Global Cybersecurity Challenges: Is India Prepared -Trilok Chand

AUTHOR BY | AIR CMDE T CHAND (RETD)

Cybersecurity Awareness in India The Internet connects approximately 2.7 billion people around the world. Spread of Internet of things could result in 75 billion devices connected to the web by 2020i. India is recording the fastest growth for internet usage. It is the third largest user of the Internet and the numbers are likely to increase exponentially with the implementation of the Digital India Programme. Indians are believed to be generally aware of the need for security of their assets and invest in multiple types of antivirus softwares. The government as well as private organisations have evolved several measures. In addition, the Digital India Programme is likely to create a better eco system for cybersecurity in India.

Manifested Cybersecurity Challenges

Cybersecurity is a major concern, as attackers require a small investment and operate under a cover of anonymity. It offers an easy method to potentially cripple industry, academia, government, as well as the military in the domains of air, land, maritime, and space. It is hence emerging as an important tool in both irregular and conventional conflicts. Adversaries include both state and non-state actors, ranging from amateur to highly trained professional hackers. Cybersecurity concerns have reached such dimensions that in September 2015, in a summit meeting, US and China signed an agreement stating that neither government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantageii.

In the recent past, the US had planned to carry out a massive cyberattack on Iran's nuclear and infrastructure facilities in case of failure of the nuclear deal negotiationsiii. The plan codenamed Nitro Zeus was intended as a follow-up to Olympic Games, the code name of a cyberattack carried out jointly by the US and Israel that destroyed 1,000 centrifuges and temporarily disrupted production at Iran's uranium enrichment facility at Natanz. Iran on its part had employed its Revolutionary Guards for siphoning off several million dollars from 50 US banks from 2011 to 2013 and had gained access to the SCADA system of a dam in Manhattan, which could have

imperiled public safetyiv. Seven Iranian firms were indicted in the US on 24 Mar 2016 for cyber crimes.

A recently published report by data-mining experts from the University of Maryland and Virginia Tech ranks India among the nations most vulnerable to serious cyberattacksv. Denmark, Norway and Finland were ranked among the best protected and the US was ranked the 11th safest of the 44 nations studied. Cyberattacks on India have increased from about 13,000 in 2011 to more than 70,000 by the end of 2015. Most attacks are reported to be originating from countries such as China, Pakistan, Bangladesh, Turkey, Algeria, UAE, Brazil, US, and Europe. A high-profile cyberattack on 12 July 2012 breached the email accounts of about 12,000 people, including officials from the Ministry of External Affairs (MEA) and Ministry of Home Affairs (MHA)vi.

Potential Global Cybersecurity Challenges

Deepweb

The deepweb, deepnet, invisible web or hidden web is a part of the World Wide Web whose contents are not indexed by standard search engines for different reasons. The portion of the web that is indexed by standard search engines is known as the surface web. The deep web also includes many common uses such as web mail, online banking and video on demand. The first conflation of the terms deepweb and darkweb came about in 2009. Early estimates suggested that the deepweb is 400 to 550 times larger than the surface web. Deepweb is growing exponentially. Most of the web's information is inaccessible. Traditional search engines cannot see or retrieve contents in the deepweb due to several technical reasons.

Inabilities of Traditional Search Enginesvii

Contextual Web: Pages with content varying for different access contexts e.g., ranges of client IP addresses or previous navigation sequence.

Dynamic content: Dynamic pages which are returned in response to a submitted query or accessed only through a form, especially if open-domain input elements such as text fields are used; such fields are hard to navigate without domain knowledge.

Limited access content: Sites that limit access to their pages in a technical way e.g., using the Robots Exclusion Standard or CAPTCHAs, or no-store directive which prohibit search engines from browsing them and creating cached copies.

Non-HTML/text content: Textual content encoded in multimedia image or video files or specific file formats not handled by search engines.

Private Web: Sites that require registration and login, i.e. password-protected resources.

Scripted content: Pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.

Software: Certain content is intentionally hidden from the regular Internet, accessible only with special software.

Unlinked content: Pages which are not linked to by other pages, which may prevent web crawling programmes from accessing the content.

Deepweb Search Engines

Some of the Deepweb search engines are: The WWW Virtual Library, Deep Web Research Tools, Surfwax, IceRocket, Stumpedia, Freebase and TechDeepWeb.

Darkweb

The darkweb forms a small part of the deep web, the part of the web not indexed by search engines, although sometimes the term deepweb is confusingly used to refer specifically to the darkweb. The darknet which constitute the darkweb include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Freenet, I2P, and Tor, operated by public organizations and individuals. Users of the darkweb refer to the regular web as the Clearnet due to its unencrypted nature. The Tor darkweb is often referred to as onionland, a reference to the network's top level domain suffix.onion and the traffic anonymisation technique of onion routing.

Web based Hidden Services in January 2015viii

A large number of services provided by the darkweb are tabulated below.

Category	Percentage
Gambling	0.4
Guns	1.4

Chat	2.2
New	2.2
(Not yet indexed)	
Abuse	2.2
Books	2.5
Directory	2.5
Blog	2.75
Porn	2.75
Hosting	3.5
Hacking	4.25
Search	4.25
Anonymity	4.5
Forum	4.75
Counterfeit	5.2
Whistleblower	5.2
Wiki	5.2
Mail	5.7
Bitcoin	6.2
Fraud	9
Market	9

Drugs 15.4

Drug traffickers make maximum use of the darkweb. Botnets, Bitcoins services, Dark net markets, Hacking groups and services, Fraud services, Hoaxes and unverified content, Phishing and Scams and Terrorism are the prominent contents of the darknetix. Some of the Darkweb search engines are: Onion.City, Onion.to, Not Evil, Memex Deep and Web Search Engine.

Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization that is responsible for coordinating the maintenance and methodologies of several databases, with unique identifiers, related to the namespaces of the Internet - and thereby, ensuring the network's stable and secure operation. Much of its work pertains to the Internet's global Domain Name System (DNS). The numbering facilities ICANN manages include the Internet Protocol address spaces for IPv4 and IPv6, and assignment of address blocks to regional Internet registries. ICANN also maintains registries of Internet protocol identifiers and performs the actual technical maintenance work of the central Internet address pools and DNS Root registries.

ICANN was incorporated on September 30, 1998 in the State of California. It is headquartered in the Playa Vista section of Los Angeles, California. Reportedly, there are criticisms from ICANN constituencies including the Noncommercial Users Constituency (NCUC) and the At-Large Advisory Committee (ALAC) that there is not enough public disclosure and that too many discussions and decisions take place out of the public sight.

Proposal for Internet Governance by the UN

During a summit meeting of India, Brazil, and South Africa (IBSA) held in September 2011, it was sought to move Internet governance into a UN Committee on Internet-Related Policy (UN-CIRP)x. The move was a reaction to a perception that the principles of the 2005 Tunis Agenda for the Information Society have not been met. The statement called for the creation of a new political organization operating under the auspices of the United Nations to provide policy recommendations for the consideration of technical organizations such as ICANN and international bodies such as the ITU.

Multi Stakeholder Approach

The Multi Stakeholder Approach is a plan for international governance of the Internet that was first proposed at the Global Multi stakeholder Meeting on the Future of Internet Governance (GMMFIG) conference (23–24 April 2014) and later developed into the NetMundial Initiative by the ICANN CEO along with representatives of the World Economic Forum (WEF) and the Brazilian Internet Steering Committeexi. The meeting produced a nonbinding statement in favor of consensus-based decision-making by the stake holders.

Multilateral Management

A few governments, including Russia, China, Iran and India, were unhappy with the final resolution and wanted multi-lateral management for the Internet, rather than broader multi-stakeholder management. But the Panel on Global Internet Cooperation and Governance Mechanisms (convened by the ICANN and the World Economic Forum (WEF), supported and included the NetMundial statement in its own report. In June 2014, France strongly opposed ICANN, stating that ICANN is not a fit venue for Internet governance and that alternatives should be soughtxii.

Cyber Warfare and Capabilities

Cyber Warfare Defined

Cyberwarfare is defined as actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption. Other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, and transnational criminal organizations. Cyberwarfare utilises techniques of defending and attacking information and computer networks connected to cyberspace, often through a prolonged cyber campaign or a series of related campaigns. It denies an opponent's ability to do the same, while employing technological instruments of war to attack his critical computer systems. Many countries have made Cyberwarfare capability development an integral part of their overall military strategy.

China

China is believed to be using Microsoft source code to build its offensive and defensive capabilities. It is also believed to use a network of its students, businessmen, scientists, diplomats, and engineers from within the Chinese diaspora. China is generally considered responsible for a number of cyber-attacks on a number of public and private institutions in the US, India, Russia,

Canada, and France, but the Chinese government denies any involvement in these activities. The PLA is reportedly using information warfare units to develop viruses to attack enemy computer systems and networks. These units include civilian computer professionals.

On 23 Mar 2016, Chinese national Su Bin, 50, pleaded guilty in a California federal court for conspiring with two unnamed persons in China from October 2008 to March 2014 to gain unauthorized access to the computer networks of defense firms to obtain sensitive military information and to export that information illegally from the US to China. Mr. Bin had earlier been charged in a 2014 indictment with hacking into the computer networks of Boeing and other contractors, as part of a scheme to steal plans for the F-22 and F-35 fighter aircraft and C-17 transport aircraft.

A report by the cybersecurity firm Mandiant has estimated the PLA Cyber Command to have 130,000 personnel divided between its various operational divisions. On 1 February 2016, China announced its biggest military reform since the 1950s, including the creation of a Strategic Support Force. According to observers, the SSF will form the core of China's information warfare force and its specific missions will include target tracking and reconnaissance, daily operation of satellite navigation, operating Beidou satellites, managing space-based reconnaissance assets, and attack and defence in the cyber and electromagnetic spaces.

USA

Cyberwarfare is a part of the US's military strategy of proactive cyber defence and the use of cyberwarfare as a platform for attack. In 2009, President Barack Obama declared the US digital infrastructure to be a strategic national asset, and in May 2010 the Pentagon set up its new US Cyber Command (CYBERCOM), to defend their military networks and attack other countries' systems. CYBERCOM is reportedly building a Cyber Mission Force of 133 teams, selected from 6,200 personnel from across the military departments and defence establishments. The Cyber Mission Force, which is expected to be fully operational in 2018, is believed to be employing capabilities across the spectrum of cyber operationsxiii. The Pentagon is likely to spend a total of $6.7 billion on cyberwarfare capability building in 2017. In all, the Pentagon is projected to spend $34.6 billion over the next five years for this purpose.

During the last week of February 2016, Secretary of Defence Ashton Carter told a House subcommittee that CYBERCOM was conducting offensive operations against the Islamic State.

This signaled a shift in the fight against the Islamic State and acknowledged the undertaking of cyberattacks during armed conflict by the US.

Russia

It has been claimed that Russian security services organized a number of denial of service attacks as a part of their cyberwarfare against other countries. Most notably, the 2007 cyberattacks on Estonia and the 2008 cyberattacks on South Ossetia, Georgia, and Azerbaijan caused a major disruption. In March 2014, a Russian cyberweapon called Snake or "Ouroboros" is reported to have created havoc on Ukrainian government systems.

India's Preparations

Cyber Security Policy of India

The cybersecurity policy of India, issued in 2013, outlines a mission to protect information and infrastructure in the cyberspace, build capabilities to prevent and respond to cyber-threats, reduce vulnerabilities and minimise damage from cyber-incidents through a combination of institutional structures, people, processes, technology and cooperationxiv.

The amended IT Act, 2008 describes the Indian Computer Emergency Response Team (CERT In) as the designated national agency to perform all important functions in the area of Cyber Securityxv. Rendering advice on proactive cyber activities also forms a part of the charter of the CERT In. Important virus alerts are issued by this organization: on 25 Feb 2016, the CERT In issued a notification regarding the existence and modus operandi of a virus named Ransomeware Locky which is injected through spam mails. It encrypts the files of the victim, and demands payment through Bitcoins for their de-cryption.

In 2011, the Indian Government created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to protect energy, transport, banking, telecom, defence, space and other sensitive areas. India now has its first National Cyber-Security Coordinator (NCSC), a position created to coordinate among all cyber agencies in the country. Experts are being recruited for cybersecurity research and development work. A few IITs could also become Centers of Excellence for cybersecurity technology development.

Cybersecurity Organisations

The important national cybersecurity organizations in India are: National Information Board, National Security Council Secretariat (NSCS), National Crisis Management Committee, National Cyber Response Centre, National Technical Research Organisation (NTRO) (includes the National Critical Information Infrastructure Protection Centre), National Disaster Management Authority (NDMA), National Cyber Security and Coordination Centre and National Intelligence Grid (NATGRID)xvi. Governance function is also carried out by the Ministries of Home Affairs, External Affairs, Defence and Communications & Information Technology. A Joint Working Group has been created among these ministries to coordinate internet governance policies. The NSCS is the nodal agency for cyber security and internet governance in India.

Prime Minister Narendra Modi on 01 March 2015 advised the National Association of Software and Services Companies (NASSCOM) to create a Cyber Security Task Force (CSTF), with the aim to develop and provide cyber security solutions to the Indian and global markets. Consequently, NASSCOM along with the Data Security Council of India (DSCI) created a task force comprising of leaders from the IT industry, security product companies, and enterprises like banking, telecom, energy sector and senior officers from the government. The vision of the task force is to build the cybersecurity industry up from the current one percent to ten percent by 2025, build a trained base of one million certified and skilled cybersecurity professionals and come up with more than a hundred successful security product companies from India, thus making it a global leader in the cybersecurity space by 2025. Several other private initiatives and blogs such as Perry4Law are also contributing to cybersecurity in India.

Cyber-Security Agency/Command of India

Cybersecurity is given a high priority in the Defence Forces. Personnel are sensitised periodically about the development in this field. An air gap is maintained between the computers hosting sensitive information and the internet connected computers. Procedural controls for keeping pen drives etc away from the sensitive areas are exercised. Breaches in cyber security are treated very seriously. However, despite the heightened cybersecurity awareness, there are growing concerns that our military establishments could be breached by organised cyberespionage.

The Indian Defence Forces are steadily moving towards Network Enabled Operations, and cyberspace forms the backbone of the system. A dedicated cybersecurity ecosystem is essential for unhindered operations in this architecture. There is an urgent need for further tightening of the cybersecurity network mechanism in the country to obviate the security threat inherent in cyberattacks.

In 2012, the Chiefs of Staff committee recommended the urgent formation of a Cyber Command along with Space and Special Forces Commands. India is now in the process of creating the Defence Cyber Agency (DCA) which could be a precursor to the creation of the Defence Cyber Command, like the one in the US. The DCA is likely to be headed by a two star general. Reportedly, the plan is to upgrade and expand the existing Defence Information Assurance and Research Agency (DIARA) into the DCA. Since the stakes are high, India is required to invest more in enhancing cybersecurity awareness, training and ecosystem improvements. It is essential to build our cyberwarfare capabilities, and to have a Defence Cyber Agency/Defence Cyber Command in place on priority for this purpose.

Recommended Approach for India

Enhanced Awareness: Cybersecurity issues affect computers and networks in a stealthy manner. A well informed user can help in early detection and mitigation of a threat. A periodic awareness campaign by the government and other big players- something like road safety week or fire safety week campaigns, should be extended for cybersecurity awareness also.

Cyber Security Training: Cybersecurity training would enhance awareness and provide deterrence. Training capsules at all levels- schools, colleges, workplaces should be periodically conducted.

Eco-System Improvements: These improvements will create a better and safer environment for internet and social media functioning. Indian efforts for freeing ICANN from vested interests could contribute to a better ecosystem. Safe and secure gateways and networks at the national level are essential. Encryption will further help secure the system.

Cyber Warfare Capability: India has centres of excellence in various cybersecurity related areas. There is a plethora of organisations dealing with various aspects of cybersecurity. None of these organisations however, seems to be dealing with aspects of cyber warfare. Concerted efforts at the national level are needed for building up the cyber warfare capability in India.

Defence Cyber Agency/Command: A central organization; oriented, equipped, manned and trained towards cyber war fighting is needed to ensure that all aspects of cybersecurity are adequately addressed. A Defence Cyber Agency/Command can serve this purpose and should be raised without further delay.

i. Segal, Adam. "The Hacked World Order." CFR.org. Council on Foreign Relations, 23 Nov. 2015. Web. 27 Feb. 2016.

ii. Segal, Adam . “The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement”. CFR.org. Council on Foreign Relations, 4 Jan. 2016. Web. 27 Feb 2016.

iii. David E. Sanger and Mark Mazzettifeb. “The New York Times”. 16 Feb. 2016. Web. 17 Feb. 2016.

iv. Tom Winter and Tracy Connor. Iranians Charged With Cyber Attacks on U.S. Banks, Dam. 24 Mar. 2016. NBC News. Web nbcnews.com/news/us-news/iranians-charged-hacking-attacks-u-s-banks-dam-n544801.

v. India among nations most vulnerable to cyberattacks. The Economic Times. 10 Mar.2016. Web. articles.economictimes.indiatimes.com/2016-03-10/news/71382331_1_researchers-machines-other-nations.

vi. Trilok Chand and Aastha Vatsyayan. Walls of Fire. Force. April 2016 Issue. Web. forceindia.net/WallsofFire.aspx.

vii. Deep Web. Content Types. Web. en.wikipedia.org/wiki/Deep_web.

viii. Owen, Gareth. "Dr Gareth Owen: Tor: Hidden Services and Deanonymisation". Retrieved 20 June 2015.

ix. Mark, Ward (30 December 2014). "Tor's most visited hidden sites host child abuse images". BBC News. Retrieved 28 May 2015.

x. "Recommendations from the IBSA (India-Brazil-South Africa) Multistakeholder meeting on Global Internet Governance", 1–2 September 2011, Rio de Janeiro, Brazil.

xi."Future of the internet debated at NetMundial in Brazil". BBC News. 2014-04-23. Retrieved2014-06-02.

xii. "France attacks ICANN as unfit for internet governance". Yahoo! News. Agence France-Presse. 25 June 2014. Retrieved 20 September 2014.

xiii. The White House Office of the Press Secretary https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

xiv. National Cyber Security Policy – 2013. http://deity.gov.in/content/national-cyber-security-policy-20131

xv. Indian Computer Emergency Response Team (CERT In.http://www.cert-in.org.in/

xvi. Arun Mohan Sukumar and Col. R.K. Sharma. The Cyber Command: Upgrading India's national security architecture. ORF Issue Briefs and Special Reports. 03 Mar.2016. Web. orfonline.org/research/the-cyber-command-upgrading-indias-national-security-architecture/