have run into roadblocks by the leak of large scale national level data snooping secrets by whistleblower Edward Snowden. The paper attempts to derive insights from ongoing initiatives reported in open source and recommend options available to charter the path for sustainable international cooperation in evolving secure cyber infrastructure.

Keywords: International Cooperation, Secure Cyber Infrastructure, Cyber crime, Cyber terrorism

I. INTRODUCTION

Digital infrastructure is the substrate of the modern society. The networked society would achieve the potential efficiency gains only if this infrastructure is reliable and secure. Most of the nations have initiated policy measures to achieve the security of the ICT infrastructure. However, without international cooperation, these national measures are inadequate against transnational cyber crime and its evolved variant cyber terrorism.

Regional partnerships may not provide adequate cyber security, since the cyber attacks can originate from non member countries. This paper attempts to view the evolution of cyber crime and terrorism with a historical perspective and describes the international response to contain the menace. The roadblocks to effective international cooperation and possible options available to the global community of nations are identified.

II. EVOLUTION OF CYBER CRIME AND TERRORISM

Since Sir Robert Peele established the world's first professional police force, London Metropolitan Police, in 1829, little has changed in the nature of the conventional crimes [1].Virtually all conventional crimes have shared the attribute of *locality*. The criminal and victim belong to same geographical location. However, the cyber domain now makes it possible to commit a crime from anywhere in the world and *locality* is not the most likely attribute. This new development has increased transnational criminal activities. While criminals have been quick to adopt new technologies, law enforcement has moved relatively slowly. There are a number of reasons, the primary one being limited funding and competing priorities [2].

The legal framework in terms of substantive and procedural law takes time to evolve and bigger challenge is harmonizing these national frameworks internationally. As the international travel has increased significantly during the last century the necessity for extradition of the criminals across national jurisdictions has evolved. Thus, even before cyber crime across national boundaries became a reality; it was common for traditional criminal cases to raise issues of jurisdiction.

Historically, a majority of the difficult jurisdictional problems had stemmed from a conflict of laws between two or more countries, namely, where a specific activity is considered legal by one country but held illegal in another nation. A second source of jurisdictional problems arise when either an accused is located in a country X (say) but the victim resides in a different nation (say Y); or the accused and victim

978-1-4799-4562-7/14/$31.00 ©2014 IEEE

belong to the same jurisdiction but the criminal evidence is found abroad [1].

Under extradition, one nation hands over an accused individual to stand trial for an offense in a different country. Extradition is generally governed by existing extradition treaties between the corresponding nations. In principle, for one government to deliver an accused to another government for prosecution, "dual criminality" must exist. That is, the suspect's offense must be viewed illegal in both jurisdictions. Otherwise, extradition cannot be granted. In the context of cyber crime, where the electronic evidence is very fragile and its timely collection crucial for successful prosecution, this challenge at international level can be overwhelming for the law enforcement agencies.

III. INTERNATIONAL EFFORT TO CONTAIN CYBER CRIME

The past two decades has witnessed a number of initiatives by international bodies like; the Organization for Economic Cooperation and Development (OECD), Council of Europe (COE), G-8, European Union, United Nations [3], and the Interpol, which recognized the inherent cross border reaches of cybercrime, the limitations of unilateral approaches, and the need for international harmony in legal, technical, and other areas [1] [4].

IV. CHALLENGES OF SECURITY IN CYBERSPACE

According to [5] the security issues raised by cyberspace pose special challenges to those wishing to bring it into a classic international security framework. These special features pertain to four aspects viz. actors, attribution, authority and activity.

Actors

A key challenge of cyberspace is that it is populated by both state and non-state actors. An additional problem is that these two categories of users are not readily identifiable. It is for the sovereign states to ensure that non-state actors within their jurisdiction respect the law, including international legal obligations that have been incorporated into national law. The cyber criminals or terrorists residing in a country A and targeting victims in another country B while insulated from direct action of law enforcement agencies of country B are still the responsibility of the country A in terms of any collaborative treaties signed between the two countries. To achieve effective implementation very close, proactive and flexible interaction between law enforcement agencies of the two signatories is essential. The matrix becomes more involved when the number of member states increases and the eco-system should evolve to bring in transparency amongst all stakeholders. This transparency precludes possible use of the cyber space by the state actors as reported by Snowden for intelligence collection and potential cyber operations by the armed forces. This is the possible dilemma of the states who would like to use the anonymity of cyber space in support of their larger strategic objectives.

Attribution

The verification tools of the International Monitoring System of the Comprehensive Test Ban Treaty Organization (CTBTO) were easily able to detect the nuclear tests by North Korea in 2006 and 2009 [5] and led to necessary international response. In cyberspace, however, a cyber attacker can hide himself readily, and even disguise his attack to appear to originate from a third party. The problem of attribution for a cyber-action is clearly one that will complicate any effort at security controls. Uncertainty about attribution will also constrain retaliatory action. The current level of research in reliable attribution is not adequate. The cyber crime treaties cannot be implemented unless trust exists between signatories that best efforts are being put to identify the criminals and therefore, transparency is first precondition for success.

Authority

The designation of a state agency that would lead the response to an international cyber-attack would depend on the nature of the attack. The vast majority of hostile cyber-activity originates with criminal elements, for which law enforcement agencies are normally responsible. A response to use of the Internet by terrorists might entail pooling resources from both the national security and law enforcement communities. The fact that hostile international cyber-activity is not exclusively or even predominantly a national security phenomenon adds a further complication to the development of internationally acceptable approaches for regulating or policing such activity. International collaborative initiative for countering cyber- crime; the 2001 Budapest Convention on Cybercrime by the Council of Europe has run into road blocks in absence of mutual trust and attempts to erect barriers to the operational procedures (remote log in to the suspected computer systems) considered crucial for timely collection of the evidence, which is in any case very fragile.

Activity

Hostile international cyber-activity, as already noted, can be perpetrated by state or non-state actors. Within state actors too, the military and intelligence arms of nation states operate under different norms. Intelligence agencies of all countries with means and capacity will keep tabs on adversaries and on activities they perceive as threats. No international agreement or legislation will change that. When such attempts to spy are exposed, as by Snowden, there will be a degree of furor and then it will be business-as-usual [6].

V. THE POSSIBLE OPTIONS

Necessity for a review of the cyber space use

Considering the above four special feature of cyber domain that seem to discourage international treaties to combat cyber crime and terrorism, we conclude that bilateral and multilateral trust and transparency amongst signatories is a precondition for success. All nations have to realize that dual use of cyber space for commercial and military use is fraught with unacceptable risks. If we look at the international treaties [5] for Nuclear Weapons, Chemical Weapons Convention, Biological and Toxin Weapons Convention, Outer Space Treaty of 1967 prohibiting the placement of weapons of mass destruction in outer space and the militarization of the Moon and other celestial bodies and more recently, the Ottawa and Oslo treaties banning anti-personnel landmines and cluster munitions respectively, as precedence, there is hope for international cooperation in cyber space. The efficiency gains provided by the cyber domain are very valuable for mankind and using them for mutual destruction would be a serious folly.

Once all nation states share this common perception, combating cyber crime and terror would not be an impossible mission. The *Budapest Convention* (Council of Europe (COE) convention on cyber crime-2001) was a good attempt to seek international cooperation to harmonize the law enforcement efforts of all nations against cyber crime. However, lack of trust and international political compulsions to use the cyber domain for projecting the state power have sabotaged this potential collective action against cyber crime. With the development of new technologies such as cloud computing, "smart" phones and social media, as well as the emergence of botnets and the expansion of encryption, the Budapest Convention requires updating [7] before being ratified by all nations.

We need to realize that the state actors particularly militaries and intelligence agencies would certainly be using the ICT networking technologies for achieving the efficiency gains in their core activities. It is important that their ICT networking infrastructure is protected from; non-state actors viz. criminals/ terrorists and competing state actors viz. militaries and intelligence agencies. Use of the commercial internet technologies for such segment is fraught with risk and therefore, there is a case to evolve hardened systems for such niche groups.

Role of deterrence in combating Cyber crime and terrorism

Deterrence theory can be applied to all cyber crimes including cyber terrorism [8] [9]. The impact of deterrence (deterrence effect) is positively correlated with the identification probability, and it also may be positively correlated with punishment level. Keeping the potential punishment severity unchanged, the deterrence effect will be determined by the identification probability. The identification probability depends upon the capability to track cyber terrorists [10]. Thus, to increase the impact of deterrence on cyber terrorism, the identification probability must be increased. An inability to track cyber terrorists would make it difficult for local and international jurisdictions to track the entire network of cyber terrorists as well as to prosecute them due to the lack of proof of identification of these cyber terrorists. The potential adoption of a new variant of Cyber Crime and Terrorism convention by all nations would provide the eco-system that may put the criminals and terrorists under pressure and increases the success probabilities of the international law enforcement agencies.

VI. CONCLUDING REMARKS

This paper has attempted to unveil the underlying reasons for the failure of the 2001Budapest convention. The attraction of the Cyber domain as the new high ground for projecting the nation's power, as nuclear weapons have been in the past, has prevented the nation states to see the logic of unrestricted international collaboration to combat Cyber crime and terrorism. We still have a window of opportunity before compulsions of geopolitics establishes cyber warfare as a doctrine of choice amongst nations. The peaceful use of cyber domain for the good of mankind offers unimagined opportunities as peaceful use of its precursors nuclear and space technologies are known to provide. The only difference with cyber domain is that its dual use for peace and war does not seem feasible. The common enemies for all nation states are cyber criminals and terrorists. The collaboration with adequate trust and unrestricted access to the law enforcement agencies across the national boundaries would certainly mitigate this transnational menace.

REFERENCES

[1] M. Goodman, "International Dimensions of Cybercrime" in S. Ghosh and E. Turrini (eds.), *Cybercrimes: A Multidisciplinary Analysis*, DOI 10.1007/978-3-642-13547-7 17,_c Springer-Verlag Berlin Heidelberg, 2010

[2] M. D. Goodman, "Why the police don't care about computer crime". *10 Harvard Journal Law & Technology, 465*, *468–469* , 1997

[3] United Nations , International review of criminal policy: United Nations manual

on the prevention and control of computer-related crime. *CNET.com*.,1994

[4] N. Choucri, S. Madnick and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives", *Information Technology for Development*, 2013, DOI: 10.1080/02681102.2013.836699

[5] P. Meyer, "CYBER-SECURITY THROUGH ARMS CONTROL", *The RUSI Journal*, 156:2, 22-27,2011 DOI:10.1080/03071847.2011.576471

[6] S. Saran, "Internet realpolitik" *ORF Cyber Monitor, Volume II, Issue 3, March 2014*

[7] R. Broadhurst and L.Y.C. Chang, "Cybercrime in Asia: Trends and Challenges", In J. Liu et al. (eds.), *Handbook of Asian Criminology*, DOI 10.1007/978-1-4614-5218-8_4,© Springer Science+Business Media New York 2013

[8] J. Ginges, "Deterring the terrorist: A psychological evaluation of different strategies for deterring terrorism", *Terrorism and Political Violence*, *9*(1), 170–185,1997

[9] M. P. C. Carns, "Reopening the deterrence debate: Thinking about a peaceful and prosperous tomorrow". *Small Wars & Insurgencies*,*11*(2), 7–16 , 2001

[10] J. Hua and S. Bapna, "How Can We Deter Cyber Terrorism?, *Information Security Journal: A Global Perspective, 21:2, 102-114,*2012 DOI: 10.1080/19393555.2011.647250

About Authors

Dr Manmohan Chaturvedi is a retired Air Commodore from Indian Air Force with PhD in Information Security domain from IIT Delhi. He has about 35 years of experience in managing technology for IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with operational and policy dimensions of Information and Communication Technology. He graduated from Delhi College of Engineering and completed post graduation from IIT Delhi. Currently he is a Professor at School of Engineering and Technology, Ansal University with research interests in vulnerability of evolving ICT infrastructure and protection of Critical Information Infrastructure.

Dr. Aynur Ünal's career combines unique entrepreneurial, industrial and academic experiences that span over 35 years. Educated at Stanford University (Ph.D. class of '73), she comes from a strong engineering design and manufacturing tradition. Currently she is the Dean of School of Engineering & Technology, Ansal University, Gurgaon, India.

Preeti Aggarwal holds M.Tech(IT) from GGSIPU, New Delhi, M.Sc(Informatics) and B.Sc(H) in Electronics from University of Delhi and is currently pursuing Ph.D. in the area of 'Information Security in cloud through Data Mining techniques' from Ansal University, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon. She is also a life time member of Computer Society of India.

Shilpa Bahl holds M.Tech in IT from UIET, Krukshetra university ,Kurukshetra and B.Tech in Electronics & communication From Kurukshetra university and is currently pursuing Ph.D. in Software testing and Information Security from Ansal university, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon, having Six years of teaching experience in Computer Science department.

Sapna Malik is a Ph.D. candidate at the School of Engineering and Technology, Ansal University, India. She holds M.Tech in IT from GGSIPU, New Delhi, India and B.Tech in CSE from Mayarishi Dayanand University, India. She is working as Assistant professor in department of Computer Science Engineering in Maharaja Surajmal Institute of technology, Delhi, India. Her research interest includes Cloud computing, Network Security and Virtualization.