CYBER CRIME, CYBER ATTACK, CYBER WARFARE – THEIR IMPACT

Iran's controversial uranium-enrichment programme - the key to its controversial nuclear plans - shuddered to a halt for at least one day in the month of November, 2010, revealed a confidential United Nations report. Iran's nuclear chief, Ali Akbar Salehi, blamed it on unspecified "enemies". The 'enemies' had attempted to infect Iran's nuclear activities with the self-replicating Stuxnet worm 18 months ago. But, he claimed, they were foiled by vigilant young Iranian computer experts. The virus has been described as the world's first cyber-guided missile.

A massive cyber attack cut Internet connectivity in Myanmar in 2010, just three days before the nation's first election in 20 years.

The Economic Times in its edition published on 18th June, 2008, London reported that, "Half of the people from a village named Wychbold in Worcestershire have become victims of an international credit card fraud with money being withdrawn from their accounts in India, Sri Lanka, Denmark and the Dominican Republic."

Recently, international investigators busted a vast Internet fraud network and charged 38 suspects, most of them Romanians living in the United States. The suspects were accused of using a technique known as "phishing," or sending messages to Internet users that appear to come from their bank, eBay or PayPal in order to get their banking information and steal their money. These hackers transmitted the information to US-based accomplices, who used it to make fake bank cards and withdraw cash from ATM machines, according to the indictment.

The Crime Branch of Pune Police investigated a major scam that was taking place in one of the prestigious hotels in India, the 'Le Meridian'. In this scam in all four people were involved, one amongst them was a cashier at the hotel. They cheated over thirty customers of the hotel by copying their credit card details on blank or blocked plastic cards. These fake cards were then used for purchasing expensive goods.

Similarly, in southern California criminals were using illegal electronic devices to steal personal information of credit and debit card users. Recent innovations in criminal technology made this spate of crimes possible. They used a tool known as a 'skimmer' to produce their own

duplicate credit and debit cards to break open the accounts of debit and credit card holders.

The article, 'The Law of Cyber Attack' written by Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel in the International Conference on Cyber Laws, 2014, quoted:

An act is a cyber crime when the act by a non-state actor is criminalised under state or international law.

An act is a cyber attack when it is carried out by state or non-state actors, involves active conduct, aims to undermine the function of a computer network and has a political or national security purpose. Not all cyber crimes are cyber attacks.

An act is called cyber warfare when cyber attacks have effects equivalent to those of a conventional armed attack or occur within the context of armed conflict. All cyber warfares are cyber attacks but not vice versa.

Crimes such as fraud of international credit cards or cheating customers of the hotel by copying their credit card details come under purview of cyber crime. But the attempts to infect Iran's nuclear activities with the self-replicating Stuxnet worm and the internet shutdown in Myanmar prior to elections are all examples of cyber attack.

The effects of a single, successful cyber crime can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cyber crime on society and government is estimated to be billions of dollars a year. Cyberwarfare has the impact intruding network jeopardizing national security, public safety and economic challenges. Technology, in this case, becomes a double-edge sword. The very technologies that empower us to lead and create also empower individual criminal hackers, organized criminal groups, terrorist networks and other advanced nations to disrupt the critical infrastructure that is vital to our economy, commerce, public safety, and military.

Attacks on computer networks have started crossing the line from mere theft and disruption to destruction, posing a threat to the national and political security of nation states. This is the gruesome face of cyber crime to day. Which law governs these attacks?

The United States military sector has strengthened the awareness that a threat moving through cyberspace may constitute a serious danger to the safety of citizens and the stability of the government. This consideration, however, is open to other scenarios, including the use of the military operations in cyberspace for offensive purposes that offer many advantages compared to a conventional attack. Different from what leads to a conventional attack, a cyber attack can be conducted in a silent way in times of peace and this leads to having to consider the extremely insidious threat that requires a high level of alertness.

Every war is fought with proper weapons and cyber warfare is not an exception. Cyber weapons, tools and software are being used to offend enemies in cyberspace. But despite the frequent usage of the term "cyber weapon", today there is no formal and legal definition for it. The impact of the absence of a global recognized definition for cyber weapons is serious. The lack of definition makes it impossible to distinguish a cyber weapon and its proper use, and to evaluate the legal and political responsibility of the aggressor and the real level of threat made in a cyber warfare context.

The anonymous nature of cyber weapons accelerates the impact of destruction since cyber agents can operate under cover not having to reveal the real origin of the attack. Further it also helps to bypass the sanctions of the international community because of the nature of the offence.

According to the United States Government view on cyber war, the use of cyber weapons is complementary to conventional military strikes. It could be possible to:

- Support offensive operations destroying enemy defence infrastructures.
- Probe the technological capabilities of the enemy by evaluating the ability of an agent to infect enemy system.

The cyber security marketplace is flooded with products that promise quick fixes but it is becoming clear that the increasing persistence and sophistication of attacks will require solutions beyond the traditional.

It is thus apparent that cyber criminals are not under the pressure of arrest and prosecution, creating havoc in the society. Not only are they targeting

the social fabric of the society- the trust of the people, the financial muscle of the industry but also the national and political security of nations.

Application of the law is a challenge to the law enforcement wing of the Government. World over the governments as well as the private sector organisations are devising measures to control and curb cyber crime. But the dynamic nature of this crime makes it difficult to put it within a legal framework.

Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce. As e-business expands globally, the need for strong and consistent means to protect networked information will grow.

In the year 2000, McConnell International LLC, a leading organisation in United States of America rated the capacity of mid-level economies' to participate in the digital economy. In considering information security of nations, the report evaluated public trust in the security of information processed and stored on networks in each country. In this context, information security included:

1. an assessment of the strength of legal protections and progress in protecting intellectual property rights, especially for software;
2. the extent of efforts to protect electronic privacy; and
3. the strength and effectiveness of the legal framework to authorize digital signatures.

The E-Readiness report further examined the existence of legal frameworks to prosecute cyber criminals. This is because a predictable environment of strong deterrence for computer crime is critical to the effective protection of valuable information and networks. Several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors. However, very few amongst them were able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of cyber crime would be held accountable for their actions. The survey further revealed that nearly half of the countries included in the study were rated as requiring substantial improvement in information security. In addition, only a small fraction of countries requiring substantial improvement indicated that progress was currently underway.

Over fifty national governments participated in the survey by contributing recent pieces of legislation, copies of updated statutes, draft legislation, etc. Some of them submitted that no concrete course of action has been planned to respond to a cyber attack on the public or private sector. Countries that provided legislation were evaluated to determine whether their criminal statutes included in their ambit ten different types of cyber crimes in four categories:

1. data-related crimes, including interception, modification, and theft;
2. network-related crimes, including interference and sabotage;
3. crimes of access, including hacking and virus distribution; and
4. computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery.

It has been observed that thirty-three of the countries surveyed have not yet updated their laws to address any type of cyber crime. Of the remaining countries, nine have enacted legislation to address five or fewer types of cyber crime, and ten have updated their laws to prosecute against six or more of the ten types of cyber crime.

Some Asian countries as compared to the other nations in the world have been lagging behind in taking steps for providing an effective and efficient legal mechanism to control cyber crimes. Visa International and Mastercard, the two significant service providers around the globe, have currently listed Indonesia at the second level amongst the worst countries in the world for credit card fraud occurrence by total incidents recorded.

Amongst Asian countries, Japan and Korea are at a level higher than the others in devising and implementing cyber laws. Japanese companies pay their customers for security breaches in the form of an 'apology fine', sometimes per user account affected, which can amount to millions of dollars.

California has also been taking stringent measures to curb cyber crimes. They have strict data breach laws. The law known as ‘SB 1386’ obliges Californian state agencies or businesses to disclose data security breaches to residents if their unencrypted personal information may have been compromised. However, these databases also contain information of residents of other 49 states in the United States of America. Thus, if an organization has to notify Californian customers it is hard for it to leave the others in the dark. ‘SB 1386’ has become effectively a national data breach law because most of the databases are not limited to California. In view of Californian State Senator and co-author of the Californian data breach law, Joe Simitian, "The fundamental thinking behind the bill was

if people didn't know they were at risk they wouldn't be in a position to protect themselves. The first step in being able to protect yourself is in knowing that you are at risk. The legislation is about giving consumers the knowledge they need to protect themselves." The other states in the United States of America have since introduced similar laws, and the United Kingdom is also moving in that direction.

There is no doubt that all nations individually need to keep themselves abreast with effective cyber law mechanism. But at the same time one cannot forget that cyber crime cannot be restricted to a particular nation. Cyber crime is trans-national. Cyber crime committed in one nation may actually have an impact in some other nations.

We all are aware of the havoc created in the world by a virus known as 'Love Bug'. This virus though originated in Philippines spread worldwide and cost businesses thousands of millions of dollars. When the perpetrator of the virus was identified as a student in Philippines, there were no cyber laws in place in Philippines whereby the perpetrator could be prosecuted. On the other hand, the countries where businesses were affected had no jurisdiction to prosecute the culprit whether or not they had effective cyber laws in place. Cyber crime thus has a global impact on the nations.

Discrepancies exist even within countries. For example, in September 2000, the Australian Democratic Party criticized the South Australian (state) government for creating a haven for cyber criminals by not having updated its laws to combat computer-based crime in accordance with the laws of Australia's other states.

It is thus evident that not only are the nations required to take steps to devise and implement effective legislations but while doing so they are required to progress in congruence with each other.

Of late, due recognition is being given to the principle of harmony in national laws. In recent years, international cooperation in law enforcement has been achieved through a series of extradition and mutual legal assistance treaties (MLATs) that allow governments to share information and evidence with each other.

As a step towards achieving this harmony, the European Committee on Crime Problems (CDPC) decided in November 1996 to set up a committee of experts to deal with cyber-crime. In a Convention on cyber crime, held in November, 2001; the Committee of Ministers of the

Council of Europe adopted the Convention and its Explanatory Report. The Report touched upon the shortcomings of domestic laws in tackling the trans-national nature of crime and evolution of international laws as a solution to it. The Convention aimed principally at:

1. harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;

2. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form and

3. setting up a fast and effective regime of international co-operation.

Once the Convention on Cyber-Crime is ratified by the council's leadership and signed by individual countries, it will bind countries to creating a minimum set of laws to deal with high-tech crimes, including unauthorized access to a network, data interference, computer-related fraud and forgery, child pornography, and digital copyright infringement. Europe, through this Convention has laid the foundation for harmonisation of cyber laws and carved a path for other nations to follow. As of March 2014, 42 states have ratified the Convention, while a further 11 states have signed the convention but not ratified it.

However, the fact still persists that mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals are flouting the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques considerably increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

Does this mean that nations should resign to being victimised till adequate cyber laws are in place? The answer to this is certainly negative. Organisations must focus on self-protection, implementing cyber security plans addressing people, process and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology such as firewalls, anti-virus software, intrusion detection tools, and authentication services throughout the organizations' computer systems.

Organisations hold information. This also includes the information about third parties. This is especially true of providers of various services – bank accounts, credit cards, telephony, etc., but even other organisations also hold such information about shareholders, deposit holders, employees etc. Much of this information is private. What information is private and what is not depends on the context in which such information is held by the organisations. The private information is held by the organisations in trust and not as an owned and tradable asset.

Whether the existing laws recognise this or not, the organisations need to treat this as an ethical issue. It is also in the interest of the organisations to do so. Although legislation is a slow process and usually lags behind the social practices, eventually it does catch up. What is merely ethical today will, in course of time, become a legal obligation. When it does, the organisations that have implemented adequate safeguards, will find it easier and faster to comply with the new obligations.

Globalisation is a relentless process that cannot be wished away. Improvements in technology are driving the world to become a global village. These forces are creating problems that were never envisaged earlier. They are also not affording the luxury of time in devising and evolving checks and balances. Cyber crime is a striking proof of that because cyber crime does not involve physical presence at the site of the target of crime, a basic assumption in criminal law. But other crimes that have this property are also being conjured up by fertile criminal brains.

The new methods of transactions and trades that have emerged with the new technologies are so different from old methods that the old checks and balances are no longer relevant in their respect. While embracing these methods, organisations need to take this into consideration and make provisions against misuse. Since the new methods result in substantial savings or increased revenues or both, a part of this could be set aside for two purposes, firstly to create and maintain safeguards and secondly to recompense any loss suffered by anyone.

The Compliance Officer of the organisation plays a pivotal role in this movement. He is well equipped with appropriate knowledge and ideas essential to introduce the checks and balances within the organisation. He can also contribute significantly in the training and orientation of employees towards achieving this end. These training programmes are crucial from the point of view of implementing the checks and balances that have been defined. Because it is after all the ‘employees’ that build the organisation!

The fight against cyber crime thus cannot be an independent individual effort, neither of an organisation nor of a nation. With cyber crime now raising to the level of challenging the national and political security of nation states, it necessarily has to be a co-operative movement wherein all the nations come together!

Bibiliography:

1. http://www.mcconnellinternational.com/services/cybercrime.htm
2. http://governmentsecurity.org/forum/?showtopic=28450
3. http://www.indiaforensic.com/creditcardfraud.htm
4. http://economictimes.indiatimes.com/Personal_Finance/Credit_Cards/UK_villagers_victims_of_credit_card_fraud_in_India/rssarticleshow/3140778.cms
5. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
6. http://news.cnet.com/2100-1001-268894.html
7. http://cyberlawcybercrime.com/?page_id=477
8. http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

Article by: CS Jaee Goswami, Member of the Institute of Company Secretaries of India