Combating Cybercrime

Major General Ashish Ranjan Prasad, VSM@

Introduction

The growth of internet has been the biggest social and technological change of our lifetime. It is a great medium that allows people across the world to communicate and has become increasingly central to our economy and society. But the growing role of Cyberspace has also opened up new threats from Cyber criminals along with new opportunities. The high degree of anonymity, speed of communication, efficiency and reach to the masses has led to it being exploited by Cybercriminals. Therefore we should have a clear cut approach towards handling of Cybercrimes at national level both at organisational and individual levels. The Government should be in a position to ensure protection of the organisations and individuals from crime, fraud and identity theft etc.

Categories of Cybercrimes

Criminals from all corners of the globe are already exploiting the Internet to target individuals and organisations. Few main categories of Cybercrimes can be described as below :- [1]

(a) **Breaking into Communication Services.** Unauthorised access of information services compromises security.

(b) **Promoting Criminal Activities.** Cyber domain is being used extensively to facilitate organised drug trafficking, gambling, money laundering and arms smuggling. The use of encryption technology places criminal communications beyond the reach of law enforcement.

(c) **Cyber Piracy.** The temptation to reproduce copyrighted material for personal use, sale or free distribution violate anti-piracy laws and are treated as criminal offences.

@**Major General Ashish Ranjan Prasad, VSM** was commissioned into the Corps of Signals on 13 Jun 1981. He commanded 14 Corps Operating Signal Regiment and 2 Signal Group (Electronic Warfare). Presently, he is posted as the Additional Director General Signal Intelligence at the Integrated HQ of MoD (Army).

Journal of the United Service Institution of India, Vol. CXLVI, No. 603, January-March 2016.

(d) **Cyber-Stalking.** Computer systems can also be used for harassing, threatening or intrusive communications, by means of "cyber-stalking".

(e) **Financial Irregularities and Tax Frauds.** Hi-tech online transactions over secured channels cannot be tracked with traditional countermeasures.

(f) **Electronic Vindictiveness and Extortion.** Dependence on complex data processing and telecommunications systems is prone to damage or interference by electronic intruders.

(g) **Investment and Marketing Frauds.** The increasing use of internet marketing and investment allow fraudsters to enjoy direct access to millions of prospective victims around the world, instantaneously.

(h) **Electronic Eavesdropping.** Remote monitoring of computer radiation and eavesdropping compromises information security.

(i) **Electronic Funds Transfer Fraud.** Digital information stored in credit card can be counterfeited and misused.

(j) **Identity Theft.** Identity theft is used by Cybercriminals for monetary gains and serves as a gateway to other Cybercrimes such as tax-refund fraud, credit-card fraud, loan fraud and other similar crimes.

(k) **Theft of Sensitive Data.** Sensitive information related to government, organisations or individuals attract the attention of Cybercriminals.

Cybercrime – Impact on National Security

Use of Cyberspace in civil as well as military domains has today become an intricate component of national power. With defence forces adopting more complex Information and Communication systems and upgrading to network centric warfare, they are at higher risks of cyber-attacks. The *"Make in India", "Digital India"* and *"Smart Cities"* are flagship programmes with a vision to transform India into a digitally empowered society, foster innovation, knowledge economy and infrastructure development in India by leveraging the use of information technology. It goes without saying that this accelerated capacity building has enormous implications

for the Country's cyber-security posture. At the same time, threats from both state and non-state actors are weakening the very foundations of these concepts. None of the existing international laws on cyberspace apply to the terrorist organisations who have adapted themselves in innovative ways to become one of the most ardent users of cyberspace for a variety of criminal activities - from communication, to finance, as well as for recruitment, networking and psychological operations (Psy Ops) as we are currently witnessing. As the visual and real worlds get increasingly integrated with the Internet of Things (IoT), it is only inevitable that use of cyberspace for destructive purposes will pose a serious threat to national security.

Challenges in Handling Cybercrimes

The human society around the world is racing ahead with innovative trends in information technologies. This has also given rise to well managed criminal activities where the commodity, personal information or data moves far too quickly for conventional law enforcement methods to keep pace. Detecting, quantifying and preventing Cybercrime is a difficult task. A few challenges are as under:-

(a) The Cyberspace is not limited by well-defined boundaries and hence the actions in the Cyber domain cannot be traced to the source of origin. These features are being exploited by non-state actors for perpetration of misdemeanors in the Cyber domain.[2]

(b) The reach and complexity of the offences committed in the Cyber domain are continually on the rise thereby affecting the Government as well as the institutions and individuals.

(c) As the volume and value of information hoisted in the electronic domain have increased, innovative methods are being adopted by Cyber criminals as more convenient and profitable ways of carrying out their activities anonymously are being evolved.

(d) The ability of adversaries to produce, distribute and utilise malicious code with ease maximises their gains and at the same time pose challenge to threat evaluation and traceability.

(e) Targeted attacks are growing faster, stealthier, multifaceted and extremely difficult to analyse and are causing risk to national security.

Current Scenario at National Level

With the increase in frequency of Cybercrimes in India and registration of Cybercrimes showing an annual quantum jump over the past years, an expert group set up by the Home Ministry has suggested setting up of a dedicated body which is proposed to be called Indian Cybercrime Coordination Centre (I4C). This will facilitate online reporting of Cyber offences, apart from monitoring, analysing and countering these new-age crimes. This national body will have linkages with state police and will e-integrate around 15,000 police stations across the Country, and NatGrid. This dedicated body will have high-quality technical experts and R&D experts to develop cyber investigation tools to coordinate the aforesaid actions. Also, the body can take up long-term training programmes for the law enforcement agencies and even judiciary on investigation and prosecution of Cybercrimes.

The proposed I4C will have real-time analytics of Cybercrime along with their types. This will help strengthen India's case in seeking cooperation from global Internet firms having servers abroad, to tackle various types of Cybercrimes. Also the planned architecture should have routing of the Internet services through a single, common gateway rather than separate gateways now used by the Country's Internet service providers. There is also need to have a relook at the legal framework, including the Indian Evidence Act, 1872 and Information Technology Act, 2008 against any existing loopholes or voids to deal with Cybercrime.

In view of emerging challenges in the Cyber world and spiralling Internet crime rate, State governments also need to take stern measures. There is a need to create nodal centre for effective policing of social networking sites and anti-terror activities in Cyberspace. All types of Internet related activities ranging from virtual policing, automated threat intelligence, Cyber forensics and tracking system need to be put in place.

There is a need for security compliance and a legal system for effective dealing with internal and external Cyber security threats. India needs good coordination between law and technology to come

out with a mechanism of cooperation among states, agencies and countries to address these challenges. The strategy and roll-out plans are needed for addressing the challenges related to Cybercrime in the short-term and the mid-term, with a mechanism to review the same on a long-term basis. In addition to the existing mechanisms, a strategy needs to be promulgated which states the vision, objective and approach for Cybercrime prevention in India. For this purpose, the Indian Government has set up its own 'Cyber Security Architecture' comprising following bodies :-[3]

(a) National Cyber Coordination Centre (NCCC).

(b) National Critical Information Infrastructure Protection Centre (NCIIPC).

(c) Grid Security Expert System (GSES).

(d) National Counter Terrorism Centre (NCTC).

(e) Cyber Command for Armed Forces.

(f) Central Monitoring System (CMS).

(g) National Intelligence Grid (NATGRID).

(h) Network and Traffic Analysis System (NETRA).

(i) Crime and Criminal Tracking Network & Systems (CCTNS).

Cybercrime Early Warning, Reporting and Response

Cybercrime, like any other crime, should be reported to appropriate law enforcement authorities depending on the scope of the crime. Quick access of such reporting system should be made available to victims. Law enforcement authorities should be made aware online about the suspected criminal or civil violations. Maintaining centralised database will provide a repository to law enforcement and regulatory agencies at the national, state and local levels. The activities needed to be pursued under this initiative include :-[4]

(a) Adopting and deploying state-of-art tools and techniques.

(b) Creating a structured knowledge repository.

(c) Strengthening partnership and cooperation with industry, international Computer Emergency Response Team (CERTs) and security forums.

(d) Acquisition of intelligence about vulnerabilities, threats, and security risks collated from a comprehensive list of sources.

(e) Establishing a collaboration platform for engaging with security community.

Legal Architecture

Cybercrime raises several challenges for traditional criminal law and the criminal justice system in general.[5]

(a) The first challenge is to define the types of Cybercrimes and include the same in its conceptual framework for influencing national legislation on Cybercrime and policies at international level.

(b) The second challenge is that the Information and Communication Technology (ICT) is complex and dealing with crime involving these devices requires well-trained personnel in the investigation phase, during prosecution, and in courts.

(c) As a third challenge, many Cybercrimes occur in virtual environments like mobile phone channels or the Internet. This feature frequently clashes with the main operational criteria of the criminal justice systems, namely sovereignty and the territoriality principle, hence, it requires countries to establish clear rules on a legal system's jurisdiction over these offences.

(d) The fourth challenge is that the world of ICT moves at a pace different from that of physical world. Crimes occur in a fraction of a second and may spread with astonishing speed.

(e) Lastly, the challenge due to virtual nature of Cybercrimes wherein a perpetrator may be in a different jurisdiction from the victim and the legal definitions of the criminal behaviour in the two legal systems may not match.

Law enforcement agencies must, therefore, take rapid action for collecting and preserving the digital evidence for use in criminal proceedings. If criminal justice systems are to deal effectively with these problems relating to the repression of Cybercrime, they must update their legislation and law enforcement systems where these are unable to cope with investigation and prosecution of the phenomenon. Successful policies undertaken by the foreign countries may be adopted for better utility against Cybercrimes.

Cybercrime Prevention (R&D, Training and Awareness)

There are huge gaps in the number of trained Cyber security professionals available in the Country as compared to the overall requirements. R&D in Cyber security is unsatisfactory. Non-availability of proficient Cyber experts within law enforcement agencies and inappropriate implementation of the strategy means that very few measures are in place to immobilise a larger set of Cyber sleuths to counter the menace of Cybercrime. Additionally, in order to identify the *modus operandi* of the criminals, it is essential to understand the psychology rather than just relying on tools and technology.

Spreading awareness on Cybercrime prevention is an essential requirement. The Cybercriminals are constantly seeking new ways to attack and identify potential victims. In recent times, critical infrastructure of a few countries was successfully penetrated due to the low awareness level of most users, through phishing and social engineering methods.

Citizen awareness programmes should be launched to prevent Cybercrimes, as proactive mitigation has to be achieved through multiple media channels. Mechanisms should be established for independent monitoring of awareness programmes at regular intervals to evaluate the number of people and regions covered through the awareness programmes. Awareness material should be updated regularly as well.

International Collaboration

Since the Cyber world transcends all physical barriers, and is also being transnational in nature, it is but obvious that nations across the globe need to strengthen their cooperation and form alliances as well as ensure that their legal, technical and institutional measures are put in place. Though the IT Act, 2008 categorises Cyber offence as a crime in India; it has its own limitations; thus, it lacks the necessary execution on ground. This includes investigation, prosecution and consecutive extradition of a foreign national as well.[6]

India remains a non-signatory to the Budapest Convention, which is the international treaty seeking to address Cybercrime by

harmonising national laws, improving investigative techniques and increasing cooperation among nations. It will be beneficial to have collaboration with International Cyber Security Protection Alliance.

Summary of Action Plan

A summary of action plan which needs to be initiated at the national level are given as below :-[7]

(a) **National Response.** Improve our detection and analyses capabilities to defeat high-end threats, with a focus on the critical national infrastructure.

(b) **Governance.** Establish internationally agreed 'rules of the road' on the use of Cyberspace and ensure its implementation.

(c) **Security.** Manage and ensure that the key critical infrastructure remains safe and resilient.

(d) **Cooperation.** Share information of threats in Cyberspace, including from private sector, for creation of security database at national level.

(e) **Execution.** Enable all law enforcement agencies to handle Cybercrimes and forensics.

(f) **Reporting and Response.** Build an effective chain for reporting Cybercrime and improving the police response at local level for those who are victims of crime.

(g) **International Synergy.** India should ratify all international forums so that Cybercrimes can be prosecuted across borders and offenders are denied safe havens and offshore help.

(h) **Legal Framework.** Courts of Law should be empowered with enforcement capabilities to report, react, disrupt and prosecute Cybercrime.

(i) **Core Competence.** Promoting development of a cadre of skilled Cyber security professionals to retain an edge in the area of crucial key skills and technologies.

(j) **Awareness.** Because prevention is a key, we need to work to raise awareness, educate and empower people and firms to protect themselves online.

(k) **Role Model.** Model the best practices on Cyber security in the Government's own systems thereby setting up strong standards for suppliers to the government agencies.

Conclusion

To positively impact the Cyber security ecosystem and to combat Cybercrime, it is imperative that efforts and resources are dedicated to operationalise the Nation's Cyber security strategy. If such initiatives are driven from the highest level of the Government, it ensures that all stakeholders are interested and engaged in contributing to the success of initiatives or programmes. Such commitment alone, though it is an important enabler, is not sufficient to guarantee the success of an initiative or programme. Monitoring and review mechanisms are essential to analyse and assess progress as well as to consider measures for re-calibration and course correction as may be required. It is important to define milestones and operationalise the strategy as per the desired impact of the initiatives.

Endnotes

[1] The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Nov 2011, CRET-UK.

[2] ITU National Cybersecurity Strategy Guide Dr. Frederick Wamala (Ph.D.), CISSP, Geneva, Switzerland.

[3] Strategic national measures to combat Cybercrime: Perspective and Learning's for India, August 2015, by ASSOCHAM India. p 10 – 12.

[4] XII Five-Year Plan on Information Technology Sector, Report of Sub-Group on Cyber Security, Ministry of Communications & Information Technology, Department of Information Technology, Government of India. p 111.

[5] *Op. Cit* 3.

[6] National Cyber Security Policy -2013, Ministry of Communication and Information Technology, Department of Electronics and Information Technology, Govt of India.

[7] *Ibid.*