Cyber Attacks, Threats, Espionage and Hacking

V. Rajendran
Advocate and Cyber Law Consultant
Email: rajcyberlaw@gmail.com
URL: venkrajen.in
+91-44-22473849; +91-9444073849

Cyber Crimes and Digital War

- Digital War: what constitutes a digital war
- Key features:
  - No physical barriers
  - Offender is often anonymous
  - No physical or other personal contacts
  - Victims do not even know that they are victimized
  - Legal process: filing a complaint, investigation etc
  - Trans-border, international, global reach
  - International laws and treaties

Cyber Terrorism and Cyber Crimes

- Cyber Terrorism is a cyber crime against a community, a nation or a group and often with a cause, a belief, a misguided faith
- Terrorism and crime are as old as civilisation
- Terrorism and acts of treason, Cyber Crime or cyber terrorism, espionage, sedition and attacking a nation's defence infrastructure have been spoken about in as early as 350 BC in Kautilya's Arthashastra

Critical Infrastructure and Intelligence

- The most intelligent system: Human brain
- Thinking, interpretation, non-conformance, violation and criminality – all inter-related !
- Crime *per se* is as old as human being and criminality is as old as human brain and thinking
- Use of intelligent systems in the historic past
  - Use cryptography (Caesar, Alexander, Kautilya)
  - Use of spying – in politics, governance (Arthashastra)
  - Information collection
  - Intelligence gathering – its use, abuse, misuse?

Weapons and tools in cyber attacks

- As against the ICBM, Surface to Air Missiles, a cyber attack has the key-board, mouse and network with a sound knowledge of technology as its tool and enabler
- Stuxnet infamously called the first digital weapon and many other technologies are used
- Quite often, what is technology to one, is an instrument of crime and attack for another. Or, Technology + "mens rea" (ie guilty mind and criminal intention) makes it a cyber crime

Stuxnet

- A malware that gained prominence in 2009, when it reportedly sabotaged Iran's nuclear program reportedly jointly by the US and Israel to destroy Uranium-enriched centrifugues
- Recently reported that even the US tried this to attack North Korea, some five years back and failed in its attempt
- Dreaded to be the most dangerous computer missile ever to have been used with disastrous consequences

Stuxnet

- 2010: created by the U.S. and Israel? reportedly destroyed 1,000 centrifuges that Iran was using to enrich uranium after taking over the computerized systems .
- Gen. Michael Hayden, principal at security consultancy The Chertoff Group, was director of the National Security Agency, and then the CIA, during the years leading up to the event.
- Deploying a cyberweapon to destroy what another nation would describe as its critical infrastructure
- The perpetrator demonstrated that control systems are vulnerable, but also legitimized this kind of activity
- Stuxnet was a game-changer .. Showed that a cyber event can actually result in physical damage according to an official from the U.S. Department of Homeland Security.

Duqu and Flame

- Duqu found in 2011 believed to be from 2007
- considered to be a cousin or a twin of Stuxnet
- Identical to stuxnet; purpose is different
- Captures information like keystrokes
- Filename is different, mostly with a ~
- Flame (2012) also a malware and closely related to Stuxnet exploiting the vulnerability and spreads through USB

THE LAW

TECHNOLOGY

DoS, DDoS,
Steganography, Cryptography
Fastflux, Stuxnet, Trojans,
Cyber Squatting,
IP Spoofing, Cloning, skimming
email Spoofing
Scavenging, Dumpster Diving

are all pure technologies but may be used in crimes. … Tools for cyber attacks

Maritime Transport

Maritime Industry –Transport is critical, because more than 50% of goods in EU is maritime

Maritime governance involves national, EU, other sectors and international policies

Maritime security has always been focussed on physical controls – Of late cyber security is gaining in importance

Training and awareness is the key

Co-ordination among nations, CERTs etc

Cyber Attacks in India

- ¨Common Wealth Games in India, had over 8000 attacks in their ticketing networks, all malicious, all in a matter of 15 – 20 days.
- Thousands of modems in the nation are reported to have been compromised, though not much in cyber terrorism or SCADA attack have been reported as a result. Data spying has never been ruled out.
- Many critical infrastructure attacked in the nation
- Fortunately, no major compromise reported, though data loss and data spying are frequently reported, feared and dreaded.
- Cyber-Attack on Indian Defence Research Lab Thwarted: A Quick Heal Report in October 2014

Some specific attacks

Some specific, dreaded attacks of recent years are

- **botnet** - a collection of programs that communicating with other similar programs to perform tasks sometimes simple and at time dreaded Trojan type tasks, often in DoS or DDoS .
- **Fast flux** is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies and sometimes a combination of peer to peer networking , distributed command and control, or proxy redirection (and recently used in lots of movies too) – avoid tracing
- **Stuxnet** is a computer worm discovered in June 2010 that is believed to have been created by the United States and Israel to attack Iran's nuclear facilities.
- **Zombies -** how they are used - compromised systems in a network

Origin of Cyber War - Attacks

- Basis for any crime
- Crimes and offences are always historic
- Modus Operandi differ
  - according to times
  - according to nations
  - as per individual needs and desires
  - according to the other circumstances
- Cyber war comes in different variants

Cyber Warfare – types

- Chemical warfare: targeting the critical establishments especially the plants which will have devastating effect on the society, on the nation..
- Cyber Murder- Cyber killing: Software and data diddling as a weapon to execute a murder, for a homicide
- Economic warfare: Attacking the economy of a nation, targeting the nation, trying to destabilise the nation, counterfeiting the currency
- National and International warfare: drug, mafia, arms etc
- Specific target against nations
- Extremism, fanaticism and fundamentalism
- Sheer money, money and money

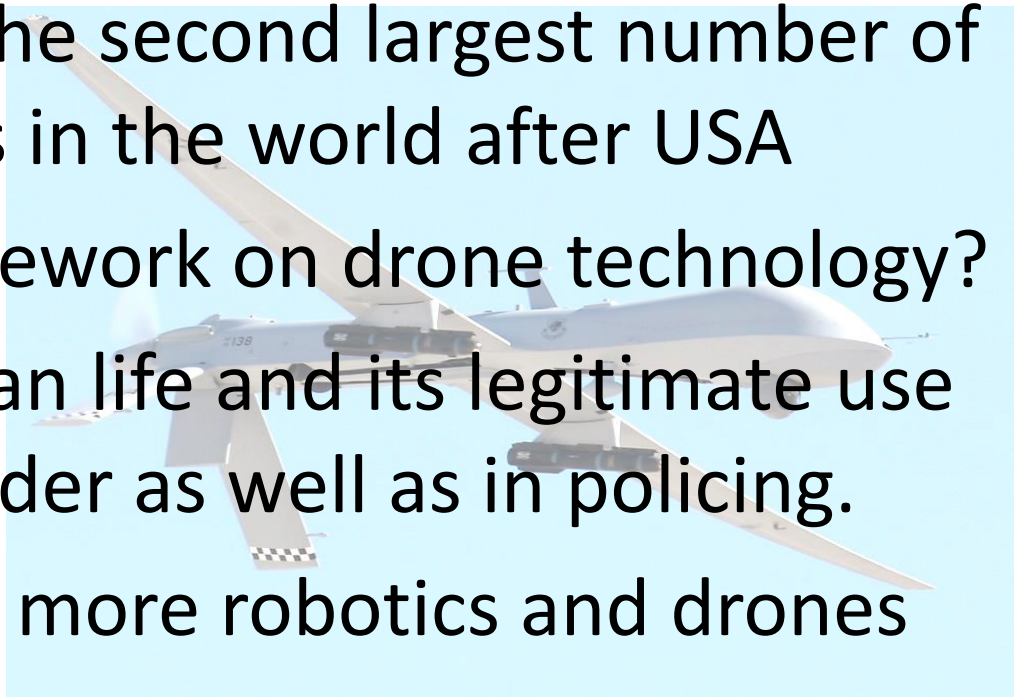
Cyber Terrorism today

Terrorism today is in different manifestations, and biological weapons. This century began with the 19 terrorists attacking the World Trade Center , then the Indian Parliament in Dec 2001. Cyber Attacks are not like the SARS, Swine Flu or Tsunami or earthquakes. It's a transformation from analog to digital and from kinetic to abstract .. Our international cyber security strategy in terms of what the MEA deals with is largely informed by the domestic stakeholders like NSCS, DIT, MHA & DOT. There is a need for norms to deal with cyber space as well as rules. Norms could be a forerunner for a rule based legal framework.

Source: IDSA Cyber Security Report, May 2012

Drones and Robotics

- Drones ie Unmanned aerial vehicle or Remotely Piloted Vehicle may become a spying weapon
- India reportedly has the second largest number of acknowledged drones in the world after USA
- DGCA's policy or framework on drone technology?
- Use of drones in civilian life and its legitimate use in eforcing law and order as well as in policing.
- In future, we may see more robotics and drones



Corporate Espionage

- Cyber weapons of today: keyboard, mouse, network and criminal intelligence
- Spying – Corporate spying
- Use of technology, networks, O/s
- Robotics, Drones – Civilian use of drones
- Virus writing – a professional job
- Cyber Crimes as a Service (like SaaS, PaaS)
- Hired hackers – hackers groups!

Ethics and Hacking

- Line of distinction: Ethics and Hacking
- Professional knowledge and hacking knowledge: its use, misuse and abuse
- Right to privacy of data, Access to it
- Doing illegal things for a legal objective or a public cause or as part of some investigation?
- Role of data portals, banks, telecom companies
- Dealing with public data: Due diligence
- Role of owner, custodian and user

Code of Ethics

- What is ethics?
- Ethics and Law, Ethics and profession
- Code of Ethics is a dynamic concept:
  - Varies according to nation, profession, industry, time, organisation, contractual obligations etc
- Significance of code of ethics in hacking
- Hacking and personal or professional approach
- Legal and ethical issues in hacking

Cyber Attack - Preparedness

- A cyber attack can never be eliminated!
- Be prepared for any attack – that is the best form of security – San Tsui, “Art of War”
- Especially in India, preparedness is the key
- Enhance the defence architecture, making them difficult to access, very hard to attack
- Build a robust preventive mechanism ie preventive steps in the form of technology, social negotiations and legal remedies

Cyber Attacks – Prevention

- Exchange of information on cyber attacks
- Bilateral treaties and multilateral convention
- Budapest Convention on Cyber Crimes – *India?*
- Treaties especially with the neighbouring nations
- Enhancing the border-states on strategic defence mechanism and
- Strengthening the key departments' defence mechanisms

Prevention contd..

- Certainty of punishment rather than severity of laws – required as deterrent
- An exclusive Data Privacy legislation in India
- Expenditure on Cyber Security – No Return on Investment quantifiable for such expenditure
- Indian Judicial System – revamp required to deal with cyber terrorism – Cyber related legislations
- Co-ordination among all stake holders: State Police, CBI, RAW, IB, NTRO, MEA, Defence and Home Ministries, BSF, CERT In etc – A Central Cyber Monitoring Agency or ehanced e-Surveillance

Hacking – Ethical Hacking?

"Hacking" was defined in the earlier version of IT A 2000 (Section 66). Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or delete or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. Hacking is punishable with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

This definition has since been removed in ITAA 2008

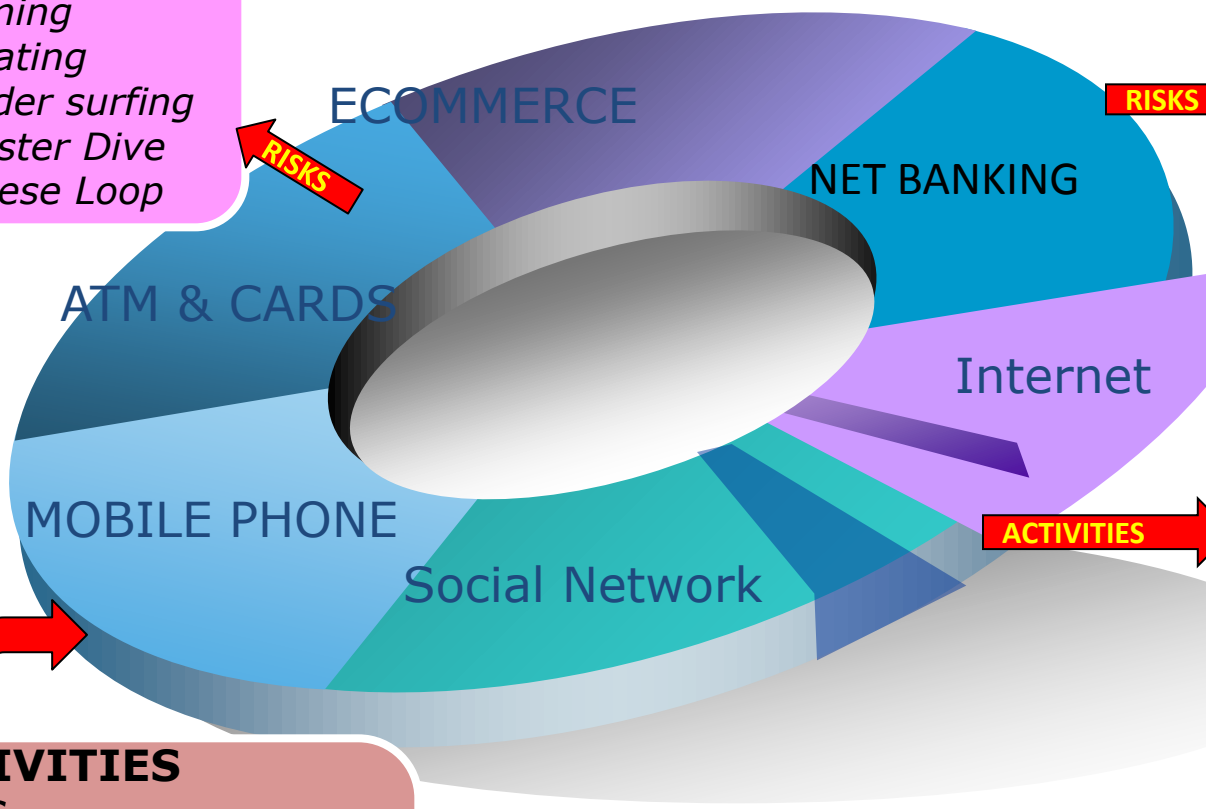
Contents and punishment for hacking still remains.

Unauthorised access to computer is of course, punishable.

The revised section still deals with the offence of unauthorised access to a computer resource, data theft, combining it with the civil offence of data theft dealt with in Section 43,

Punishment 3 years' imprisonment or a fine of Rs.5 lakhs or both.

Touch Points



RISKS
- *Skimming*
- *Tail Gating*
- *Shoulder surfing*
- *Dumpster Dive*
- *Lebanese Loop*

RISKS

RISKS

- *Phishing*
- *Pharming*
- *Vishing*
- *Smishing*
- *Key Loggers*
- *Trojan*

ACTIVITIES

- **Email**
  - Personal
  - *Business*
  - *Forwards*
  - *Enclosures*
- Project related
- Research
- Job search & apply
- Online purchase
- Internet Banking
- **Chat**
- **Downloads**
  - ✓ *Software*
  - ✓ *Application*
  - ✓ *Songs*
  - ✓ *Movies*

ACTIVITIES
- *SMS*
- *Conversation Apps*
- *Mobile surfing*
- *Mobile Banking*
- *Mobile Commerce*
- *Communication*

Hacking and Cracking

- Global Hacking Groups
- Hacking Community
- Exchange of information – informal contracts
- White Hat hacking, Black Hat etc
- Vulnerabilities in the system getting exploited
- VAPT and other forms of testing
- Port Analysers and systemic routines and tools
- Science or an art – A gift, sometimes prodigal too

Hacking – powerful tool?

NSA Report: China Successfully Hacked 600+ American Targets in 5 Years: Click the link – Aug 2015

http://snip.ly/GIdw#http://blog.lifars.com/2015/08/03/nsa-report-china-successfully-hacked-600-american-target-in-5-years/

CERT-In reports over 62,000 cyber attacks till May 2014. Totally 9,174 Indian websites were hacked by groups spread across the world

Govt admits cyber attacks but says cannot identify the culprits Cyber attacks on India increased from about 13000 in 2011 to 62000 till mid-2014.

Source: News reports and Internet

Computing professions

- Professional ethics in the IT industry
- Software and coding – pure computing
- IT and related industries – professions
- Ethics and HR:
  - Antecedent Verification, Exit Policy, Organisational concerns, legal issues, compliance issues
- Ethics and Law in the software
  - Software library, Re-usable code, Across organisations, similar use in rival firms, software ownership and piracy

Code of ethics

- Ethics in the corporate sector normally includes the corporate policy and how the company plans to implement its values
- Depends upon the corporate vision and mission
- Ethical standards set by the organisation
- Mostly related to the employees and personnel
- Applied to all layers of employees
- In specific industries, it has significant relevance eg
  - Medical, software, knowledge-based, skill-based etc
  - Related to disciplinary approach in the organisation
  - Violation often results in serious action
  - Violation very rarely viewed lightly

Ethical dilemma

- A complicated and complex situation that often involves an apparent mental conflict between moral imperatives
- Sometimes neither could be easily adopted and following one path will result in transgressing or violating the standards in another.
- Often determined by situations, persons, times and other circumstances
- Solution most often may be ambiguous
- Needs enormous amount of understanding and entire facts of the case to come out

Very relevant in the context of cyber espionage, hacking, white hat, black hat, protection of corporate e-assets when sometime offence is construed as the best form of defence

Script kiddies

In programming culture a **script kiddie** (or skiddie, skid, **script** bunny, **script** kitty) is an unskilled individual who uses **scripts** or programs developed by others to attack computer systems and networks, and deface websites.

Unlike a hacker, script kiddie does not have pursuit of knowledge, does not know how it works, immature, with some exploratory skills and mostly lacking in discipline which a hacker claims to have

Criminal Profiling

- creating threat profiles on each attack to gain a better understanding of how attackers operate.
- Cyber-threat intelligence must identify trusted sources facing similar types of attacks.
- Users need to "reach back and get context" to effectively block increasingly sophisticated threats
- Intelligence without context is just data.

Criminal Profiling

Offender profiling, also known as criminal profiling, is a behavioral and investigative tool that is intended to help investigators to accurately predict and profile the characteristics of unknown criminal subjects or offenders

Related to cyber forensics

Forensic psychology and investigation

Behavioural based – in technology including mental, physical and programming skills etc

Analyse the characteristic of the unknown criminal?

Cyber Crimes and Digital War

- What constitutes cyber crimes
- Digital War: what constitutes a digital war
- Key features:
  - No physical barriers
  - Offender is often anonymous
  - No physical or other personal contacts
  - Victims do not even know that they are victimized
  - Legal process: filing a complaint, investigation etc
  - Trans-border, international, global reach
  - International laws and treaties

The Cyber War's Most Terrifying Incidents

- The Biggest Military Hack Ever on U.S . Army, Navy &
- Air force – March 2002
- Titan Rain – Aug 2005
- Estonia Attack – April 2007
- Power Grids & Fighter Jets– Hacked Critical Infrastructure in U.S – April 2009
- Stuxnet 2010
- Operation Shady Rat – Aug 2011
- U.S Weapons Plans Hacked – May 2013
- Iran Hacks U.S Energy Companies – May 2013
- U.S Goes on the Cyber Offensive – Jun 2013

SCADA Systems

- Supervisory Control and Data Acquisition
- Generally used in industrial processes like steel making, power generation including nuclear power and distribution, aerospace, chemical plants, petroleum etc
- Central control and monitoring, information gathering and control
- CRITICALITY: software, control, access, use, integrity of data, its reliability and ….destruction?

SCADA Systems

- Supervisory Control and Data Acquisition
- Generally used in industrial processes like steel making, power generation including nuclear power and distribution, aerospace, chemical plants, petroleum etc
- Central control and monitoring, information gathering and control
- CRITICALITY: software, control, access, use, integrity of data, its reliability and ….destruction?

History of Cyber attacks - Estonia

April 27, 2007 and swamped all websites of Estonia
of including Parliament banks, ministries, newspapers and broadcasters, amid the country's row with Russia
DoS Attacks affecting individuals and all organisations, spam distribution targeting almost the entire nation
Case is still studied intensively by many countries and researchers as a state sponsored attack
Russia called accusations of its involvement "unfounded," and neither NATO or European Commsision was able to find any proof of official Russian government participation.
Later, ethnic Russian Estonian national was charged and convicted.

The Christian Science Monitor March 2011

Tomorrow's wars will be fought not just with guns, but with the click of a mouse half a world away that will unleash weaponized software that could take out everything from the power grid to a chemical plant….

Cyber war in the U.S.

April Fool's Day, 2002. Glitches in air traffic controller screens nearly cause a collision above New York's LaGuardia Airport.
Two weeks later, California Independent System Operator Corp., which controls California's power grid, somehow misplaces an electrical energy order to Southern California Edison, leaving two-thirds of San Diego in the dark.
A high-power microwave burst fries the electronics at an abortion clinic in Virginia.
Many such stories and many such incidents, no major catastrophe…? But the fear persists…

Chinese Hackers targeting Whitehall

Defence department officials confirmed a "detected penetration" of elements of the email system used by the network serving the US Defence Secretary office
People's Liberation Army (PLA) was reportedly responsible.
US gave the codename "Titan Rain" to the growing number of Chinese attacks, notably directed at the Pentagon but also hitting other US government depts.
China has officially denied responsibility.
Considered to be the most serious discovered so far

Operations Shady RAT

- A form of Cyber Attack – reported started in 2006 - Widely spoken about from 2011 – A Remote Access Tool – First started with targeting various athletic oversight organisations
- Associated with cyber espionage
- Targets include: SCADA configurations, Olympic and its related data, closely guarded national secrets, negotiation plans, many archived electronic data that may over time be left without proper security
- Generally considered to be a long and persistent attack, gradually taking out data, from the archives document stores, mostly involving Intellectual Property Rights
- Similar malware and spyware: Night Dragon Operation and Operation Aurora
- **Operation Aurora** – reportedly from China, a form of APT which led to the exit of Google from China – Origin from 2009 – 10. Many public portals were the targets including Yahoo! – Main target was: gmail accounts and other details

Some of the top attacks

1. Logic Bomb 1982 US blew up a Siberian gas pipe line
2. Epsilon, email handling service provider, considered as the costliest cyber-heist. Estimated at having a potential cost that ranges from $225m to $4bn
3. Sony: Personal information loss of credit and debit card data of millions of users … damage predicted USD 2 bn
4. Michael Calce called MafiaBoy, attacked Dell, CNN etc and loss estimated USD 1.2 bn
5. Sven Jaschan unleased a virus infected millions of computers .. Estimated loss USD 500 million

Incidents in India

- 13 December 2001 – Indian Parliament attacked - Suicide attack - Pakistan-based Islamist terrorist organizations, Jaish-E-Mohammad and Lashkar-e-Toiba. Aimed at eliminating the top leadership of India and causing anarchy in the country. 7 dead, 12 injured

Incidents in India

- 30 March 2002 and 24 November 2002 – Attaks on the Hindu Raghunath temple 25 dead.
- Attack in Hindu Ram temple Agyodhya – 6 dead
- 29 Oct 2005 – New Delhi serial blasts 60 killed??
- 2006 – Serial train blasts in Mumbai suburban train stations in 11 minutes
- 7 March 2006 –A series of attacks in the Sankath Mochan Hanuman temple and Cantonment Railway Station in the Hindu holy temple city of Varanasi - 28 killed and over 100 injured.

Incidents in India contd..

- 26 July 2008 – Ahmedabad
- Islamic terrorists detonate at least 21 explosive devices in the heart of this industrial capital, leaving at least 56 dead and 200 injured
- Indian Mujahideen claimed responsibility
- Terrorist groups from Bangla Desh and Pakistan suspected
- Investigation by Indian police led to the eventual arrest of a number of terrorists suspected and later identified as Students Islamic Movement of India (SIMI)

Incidents in India contd..

- 13 September 2008 – Serial blasts in Delhi – including India Gate, Karol Bagh, Connaught Place, Greater Kailash – Pakistani militants - 30 people dead and 130 injured, followed by
- Another two weeks later at the congested Mehrauli area, 3 dead.
- 26 November 2008 – Muslim extremists kill at least 200 dead and numerous wounded – series of attacks in India
- Lashkat e Taliba and other groups of Pakistan
- Ajmal Kasab caught – Later executed in 2013
- 7 Dec 2010 - Again bombing inVaranasi, 2 dead 37 injured.

Incidents in India contd

- 14 February 2010 – Pune bomb blast ripped through the city's popular German Bakery, close to the Osho Ashram and diagonally across from the Jewish Chabad House killing 17 people and injuring 65.
- Maharashtra Anti-Terrorism Squad (ATS) claimed involvement of Pakistan based Lashkar-e-Taiba's (LeT).
- Police arrested Mirza Himayat Baig Inayat Baig,who allegedly heads Lashkar-e-Taiba's (LeT) module in the state.ATS has also arrested Bilal Baba Hussain Fareed Shaikh (27).
- ATS has also named six other accused – all co-conspirator and absconding – Mohsin Choudharyy, Yasin Bhatkal, Riyaz, Iqba; Bhatkal, Faiyaz Kagzi and Zabihuddin Ansari.

Cyber Attacks in India 2014

- Symantec says India second largest country in cyber attacks
- India ranked 2nd in cyber attacks through social media in 2014
- Symantec report says India saw 6% of social media scams globally in 2014
- India ranks 2nd in social media scams
- India ranked 3rd in Asia for ransomware attacks
- India is 6th most bot-infected country
- About 65% of bot infections reported in metros
- 34% of cyber attacks in India were targeted at small businesses
- India saw seven ransomware attacks per hour; 170 per day; about 60,000 in 2014
- Cyber criminals are using social media, apps
- Globally, 70% of social media crimes fooled users to manual sharing of scams

Source: News Reports and Internet

Attacks - Global

- In April and May 2007, hackers unleashed a wave of cyber attacks that crippled dozens of government and corporate sites in Estonia, one of Europe's most wired countries. Estonian authorities traced the so-called denial of service attacks to Russia, and suggested they had been orchestrated by the Kremlin — a charge Moscow denied.
- The online assault followed Estonia's decision to move a Soviet World War II memorial from downtown Tallinn on April 27, 2007, sparking furious protests from Russia's government and rioting among Estonia's ethnic Russian minority.
- Experts said hundreds of thousands of computers were used in a coordinated attack against government agencies and banks.

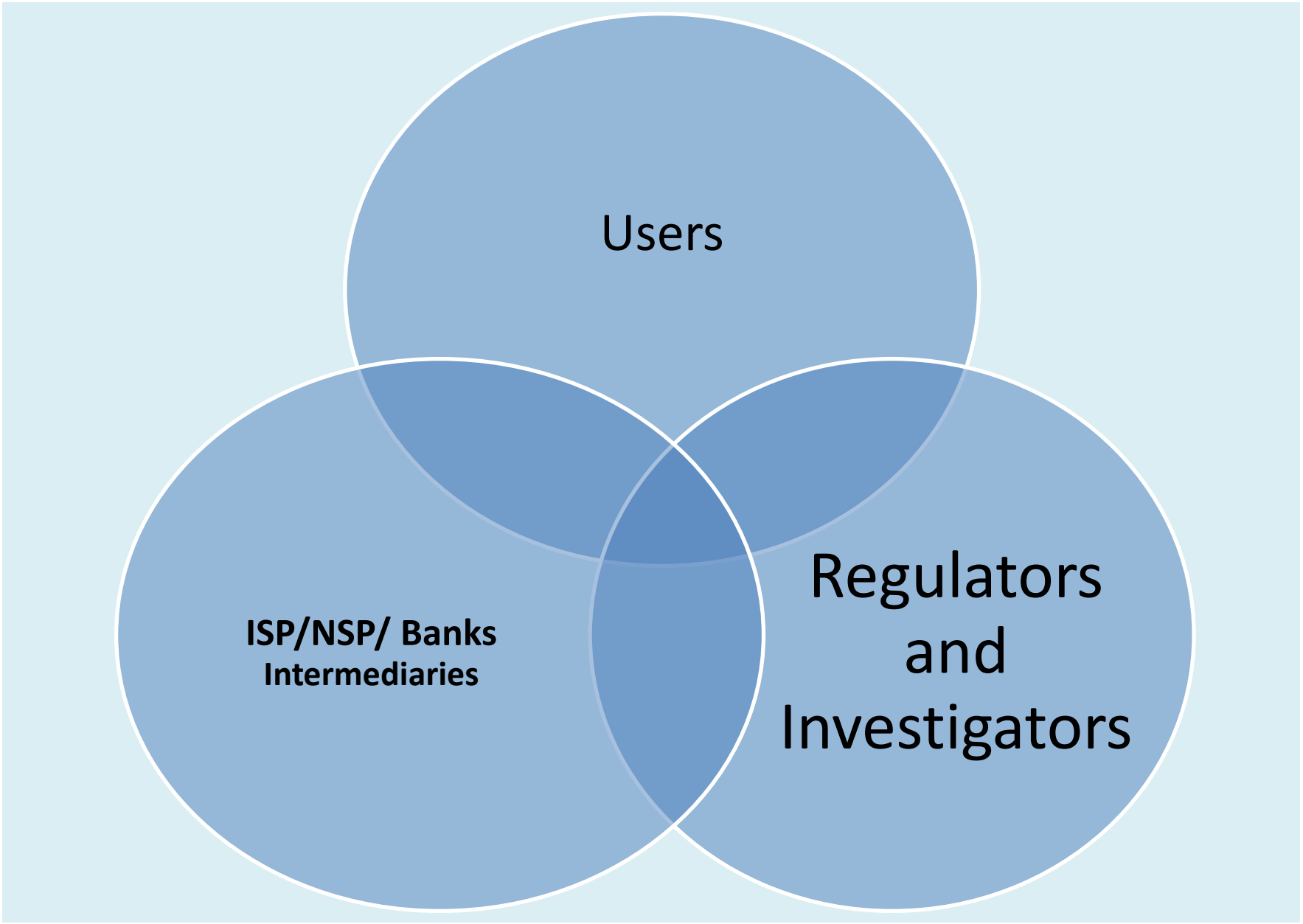
India – Information Security Policy

- India – a signatory to WTO – Members not to discriminate among products as local or foreign and not to restrict free flow of foreign goods
- Exceptions to this clause: National Security
- Products of HUAWEI and ZTE – controversy and concerns from nations like US, Australia, Taiwan leading to their preference for other products
- National Telecom Network Security Co-ordination Board proposed with norms for import of telecom equipment
- Central Monitoring System for telephone tapping, to come
- Mobile Service providers shall use Indian made SIM cards
- Telecom Security Directorate proposed

Cyber Attacks – the Future

- Mobile phones are going to the single point of convergence of technologies – a small weapon the cyber arsenal?
- Digital Evidences and Cyber Forensics
- An enhanced awareness on digital weapons and cyber evidences and a pro-active approach from the government
- Indiscriminate use of technology and unregulated reliance on digital data
- In technology, ease of use vs Security concerns?

Information Security – the stake holders



Long term …. Vision?

TECHNO LEGAL SOLUTION

Promote the use of our own Operating Systems – BOSS already developed by CDAC

- A national level firewall – an overall monitor
- Our own firewalls, Anti Virus, IDS, IPS, UTM boxes, Web filters, Search engines etc
- Our own hardware
  - Domains, server hosts, Storage devices, network equipment

TECHNO LEGAL SOLUTION

- Certainty of punishment, rather than severity of laws
- Implementable rules rather than stricter legislations
- Co-ordinated actions rather than multitude of enactments
- A robust and stronger data privacy legislation in India.