Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-05
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Cyber Security and laws of India and other countries

K. Udaya Sri, M.B.A., M.Sc., M.Tech.,(Ph.D). Asst. Professor, Dept. of MCA, NRI Institute of Technology.
E-mail : kudayasri@yahoo.com

Abstract: Our electronic devices are such a big part of our lives today that it's hard to imagine what we once did without them. But our constant use of technology to keep in touch, pay bills, stay on top of the news, shop and research things has a downside: Our data can be exposed to criminals who commit crimes such as identity theft and credit card fraud – unless we take the proper precautions. Our growing reliance on electronic devices is part of the reason why careers in cyber security are growing at a faster pace. Jobs in information security, web development and computer network architecture – three fields at the forefront of cyber security – are expected to grow 22% between 2010 and 2020.1 Understanding the threats can help everyone do their part to make those jobs easier. Here are five top cyber security threats and tips on how to protect yourself against them, according to experts.

Keywords: Cyber Security, Cyber crime, Cyber laws.

Reasons for Cyber security

India had no Cyber security policy before 2013. In 2013, The Hindu newspaper, citing documents leaked by NSA whistle blower Edward Snowden, has alleged that much of the NSA surveillance was focused on India's domestic politics and its strategic and commercial interests. This leads to spark furor among people. Under pressure, Government unveiled a National Cyber Security Policy 2013 on 2 July 2013.

Vision

To build a secure and resilient cyberspace for citizens, business and government.

Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Objective

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.

- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

- To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.

- To create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training.

- To provide fiscal benefit to businesses for adoption of standard security practices and processes.

- To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.

- To enable effective prevention, investigation and prosecution of cybercrime and

enhancement of law enforcement capabilities through appropriate legislative intervention.

What is a cyber crime?

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.What is Cyber Law?

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

National Cyber Security Policy

NCSP is a proposed law by Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India. which is due to be passed by parliament, aimed at protecting the public and private infrastructure from cyber attacks.[1] The

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

Cyber Laws of India

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways. The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking,Virus/Worm attacks,DOS attack etc.

The computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber Security is a complex and complicated branch to manage. EvenCyber Security Awareness in India and World Wide is not upto the mark. It is very difficult to find a Consolidated and Holistic Website or Online Resource in this regard.

The Conflict of Laws in Cyberspace have also touched the Cyber Security issues world wide. The Conflict of Laws Scenerio in Indian Cyberspace is also evolving. Google's Online Defamation Case is a classic example of this situation. Indian Government must ensureTechno Legal Measures to regulate Indian Cyberspace. E-Surveillance, Civil Liberties Protection in Cyberspace and Conflict of Laws have made the situation really complicated. Indian Government is contemplating formulation of an E-Mail Policy of India. An Indo-American Alert, Watch And Warn Network has also been estabilised to for

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Real Time Information Sharing in Cyber Crime Cases.

International Cooperaton and Colloboration in the field of Cyber Security is an essential requirement in the present interconnected world. For instance, Cross Border Cyber Attacks and Authorship Attribution issues are not easy to manage in the absence of International Cooperation.

If you are interested in Techno Legal Cyber Security Issues of India and World Wide, this is the right place to start with. This Platform and Website is managed by Perry4Law, Perry4Law Techno Legal Base (PTLB) and Perry4Law Techno Legal ICT Training Centre (PTLITC). This Website is also trying to Consolidate the Cyber Security Initiatives and Projects of PTLB at a single place.

We at Perry4Law, PTLB and PTLITC are managing the Exclusive Techno Legal Cyber Security Research and Development Centre of India and Exclusive Techno Legal Centre of Excellence for Cyber Security in India.

Further, PTLB is also managing a very Significant and Exclusive Techno Legal National Cyber Security Database of India (NCSDI). The NCSDI is a Techno Legal Database of Cyber and Information Security Professionals of India. NCSDI is also a National Database of Information Security, Ethical Hackers, Cyber Forensics And Techno Legal Professionals Of India. PTLB also manages the exclusive Techno Legal Cyber Security Software Repository of India.

Cyber Security in India is at its infancy stage and is still maturing. We cannot ignore Cyber Security in India as it has become an Indispensable Asset to protect Businesses, Governments, Organisations, Institutions and Individuals. The same must be a part of the National Cyber Security Policy of India and of any other Nation.

For a Secure and Strong Cyber Security of India, we have to ensureCritical ICT Infrastructure Protection in India (CIP in India) as well. There is no doubt that Critical Infrastructure Protection in India is urgently needed. The same cannot be done till we ensure Techno Legal Cyber Security Skills Development in India.

Cyber Security Skills are essential to manage Offensive and Defensive Cyber Security Capabilities of India. Further, Managing India's Cyber Security Problems, Issues and Challenges would also require Techno Legal Expertise. Crucial Cyber Security Issues like Cyber Warfare Against India, Cyber Terrorism Against India, Cyber Espionage Against India, etc require tremendous Techno Legal Expertise.

Formulation of an Effective and Robust Cyberspace Crisis Management Plan of India and its Actual Implementation in the best possible manner by Indian Government and various Cyber Security Stakeholders of India is also need of the hour.

Projects like National Cyber Coordination Centre (NCCC) of India,Central Monitoring System (CMS) Project of India, National Counter Terrorism Centre (NCTC) Of India, National Intelligence Grid (Natgrid) Project of India, National Critical Information Infrastructure Protection Centre

(NCIPC) Of India, etc must be managed not only in a Techno Legal Manner but also in a Constitutional Manner.

We also need to ensure a Techno Legal Framework for India. For instance, we must formulate Encryption Laws and Regulation in India,Cyber Security Laws in India, Data Security Laws in India, Data Protection Laws in India, Privacy Laws in India, etc.

At the same time we must ensure a Strong and Effective Legal Enablement of ICT Systems in India. The same must also be supported by Cyber Forensics Capabilities in India. The ICT Trends of India 2009-2012, Cyber Law and Cyber Security Trends in India 2011, Cyber Crimes Trends in India 2012, Cyber Laws Trends in India 2012, have shown little advancement in this regard in India. A Sound Cyber Security Policy of India and effective Cyber Security in India is also going to benefit the "Indian Outsourcing Industry" that may face difficulties and harsh decisions in the absence of Data Protection Law in India, Privacy Rights Protection Laws in India, Inadequate Cyber Security in India, etc

1. Hacking

Hacking is not defined in The amended IT Act, 2000. According to wiktionary, Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network . Also, in simple words Hacking is the unauthorized access to a computer system, programs, data and network resources. (The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

2. Data Theft

Accoriding to Wikipedia, Data Theft is a growing problem, primarily perpetrated by office workers with access to technology such as desktop computers and handheld device, capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD Storage and other hand-held devices.According to Information Technology (Amendment) Act, 2008, crime of data theft under Section 43 (b) is stated as - If any person without permission of the owner or any other person, who is in charge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held

or stored in any removable storage medium, then it is data theft.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379, 405 & 420 of Indian Penal Code, 1860 also applicable. Data Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

3. Spreading Virus or Worms

In most cases, viruses can do any amount of damage, the creator intends them to do. They can send your data to a third party and then delete your data from your computer. They can also ruin/mess up your system and render it unusable without a re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Usually the virus will install files on your system and then will change your system so that virus program is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victims.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 also applicable. Spreading of Virus offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate

4. Identity Theft

According to wikipedia Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Cyber security laws in other states

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Russian media report here and here that Russia and China are preparing to sign a cybersecurity treaty when Vladimir Putin visits China on November 10. The reported agreement would be the latest addition to the increasingly complex landscape of international agreements related to various aspects of cybersecurity—an area that in recent months has also added an African Union treaty and a NATO declaration. The long-term effect of the bilateral and regional agreements is unclear: they could pave the way for broader multilateral treaties or less formal agreements, or they could entrench opposing views and thereby make broad international agreements more difficult. The most likely outcome may be somewhere in the middle.

The details of the Russia-China treaty are sketchy. Media reports indicate that the treaty would allow Russia and China to develop "joint projects and conduct[] joint cybersecurity operations" and to cooperate on "information security." "Information security" typically refers not just to the security of systems and networks, which is what the United States and other countries mean in using the term "cybersecurity," but also to regulation of information content. For example, a Shanghai Cooperation Organization agreement on "Cooperation in the Field of Information Security," signed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan in 2008, lists as a major international information security threat the "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environments of other States."

With the exceptions of the Shanghai Cooperation Organization agreement and, most importantly, the Council of Europe Convention on Cybercrime (or Budapest Convention), cybersecurity has been a rather agreement-poor area. But the new Russia-China agreement will be the latest in an increasingly long list of recent cybersecurity-related agreements.

In June, the African Union (A.U.) adopted the "African Union Convention on Cyber Security and Personal Data Protection." The Convention addresses e-commerce and personal data protection, but also cybersecurity and cybercrime. It commits A.U. member states to develop national cybersecurity policies and to adopt criminal legislation to address, for example, attacks on computer systems and data breaches. It also, however, addresses information content. The Convention requires states to adopt criminal provisions regarding computerized production and dissemination of child pornography. Other provisions—more controversial for U.S. audiences accustomed to the scope of U.S. First Amendment protections—require criminalization of computerized creation and dissemination of "racist or xenophobic" ideas, discriminatory threats or insults, and expressions of denial, approval, or justification of genocide or crimes against humanity.

In September, NATO endorsed an "Enhanced Cyber Defence Policy," building on its 2011 "Policy on Cyber Defence." In a declaration accompanying a meeting of heads of state, NATO affirmed that "international law, including international humanitarian law and the UN Charter, applies in cyberspace," and clarified that "a decision as to when

a cyber attack would lead to the invocation of Article 5 [governing collective defense] would be taken by the North Atlantic Council on a case-by-case basis." (See paragraph 72 of the declaration.)

The long-term impact of the proliferation of regional agreements on prospects for an overarching international cybersecurity treaty is not entirely clear. On the one hand, development of a number of agreements could help build toward a broad international consensus: groups of states could agree on the same positions seriatim, or if a series of agreements come to differing conclusions, then at least bargaining positions would be clearer for purposes of negotiating a broad multilateral treaty. On the other hand, regional agreements could lock states into divergent positions and render subsequent compromise on a single international agreement more difficult. The recent agreements may be heading in this direction by entrenching the Russian-Chinese view of the importance of "information security" (as opposed to the U.S.-European Union emphasis on "cybersecurity") and establishing an A.U. position in support of criminalizing expression that would violate the U.S. First Amendment.

The most likely outcome may be somewhere in the middle.

As I explore in more detail in a forthcoming article, specific issues may be ripe for broader international agreements. For example, although A.U. member states have generally refrained from joining the Budapest Convention (A.U. member Mauritius is an exception), some of the cybercrime provisions of the new A.U. agreement suggest overlap with the Council of Europe and could form the basis for a broader treaty in the future, despite potential disagreements over particular questions, like treatment of computer-based racist speech. For its part, the United States has advocated harmonization of cybercrime laws across countries specifically by encouraging countries to ratify the Budapest Convention, as the United States and a handful of other non-Council of Europe countries have done. The development of a competing regional cybercrime treaty may cause the United States to reconsider its insistence on the primacy of the Budapest Convention and to look more favorably on the possibility of a new, truly international cybercrime treaty that would span regions.

In contrast to the potential consensus developing on cybercrime, the disagreements over the questions of cybersecurity and sovereignty are more fundamental and render broader international agreements less likely. China and Russia's conception of "information security" leads them to advocate for a sovereignty-focused governance model that is antithetical to the multistakeholder, bottom-up approach that the United States andEuropean states have advocated. Regional agreements that entrench these fundamentally different approaches are more likely to be hindrances, rather than stepping stones, to broader future agreements. However, regional agreements like the NATO declaration may nonetheless provide helpful clarity about how particular countries and their allies view specific behaviors in cyberspace and how they will respond to cybersecurity incidents. In other words, although conflicting regional agreements may not foster

broader agreement, they may at least help to promote clarity and avoid conflict.

References

1. "Amid spying saga, India unveils cyber security policy". Times of India. INDIA. 3 July 2013. Retrieved 24 September 2013.

2. "National Cyber Security Policy 2013: An Assessment". Institute for Defence Studies and Analyses. August 26, 2013. Retrieved 2013-09-24.

3. "For a unified cyber and telecom security policy". The Economic Times. 24 Sep 2013. Retrieved 2013-09-24.

4. "National Cyber Security Policy Of India 2013 (NCSP 2013)". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 26 December 2013. Retrieved 2014-08-14.

5. "Cyber Security Trends And Developments In India 2013". Perry4Law's Techno Legal Base (PTLB). 30 December 2013. Retrieved 2014-08-14.

6. "Cyber Security Breaches Are Increasing World Over And India Must Be Cyber Prepared". Perry4Law Organisation. 22 May 2014. Retrieved 2014-08-14.

7. http://blog.devry.edu/2014/02/top-5-cyber-security-threats-that-could-affect-your life.html#sthash.tuDhdCdD.dpuf