CYBER POLICY AND LAW IN INDIA

TechLegis
ADVOCATES & SOLICITORS

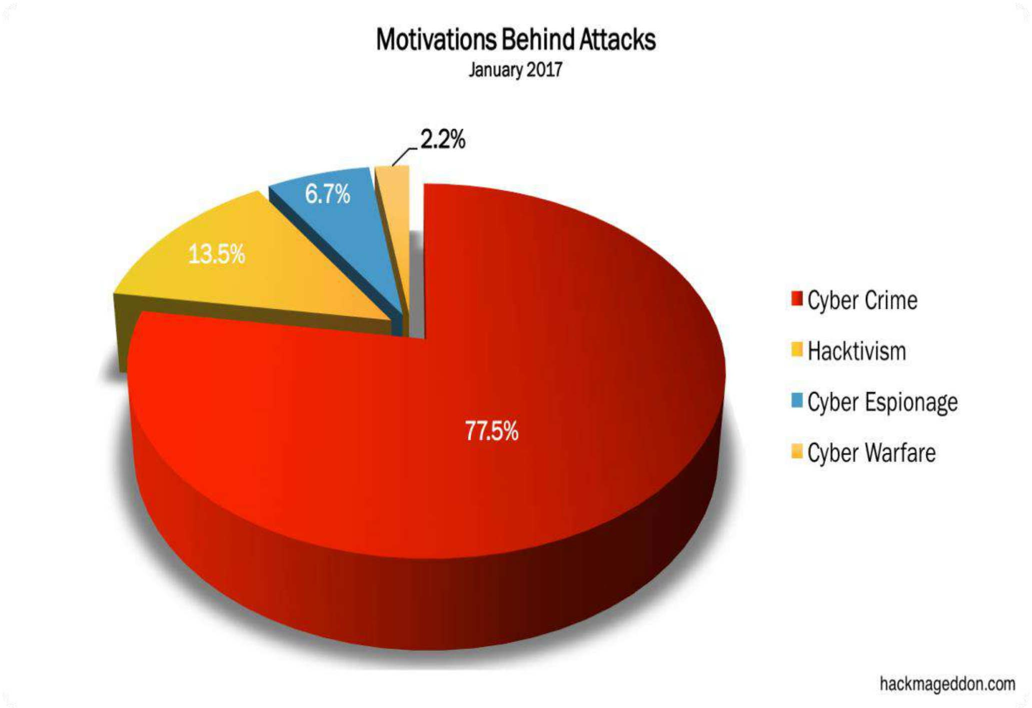
DEFENSE ATTACHE SYSTEM
UNITED STATES OF AMERICA

TOPICS OF DISCUSSION

- Current and intended Government of India Cyber Policy and opportunities to partner with the U.S. Government
- Government and commercial cyber partnership
- Government of India views on international Cyber regulations, including I.P.
- Lessons learned and future intentions with criminal, insurgent, terrorist, or foreign use of the internet, social media, email and bitcoin…and how regulation could impact the general population
- Government of India intentions on offensive or defensive information operations: DOS, darkweb, and botnets

India – US Convergence

Cyber-attacks plague both nations. This is an uncharted territory that has no defined global rules and enforcement.



- India with its vast resource of IT professionals, and the U.S. with its position as a technology and enforcement leader, can develop a trans-national agenda for rules and regulations to avoid cyber terrorism and potential war.

- Both should take the lead in creating a common code of conduct and regulations in the cyber world to avoid future conflict between nations stemming from cyber-attacks.

U.S and India Cyber Relationship Framework

Memorandum of Understanding (MoU) signed earlier this year between the Indian Computer Emergency Response Team (CERT-In) and the Department of Homeland Security.

Purpose of MoU:

- for **cooperation** in the field of cyber security.
- For **promotion** of closed cooperation and **exchange of information** regarding Cyber Security in accordance with the relevant laws, rules and regulations.
- For continuation of Partnership (similar MoU back in 2011).
- Establishment of **bilateral commitment** to an open, interoperable, secure and reliable cyberspace environment.
- **implementation** of a range of bilateral & cooperative **measures to combat cybercrime**.
- to deepen ties and to look to each other as **'priority partners'** in the Asia-Pacific and Indian Ocean region

U.S – India Cyber Dialogue

The **5th Cyber Dialogue** is a forum for **implementing** the Framework for the India–U.S. Cyber relationship.

Deepening bilateral cooperation on a wide range of cyber issues and strengthening the **U.S.-India strategic partnership** by:

- **Exchanging information** on cyber threats and issues of mutual concern, and discussing possible cooperative measures;
- Promoting bilateral **cooperation on law enforcement** and cybercrime issues;
- Creating a **mechanism for cooperation**, including setting up appropriate sub-groups;
- **Affirming** common objectives in international cyber forum, especially the application of **international law to state behaviour in cyberspace**, the affirmation of **norms of responsible state behaviour,** and the development of practical **confidence-building measures**;
- Confirming support for the preservation of **openness and interoperability**, enhanced by the **multi-stakeholder system of Internet governance**; and,
- Coordinating **cyber capacity-building efforts**, including testing and standards with respect to cyber-security.

Initiatives undertaken

- US National Institute of Standards and Technology and the Indian Department of Information Technology- **joint study** of the US Federal Information Security Management Act (**FISMA**)
- The US-India Information and Communications Technology **(ICT) Dialogue**, which focused on increasing economic growth, trade, and investment in the ICT sector; and the US-India Trade Policy Forum
  - which seeks to enhance trade in ICT services and goods while also addressing related cyber-security issues.

- A few top technology-sector executives and US government officials visited India in September to discuss economic innovation and looked forward to the upcoming visit of an **Indian Technology Delegation to the United States.**

- The **International Observer Program of the US Cyber Storm III** national cyber incident response exercise included representatives from CERT-India.

  - Indian and US experts also collaborated to develop recommendations for norms of behaviour in cyberspace.

Opportunities

- It is in the interest of both nations to pursue a convergent and collaborative strategy to counter global terrorism.

- US can help with capacity building in the areas of research and dealing with incidents as well as their mitigation.

- Role of US to carry India to the high table of all internet governance initiatives and cyber security leadership.

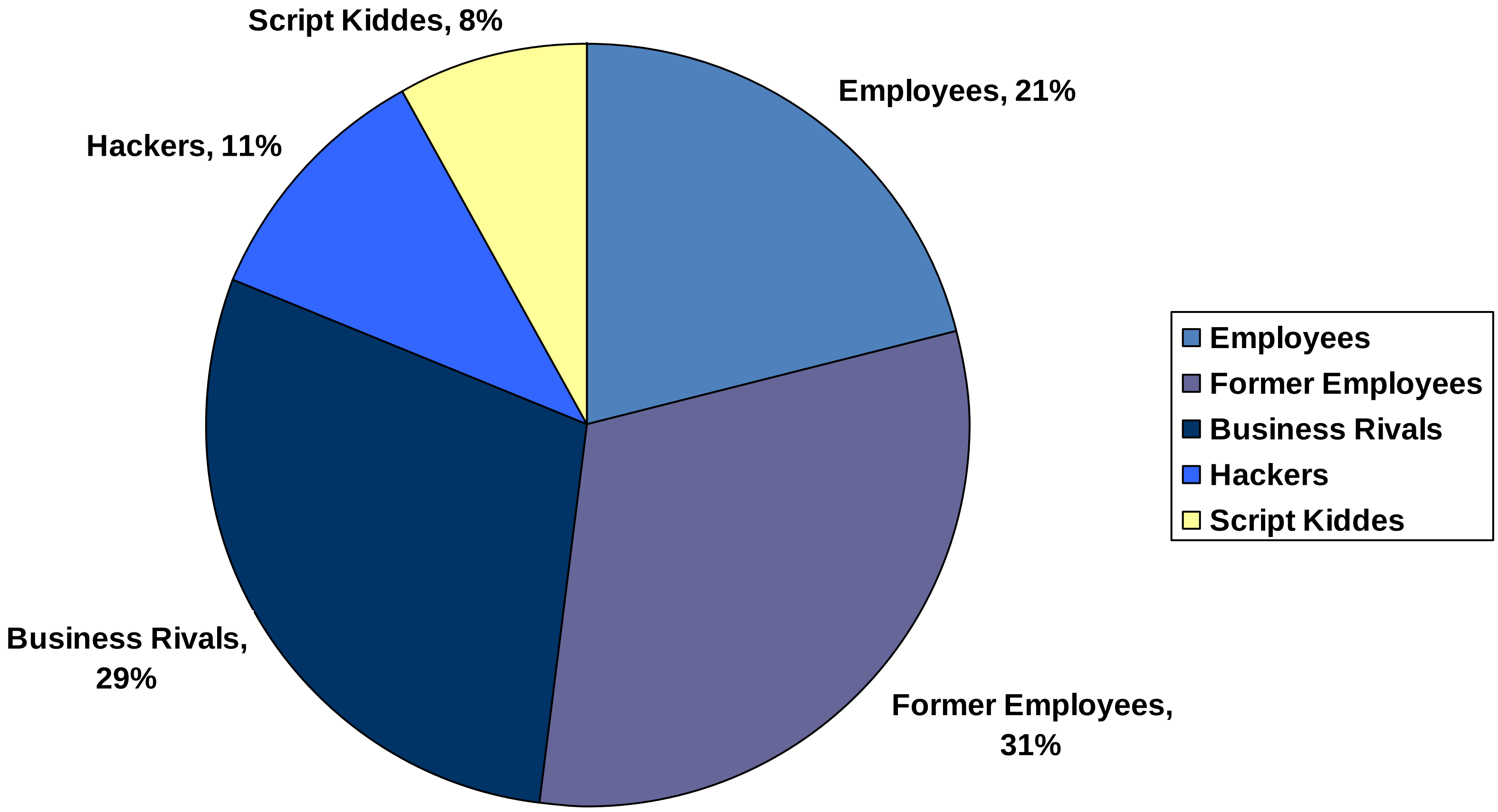
- US plans to transition the management of *the Internet Corporation for Assigned Names and Numbers* in the next few months to the global community, it will be logical for India to be seen as active in the new ecosystem.

- India and the US have to set the stage for more cohesive and open cyberspace engagement so that all tendencies for the Balkanisation of the internet are nullified.

- Dire need to engage with European institutions on data movement and protection.

- Harmonization to reach common threshold in Cyber Space with respect to laws.

Computer Crime & Abuse Report India



THREATS

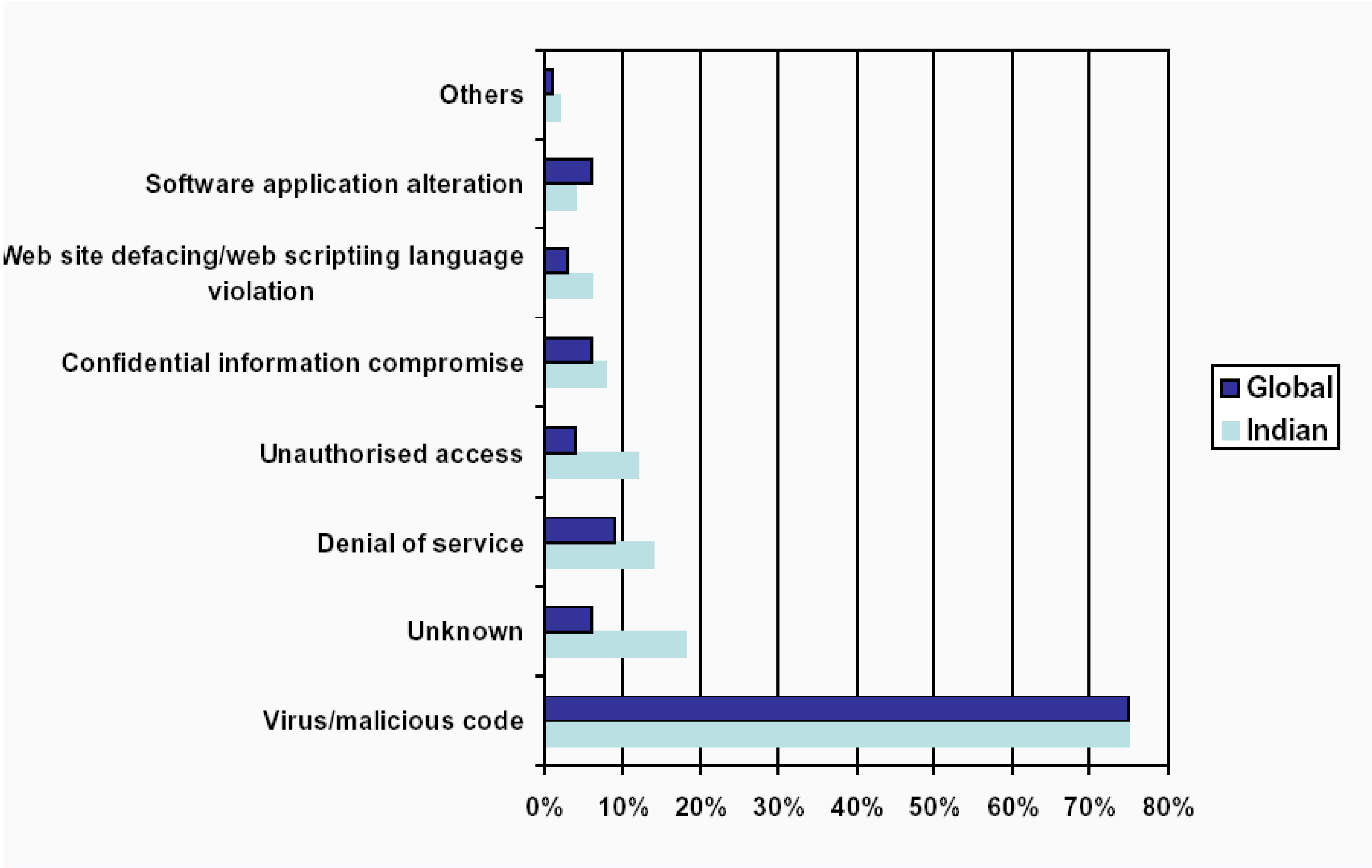
66% of employees say that co-workers, not hackers, pose the greatest risk to consumer privacy.

(Source: Harris Interactive)

54% of consumers said they would be more concerned if their private information fell into the wrong hands due to malicious or accidental incident caused by an employee rather than a hacker.

(Source: The Ponemon Institute)

CYBER CRIMES-NATURE OF EVENTS



Government and Commercial Cyber Partnership

Partnership between Government and Corporates to develop world-leading cyber security technology is the first step in the development of Cyber Innovation to make nation Secure.

For Example:

- The Government of Telangana has signed an agreement with network solutions giant Cisco Systems Incorporation, to cooperate on a host of technology initiatives, including Smart Cities, Internet of Things, *cybersecurity,* education digitisation of monuments.
- Indian government is all set to establish smart cities in India with all cyber security measures along with possible legal issues that may arise.
- NASSCOM and Symantec along with Data Security Council of India (DSCI) signed Memorandum of Understanding (MoU) for 'Building Cyber Security Skills' -- an initiative to develop skilled and certified professionals.

National Encryption Policy

- Earlier there was no specific legislation covering encryption of electronic communication in India so issues relating to ‘electronic data processing’ were covered under the Information Technology Act 2000.
- Further, guidelines by different Government departments provide for different levels of encryption.
  - There existed stark discrepancies between the level of encryption recommended under the IT Rules, SEBI Guidelines and RBI internet banking guidelines on the one hand, and on the other the Department of Telecommunications Licensing Regime relating to the ISPs, NLDs and ILDs.
  - These different guidelines created lot of confusion which prevailed for almost 10 years
- Subsequently IT Act was amended in 2008
  - whereby section 84A allows the government to define and prescribe encryption standards
- The draft of National Encryption Policy was released by the Department of Electronics and Information Technology on September 21,2015 which was withdrawn by Union Communications and IT Minister Ravi Shankar Prasad next day.
  - Policy was panned for being ambiguous and does not reflect final view of government.

- After one year in 2016, Government has restarted the work on drafting the blueprint, asking industry bodies for suggestions.

- The Ministry of Electronics and IT asked industry associations including Cellular Operators Association of India (COAI), Association of Unified Telecom Service Providers of India (AUSPI), and Internet Service Providers Association of India (ISPAI) seeking their opinions and inputs that will facilitate a "robust and secure" encryption policy.
  - Deadline to submit response : August 1, 2017.

- The reworked encryption policy, should be in sync with changes in technology.

- As per the proposed policy framework, the capability to encrypt and decrypt data should be within government.

Regulations

The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce.

- Government has set up cyber forensic training and investigation labs in Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu and Kashmir.
- Indian government has started drafting rules of Data retention for Section 67C of the Information Technology Act, 2000.
- *The Supreme Court of India has always ensured privacy:*
  - For example, telephone interception is permitted by Section 5(2) of the Indian Telegraph Act, 1885. The Supreme Court upheld the validity of telephone interception, but subjected it to a number of safeguards that were absent in the Act. This includes limiting the time and purpose of the interception.
  - Even when the validity of blocking of websites under Section 69A of the IT Act was challenged, the Supreme Court upheld it only on account of the number of procedural safeguards contained in the rules.

- Year 2017 has seen a number of Aadhaar data leaks:
  - Government is working on various legal and other challenges concerning the Aadhaar ecosystem.
- Remedial measures against damages from ransomwares and cyber attacks and to prevent such incidents have been advised by CERT-In.
- The Reserve Bank of India issued warnings in December, 2013 regarding the use of bitcoins and cautions users of Virtual Currencies (notification via Press Release: 2016-17/2054)
- Government in India is considering ways to regulate the currency and has also set up committee to study the circulation of crypto currencies in India.
  - setting up a task force which will take 6 months to come up with recommendations.

Microsoft's Cyber Security Center in India

- 1st approach of Microsoft was to establish data centers and now second one is to establish Cyber security Engagement center.
  - *In October 2016, Microsoft launched its Cyber security Engagement center (CSEC) in India which is situated in Gurugram.*

- It is **seventh** Cyber-security Center in the world and will function as a satellite to the company's Redmond Digital Crimes Unit (DCU).

- The Aim of CSEC is :
  - To drive public-private partnerships to fight cybercrime, strengthen the cooperation with Indian businesses, government and academic organizations on cyber-security, and increase its contribution towards securing Indian computer and internet users from cybercrime threats.
  - It brings together Microsoft's Digital Crime Unit experts comprising attorneys, investigators and security response experts from across the company.
  - The CSEC will leverage Microsoft's DCU Cyber Threat Intelligence Program that monitors and analyze malware infections; provide malware threat assessment and provide actionable information

Cyber Swachhta Kendra

- It was launched and became operational in year 2017

- The " **Cyber Swachhta Kendra** " (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY)
  - to create a secure cyber space by detecting botnet infections in India
  - to notify, enable cleaning and securing systems of end users so as to prevent further infections.

- It is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country.

This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies.

CISCO's Partnership with MeitY

Cisco and Ministry of Electronics and Information Technology's (MeitY) Indian Computer Emergency Response Team (CERT-In) signed a Memorandum of Understanding (MoU) to achieve initiatives:

- Cisco and CERT-In will establish a threat intelligence sharing programme wherein personnel from Cisco and CERT-In will work together to address digital threats and learn new approaches to enhance cyber-security.
- Cisco's global Security & Trust Organization (S&TO) and Cisco India announced the formation of Cisco S&TO-India that will help the government shape the national cyber-security strategy and initiatives.
- Cisco to launch Security Operations Centre (SOC) in Pune in next 3 months which will provide services ranging from monitoring and management to comprehensive threat solutions and hosted security that can be customised.
- Cisco in April,2017 launched its fifth global cyber range lab in Gurugram with an aim to train Indian firms and government agencies on real-world cyber attacks.
  - *It will provide specialised technical training workshops to help security staff build the skills and experience necessary to combat new-age cyber threats.*

GoI - Social Media Misuse and Fake News

- There has been tremendous misuse of social media where people have posted objectionable or illegal content on it.
- The recent case of a man being lynched to death on mere rumours of his storing beef has caught national headlines which led to fuelling of social media activities.
  - the reason Uttar Pradesh Chief Minister Akhilesh Yadav directed his administration to take stern action against those "creating disharmony and inciting hatred" by circulating "baseless" content on social media.
- The action by Uttar Pradesh Police authorities represent a new trend where increasingly now service providers and intermediaries can be called upon by governments to remove or disable access to communally sensitive content, as well as also force them to give the details of the persons behind the same.
- As a nation, we have just very few cases pertaining to misuse of, and cybercrime on, social media.
  - However, given the speed of adoption of social media, it is but natural to expect that more and more cases of misuse of social media need to be registered, investigated and prosecuted.

Wanna Cry Cyber Attack

Cybersecurity experts identified the malicious software as a variant of ransomware known as WannaCry.

- People across the globe specially India were confronted with a message “Oops, your files have been encrypted!” and demanded $300 in Bitcoin, an anonymous digital currency preferred by criminals, to restore access.
- IT Minister Ravi Shankar Prasad said *"There is no major impact in India unlike other countries. We are keeping a close watch. As per the information received so far, there have been isolated incidents in limited areas in Kerala and Andhra Pradesh”.*
- When lot of computers got infected then,
  - The IT ministry reached out to key stakeholders like RBI, National Payments Corporation of India, NIC and UIDAI (Aadhaar) to advise them to protect their systems against ‘Wanna Cry’ ransomware to ensure that the digital payments ecosystem in the country is protected.
  - also instructed cyber security unit CERT-In to gather information on ‘Wanna Cry’ ransomware that has wrecked havoc .
  - The ministry also reached out to the Department of Telecom (DoT) to alert internet service providers (ISPs) to secure their networks as well as the Data Security Council of India (DSCI) and CDAC to ensure that users across the country, especially those in the private sector

Net Neutrality debate

- TRAI came out with a consultation paper on the growth of Over-the-top (OTT) players like WhatsApp or Skype.
  - The Internet and Mobile Association of India (IAMAI) has slammed TRAI saying OTTs are already regulated and governed by the IT Act.
  - TRAI has received over 7-8 lakh comments on the discussion paper that they had first put up on their site on 27 March.
- Rahul Gandhi attacked government over net neutrality issue by saying that 'Digital India' scheme cannot become a "euphemism" for an Internet controlled by large remote corporations’.
- Telecom minister Ravi Shankar Prasad on Sunday asserted the government’s stand on non-discriminatory access to internet saying the issue of net neutrality is being debated by Trai, Thereafter, the government will take its structured view.
- Our plea is that application based traffic management, and allowing telecom operators and ISPs to manipulate user access to websites and apps without checks and balances would lead to discrimination,” Nikhil Pahwa, Co-founder, Internet Freedom Foundation, said.

Lessons learned and Future Intentions

- The speed at which Internet is available has implications in terms of innovation, economy and possibly the degree to which society benefits from technology.
  - Cyber crimes including all social media crimes have affected our country largely.
  - India must invest heavily in infrastructure and access.
- After WannaCry attack, , government in India is considering ways to regulate the currency and has also set up committee to study the circulation of crypto currencies in India.
  - The Reserve Bank of India is also considering using the blockchain technology in banking.
- India does not have any law on privacy so One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

Government’s initiatives against Cyber-attacks

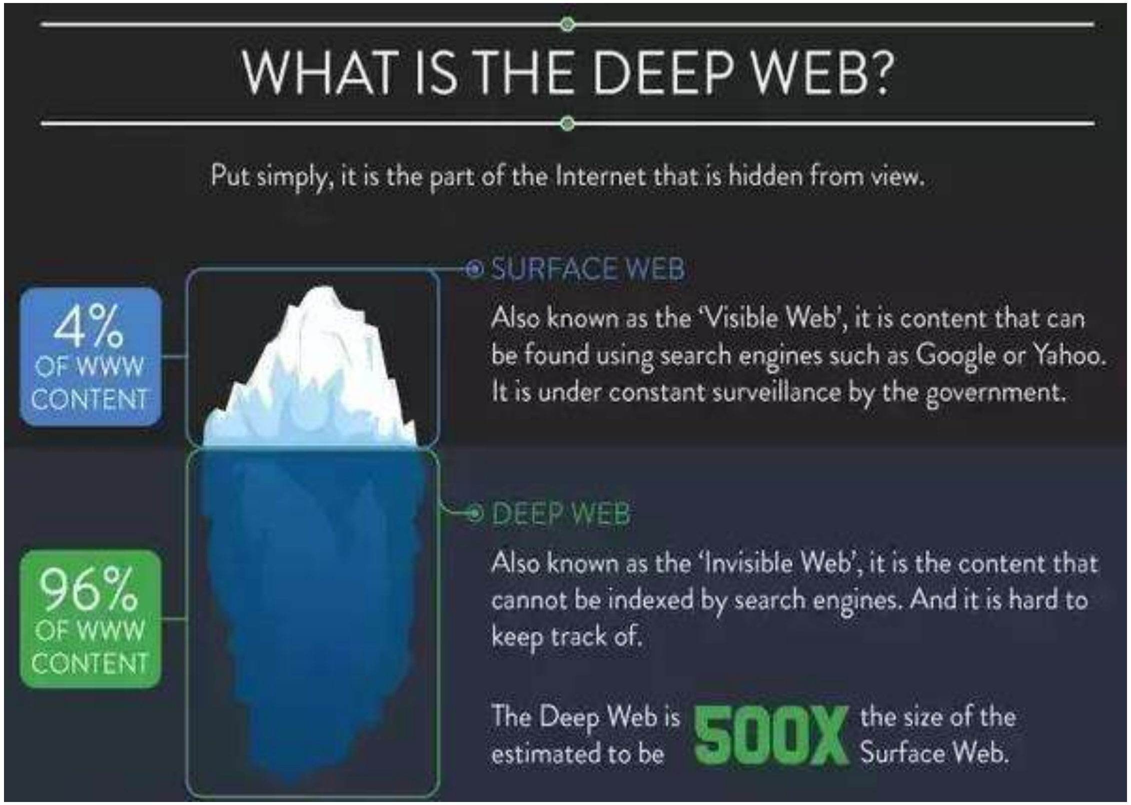
- Due to recent ransomeware attacks,
  - The government is contemplating the establishment of a defensive National firewall aimed at protecting data servers supporting state-owned banks and enterprises against cyberattacks launched by criminals and countries seeking to undermine India's key institutions.
  - "While a firewall may be able to give some protection, but the way we use internet, the attackers may be able to bypass these protections, and so it is important to have a multi-layered protection .
- Government is taking steps against cyber attacks through it’s Computer Emergency Response Team (CERT-in) by launching "Cyber Swachhta Kendra" -- a new desktop and mobile security solution for a secure cyber space in the country.
  - It is Botnet Cleaning and Malware Analysis Centre.
- IT minister also launched USB Pratirodh, which will control the unauthorised usage of removable USB storage media devices like pen drives, external hard drives and launched App Samvid, to protect Desktops from suspicious applications from running.

- The government also announced it would set up CERT-Ins at the state level as well.
- The Indian government has set up a National Cyber Coordination Centre to handle cyber-threats and national security issues in co-ordination with the country's intelligence agencies.
  - "NCCC can be an umbrella organisation coordinating between all law enforcement agencies and defence groups in beefing up national security," says Mumbai-based Prashant Mali, advocate and president of Cyber Law consulting.
- The IT minister also announced:
  - The government will set up 10 more STQC (Standardisation Testing and Quality Certification) testing Facilities.
  - Also empowering the designated forensic labs to work as the certified authority to establish cyber crime
- India’s armed forces fare marginally better, have deployed “red teams” that do penetration testing to protect their own networks against cyber warfare.
- Indian agencies rely on private expertise on an *ad hoc* basis, or buy zero-day vulnerabilities from the ‘dark net’.

- Customer's limited liability for electronic frauds policy finally notified by the Reserve Bank of India.
- Government has issued titled Advisory on Functioning of Matrimonial Websites in Accordance with The Information Technology Act, 2000 and Rules made thereunder.
- Indian government has now decided to formulate a cyber crimes prevention strategy for India.
- Gmail and Yahoo have made telephone number mandatory for creation of new email addresses in a bid to check spam and abuses.
  - this step of Gmail and Yahoo may violate the provisions of various Indian laws thus Indian government and Delhi High Court are in the process of formulating an e-mail policy of India.
  - Delhi High Court has accused central government of sitting over e-mail policy of India. The Delhi High Court has also directed central government to issue notification regarding electronic signature under Information Technology Act 2000 and draft The encryption policy of India.

“Deep Web” or Dark Web has made its presence felt in Indian metros including Hyderabad with several covert illegal deals in child pornography, weapons, drugs and even hiring of killers being carried out by Indians.

- Cyber crime officials are constantly monitoring the Deep Web.
- They are examining ways to build surveillance capabilities.
- Activities on Tor can be punished under the Information Technology Act, 2000.
    - The moment people clinch deals for illegal goods and services on Deep Web they are liable for legal consequences, both civil and criminal



WHAT IS THE DEEP WEB?

Put simply, it is the part of the Internet that is hidden from view.

SURFACE WEB

Also known as the ‘Visible Web’, it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.

DEEP WEB

Also known as the ‘Invisible Web’, it is the content that cannot be indexed by search engines. And it is hard to keep track of.

The Deep Web is estimated to be 500X the size of the Surface Web.

Level 1, Redfort Capital Parsvnath Towers
Gole Market, Bhai Veer Singh Marg,
New Delhi – 110 001, India
Mobile: +91 9891427685
Board Tel: +91 11 66782480
General Fax: +91 11 66782403
www. techlegis.com
Email: salman.waris@techlegis.com

The logos etc. used in the presentation are for information only and not for any commercial exploitation. We do not claim any rights over the same

"This Presentation provides certain general information existing as at the time of production. This Presentation does not purport to identify all the issues or developments pursuant to the transaction. Accordingly, this presentation should neither be regarded as comprehensive nor sufficient for the purposes of decision-making. TechLegis, Advocates& Solicitors does not undertake any legal liability for any of the contents in this presentation. The information provided is not, nor is it intended to be an advice on any matter and should not be relied on as such. Professional advice should be sought before taking action on any of the information contained in it. Without prior permission of TechLegis, Advocates& Solicitors, this document may not be quoted in whole or in part or otherwise referred to in any documents."