MAPPING DIGITAL CRIME WITH CYBER ACTS

As the cyberspace playing field grows, so does the cyber assets, vulnerabilities and potential threats.

Security cannot be guaranteed and the task of securing a nation is hard. On the other hand, threats to National Security are many. Amongst these threats, in an ever-expanding interconnected world, threats via cyberspace are getting more serious, with each cyber-attack giving tantalizing clues of worse things that could happen. In the previous blog in this series about the Cyber Security, a brief introduction to the terms National Security and Cyber Security were given. These days, we also come across several other terms related to cyberspace like Information Security, Data Security, IT Security, ICT Security and so on. Quite often, there is a lack of clarity on the scope of each.

With the increasing risks of cyber-attacks due to the widespread reach of cyberspace, it is clear that measures taken to secure the assets and people of the nation will have to be enhanced and adapted with time. To define an effective strategy, it is essential to understand

- **the various types of cyber-linked Assets that need to be protected and how they can be classified**
- **the Vulnerabilities that exist which could be taken advantage off by adversaries**
- **the various Threats possible and how they can be classified**
- **what measures are needed to Protect these assets, how to Prevent and Deter such attacks and appropriately Respond to, if an attack occurs.**

In the broader realm of National Security, assets of a nation can be classified into two types:

- **Tangible Assets (Critical Infrastructure, Banking Institutions, Food, Water, etc)**
- **Intangible Assets (Identity, Privacy, Reputation, Governance, Public Confidence etc)**

To classify the subset of assets whose protection fall within the purview of Cyber Security strategies, one good approach could be to split the assets first based on whether they are information and non-information related. The latter includes information that is stored in print or writing, for example, books, files, art works, etc. Digital information corresponds to information stored in digital forms like memory disks or memory drives. The scope of Information Security covers protection of information of all kinds, be it digital or not, and that of systems, tools, objects and various means that are used to store them. It also includes aspects like authorized access, secure transmission and usage of information.

Digital data rely on special hardware and software for its storage, processing and transmission. These are typically grouped together under Information and Communication Technology, which include hardware assets, software assets and associated application databases and services. Protection of ICT assets is a subset of Information Security and normally comes under the scope of ICT Security or IT Security. It also includes protection to ensure authenticity, non-repudiation, accountability and reliability of digital information.
The trend we see is that the reach of ICT technologies to store, process or transmit information is expanding and hence, the scope of IT/ICT Security will soon form a large part Information Security.

Cyber related information assets are tangible assets. There are also non-information assets that rely on ICT infrastructure for their operations. These include power grids, medical facilities, etc. Cyber-attack can not only target ICT systems but can be carried out using ICT systems to wreck operation of other non-ICT systems or infrastructures. In addition to this, there are also intangible

assets that are more people-centric like identity, trust, reputation, privacy, brand name, social status, etc. In some cases, the information itself can cause a security threat through subversion or propaganda.

Any adverse impact on these non-information-based assets and intangible assets can have direct or indirect financial and non-financial implications. Examples include attack via cyberspace to bring down the power grid, cyber terrorism, hacktivism, etc. Though it is quite often hard to quantify the losses due to cyber-attacks on intangible assets, the importance of securing these assets from cyber-attacks is paramount. Therefore, the scope of Cyber Security is wider than IT Security. It is not just limited to ICT protection, but also includes protection of people and systems which use or interface with ICT systems. The scope of cyber security is increasing progressively with time as more and more people and systems get connected to the cyber space.

Hostile attacks via cyber space occur due to Vulnerabilities that exist in the system. Cyber technology is a mix of computer hardware and computer software written to perform a specific functionality. Vulnerabilities that exist in ICT systems are openings for potential cyber-attacks.

Vulnerabilities need not necessarily have to be in ICT hardware or software systems, it can also be due to bad processes and bad practices by people using it. Quite often, people are the weak link in a secure system. While every effort can be made to make a product secure enough to make it fully resilient from attacks through security audits, exhaustive penetration attack testing, etc, vulnerabilities will exist, which will be known only when some attack exploits it, either as part of some authorized testing or when it was used to perform some malicious attack. Hence, management of vulnerabilities should follow a continuous process of improvement cycle, so that, with each iteration, the count reduces over time.

And with these vulnerabilities, comes Threat of attacks. Cyber Attacks at a very broad level can be classified into two main categories, which overlap each other;

- **Cyber Crime**
- **Cyber War**

Cyber-attacks like Cyber Espionage, Cyber Hacking, Cyber Subversion, Cyber Sabotage fall in the overlap area as they can be classified as acts of cyber war or just cybercrime or both, depending on the actors involved and the objective of the attacks. Crime crimes typically have a legal framework to deal with such incidents, unlike cyber war attacks.

From cybercrime perspective a good way to categorize the type of crimes:

- **computer integrity crimes: offences relating to the confidentiality, integrity and availability of information or computer systems**
- **computer-assisted crimes: offences assisted by computers**
- **computer content crimes: offences that focus on the content of computers**

Now, that we have tried to map the various types of assets that have a touch point with cyberspace, the kinds of vulnerabilities that can exist and a classification of the types of cyber-attacks, the question that arises in the Indian context is 'Is India's National Cyber Security Policy 2013 and the Legal framework able to address the challenges of Cyber Security today and in future?'

PARALLEL PROVISIONS IN THE IPS & IT ACT

Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 years or a fine or Rs. 5,00,000 or both.

Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the

words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 years or a fine or both.

It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description[1] for a term which may extend to 2 years, or with fine, or with both." This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 years or a fine or both.

Section 425 of the IPC deals with mischief and states that "whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 months or a fine or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 years or a fine of up to Rs. 1,00,000 or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

Identity theft and cheating by personation: Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 years and also a fine. Forgery has been defined in section 463 of the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment mat extend to 7 years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

Obscenity: Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 years, to be accompanied by a fine which may extend to Rs. 5,00,000, and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 10,00,000. The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 10,00,000 and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to Rs. 10,00,000.

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes,

publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 years, and with fine which may extend to Rs. 2,000 and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 years, to be accompanied by a fine which may extend to Rs. 5,000.

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 months, or with fine, or with both.