ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

India-ASEAN Cooperation on Cyber Crime

Dr. Sukhdeep Singh
Assistant Professor,
Punjabi University Guru Kashi College,
DamdamaSahib (Bathinda)

Abstract *Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers (PCs).Cyber threats are causing increasingly serious risks to the economy as well as to national and international security. They are now widely accepted in the international community as a top-tier risk, if not the most pertinent risk, to national and international security. A number of international and regional organizations, bodies and fora are working on cyber security issues, albeit to largely varying extents. Inter alia these include the OECD, the OSCE, the EU, the Council of Europe, BRICS, the OAS, AU, APEC, the Shanghai Cooperation Organization, the G8/G20, the UN, the Internet Governance Forum, ASEAN, SAARC etc. This paper will discuss the India-ASEAN cooperation in Cyber Crime/Cyber Security fields.*

Keyword: *Cyber Crime, Cyber Security, ASEAN, Terrorism, Cooperation, ICT, Internet Security.*

INTRODUCTION

The internet nowadays also has created a new realm, cyberspace, and in the era of high-speed connection, many people labeled the cyberspace as a lawless and borderless world of which freedom is the main issue. Anyone supposed to be free tobe connected, search for anything they need from every source they find and transform their creation in digital form. Some people even go beyond and use the internet to get what they need in illegal ways. As Cyber Security become a global problem, the need to arrange a cooperation to overcome cybercrime threat is inevitable. Many countries started to realize the importance of having cooperation to tackle the growth of cybercrime.

Cyber space is largely an ungoverned space. The safety and security of an ordinary individual is at risk in cyber space. Highlighting the existence of states run mass surveillance programmes, Snowden revelations have brought home a tension between national security concerns on the one hand and the right to privacy of the individuals on the other. The impact on industry has also been significant as shown in greater focus on encryption technologies and reconsideration of the safety and security of cloud technologies. Instability in cyberspace can endanger global stability. The protection of critical networks from cyber attacks is therefore a key cyber assurance challenge.
The Association of South-East Asian Nations (ASEAN), considered one of the world's fastest growing regions, today resolved to significantly enhance cooperation with India in combating growing challenges of maritime security, terrorism, drug trafficking and cyber crime besides expanding trade ties. The United Nations General Assembly adopted the non-binding Resolution 68/167which emphasizes the protection of the rights to privacy against unlawful surveillance. The Resolution unequivocally states that the same rights that people have offline must also be protected online.

Tackling Cyber crime remains the most difficult issue in cyber security. Nearly 80 per cent of cyber incidents can be classified as cyber crime. Hundreds of billions of dollars are lost in business to cyber crime. The growth of the Dark Netin habited by cyber criminals escaping the normal search engines is a matter of great concern. Similarly, the use of cyber space, particularly the social media by terrorists for propaganda, recruitment, training, radicalization etc. is worrisome. The scope for the international and regional cooperation in tackling cyber crime and cyber terrorism is significant.

ASEAN's centrality in the regional architecture of the wider Asia Pacific region and its potential role as a neutral broker is significant in terms of international cyber security cooperation. In the context of U.S.-China relations and recent political focus on the impact of state and economic cyber espionage, a 2012 Council on Foreign Relations working paper's[1] references to ASEAN's history of working together with the United States and China and to how ASEAN is seen as a neutral broker by most major powers, is particularly important.

Regional cooperation efforts can stimulate progress, fueling collective security and the further enhancement of national cyber security measures no matter where a state is on the spectrum of ICT development. In fact, such disparity in ICT development can advantage countries with a less developed ICT infrastructure and less connected critical infrastructure. As less digitally developed countries become more connected, lessons may be

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

applied from other states' experiences in countering cyber related threats, best practice policies and measures may be implemented, and both security and data privacy by design may be incorporated from inception in the development of ICT and connected critical infrastructures.

ASEAN was formed in 1967 and its founding fathers had envisioned an organization which would include all the ten countries of Southeast Asia (SEA). It began with five Southeast Asian states (Indonesia, Malaysia, the Philippines, Singapore and Thailand); and others including the LMCV countries (Laos, Myanmar, Cambodia and Vietnam) joined later. An eleventh country, East Timor, is yet to be granted membership. The SEA countries are diverse and at varying stages of development- with Singapore at the forefront and Myanmar still a Least Developed Country (LDC). The emergence of India from a gloomy to a glowing position in the global arena, coupled with a number of virtues like enormous size, huge population, convenient geostrategic location, progressive military might, meteoric economic growth inspired various states including South-East Asian nations to devise collaborative ties with India.

The Look East Policy of India, framed by Mr. Narasimha Rao Government in the early nineties, is a substantial manifestation of India's focused foreign policy orientation towards South East Asia; an immensely resourceful and flourishing region. The economy of South East Asia is a virtually untapped market which is up for grabs by major regional economic entities such as India, China, Europe or the USA. India's compatibility with the South East Asian countries with regard to better regional cooperation lies in the fact of its abstinence from exhibiting hegemonistic ambitions, making it more benign towards South East Asia. The camaraderie between India and South-East Asia is clearly visible through the dynamic persuasion of India's Look-East Policy.

INDIA AND CYBER SECURITY

India is dealing with the challenges of cyber security in multiple ways. One of the most important areas has been the formulation of National Cyber Security Policy in May 2013 and conceptualization of a Cyber Security Architecture under which critical cyber security institutions will be constructed. The salient aspects of this architecture include:

- Operationalisation of a National Critical Information Infrastructure Protection Centre (NCIIPC).
- Establishment of Cyber Security Assurance and Certification Bodies for testing, evaluation and cyber security audit.
- Creation of a R&D fund for setting priorities for research, indigenization and human resource development.
- Public Private Partnership on cyber security.
- Capacity building and creation of 500,000 cyber security professionals.

India is now engaged in implementing some of the policy initiatives.[1]

INDIA-ASEAN COOPERATION IN CYBER SECURITY

It is in the above context that India and ASEAN should look for cooperation in cyber security. The two sides can:

- Enhance their dialogue on cyber security both at official and Track 2levels and harmonize their positions on the key issues of cyber security. It will be useful to be aware of each other's' points of view on issues of Internet governance, cyber warfare, cyber law etc.
- Both India and ASEAN countries have set up a number of institutions to strengthen cyber security. It would be useful if institutional level dialogues can be set up. For instance, the CERTS could cooperate with each other on technical issues pertaining to cyber security. Academic and research institutions would also benefit from cooperation with each other.
- Another area of cooperation could be tackling cyber crime and cyber terrorism. Here the law enforcement agencies of the two sides could cooperate in real time. There is need to enhance understanding of how terrorists use social media and other cyber resources for terrorism purposes.
- India and ASEAN could also synergies their strengths in software and hardware to produce secure and safe ICT products and services. This will be a win-win situation for both.
- Finally, there is a huge scope for cooperation in capacity building and skill development. Indian government's cyber policy envisages producing cyber security professionals in large numbers. The engineering and technical courses are being reoriented to focus on cyber security. India and ASEAN can cooperate in capacity building in cyber field.[2]

The ASEAN are also keen on expanding cooperation in host of other areas such as maritime security and dealing with illicit drug trafficking and cyber crime. Like other regional blocs however, ASEAN faces obstacles of its own. Frequently cited limitations include structural and organizational limitations, a small staff at the Secretariat, decision-making by consensus, disparity in development among Member States, divisions within Member States, an aversion to intervening in the affairs of other Member States, and little capability in handling

978-93-85670-72-5 © 2016 (RTCSIT)

traditional or non-traditional security challenges, and little capacity has developed to combat drug-trafficking, human trafficking, terrorism and other high priority non-traditional security threats.[3] The aforementioned CFR Working Paper[4] outlines how, until now, ASEAN has been more successful in promoting trade integration and creating regional forums for discussing security issues than it has been in promoting more concrete security or economic integration.

ASEAN is one of the world's fastest growing regions and both sides are likely to seek greater economic engagement besides expanding cooperation in areas such as maritime security including freedom of navigation, drug trafficking and cyber crime. ASEAN is India's fourth largest trading partner and India is the sixth largest trading partner for the ten member grouping. Between April 2007 and March 2015, India invested USD 38.6 billion in ASEAN, while the ASEAN invested USD 32.4 billion in India. Apart from the 10-ASEAN Member states, East Asia Summit members include India, China, Japan, South Korea, Australia, New Zealand, the US and Russia.
In dealing with cyber threats, some of the most significant global challenges of common interest to ASEAN Member States include:

- The increasing volume and complexity of threats.
- The dilemma of accurate attribution.
- An increasing number of state and non-state actors.
- The lack of harmonised definitions and understanding of "cyber" terminology etc.

ASEAN's vision to build the ICT sector is to create a technologically advance and well-connected region. But ASEAN's development on ICT is lacking in incorporating the security aspect. Knowing the important yet fragile system of ICT, ASEAN needs to be ready to face cyber threat that might occur. So far, nine out often ASEAN member countries have Computer Emergency Response Team (CERT), the only country remained is Laos who has not establish their CERT. CERTs of the nine countries also are members of Asia Pacific Computer Emergency Response Team (APCERT), a regional organization consist of 29 teams of CERT (21 teams are full member and 8 teams are general member) from 22 Asia Pacific Countries. The existence of CERT team is vital to be "cyber police" to secure the national cyberspace, and the cooperation among them is needed to build a network to fight cybercrime.

ASEAN should further strengthen its relations with ASEAN dialogue partners and the international community by cooperating to tackle cross-border cyber challenges. It should also consider engaging other regional bodies and possibly establish joint working groups with the European Union and the East Asia Summit. In the future, ASEAN member states should agree a common position on shared norms for responsible state behavior in cyberspace and the applicability of international law for the use of advanced cyber capabilities and techniques.

CONCLUSION

Cooperation among those teams is also necessary because cybercrime is a contemporary threat to security which runs on a borderless cyberspace. But to enhance the level of cooperation, a more powerful form of formal agreement have to be conducted so ASEAN member countries will have the same interpretation on defining cyber crime and ensuring their steps on overcoming the problem is organized in the suitable framework. The agreement also have to cover the borderless nature of cybercrime, enables ASEAN member countries to investigate cybercrime case in neighboring countries in the region and processed the case according to regional agreement. India-ASEAN has greater cooperation between the member countries of the grouping and India in combating transnational and non-traditional security challenges and specifically sought better coordination to deal with combating terrorism, illicit drug trafficking, human trafficking and cyber crime.

REFERENCES

[1] Joshua Kurlantzick, "Council on Foreign Relations", *ASEAN's Future and Asian Integration, International Institutions and Global Governance Program*, November 2012.pp7-9.
[2] Dr. Arvind Gupta,"Indian ASEAN Dialogue on Cyber Security", *NSA*, New Delhi, 2015, pp.3-7.
[3] \Joshua Kurlantzick, *op.cit*.p.11.
[4] Khanisa,"A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation", *Journal of ASEAN Studies*, Vol.1, No.1 (2013), pp. 41–53.

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India