MEMBERS' REFERENCE SERVICE

LARRDIS

LOK SABHA SECRETARIAT, NEW DELHI

REFERENCE NOTE

**No.35/RN/Ref./July/2017**

**For the use of Members of Parliament** **NOT FOR PUBLICATION**

# CYBER WARFARE AND NATIONAL SECURITY CHALLENGES

*Prepared by Smt. Neelam Sethi, Additional Director and Shri Abhishek Thakur, SLA of Lok Sabha Secretariat under the supervision of Shri Atul Kaushik, Additional Secretary, Smt. Kalpana Sharma, Joint Secretary and Shri C.N. Sathyanathan, Director.*

*The Reference Note is for personal use of the Members in the discharge of their Parliamentary duties, and is not for publication. This Service is not to be quoted as the source of information as it is based on the sources indicated at the end/in the text.*

# Cyber Warfare and National Security Challenges

## Introduction

*"Cyber[1] warfare"* is an extension of policy by actions taken in cyber space by state or no state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security. It is mainly an Internet-based conflict involving politically motivated attacks on information and information systems. Cyber attacks[2] can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities[3].

## Background

Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. It has also created new vulnerabilities and opportunities for disruption. The cyber security

[1] "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. Common usages include cyber culture, cyberpunk, and cyberspace.

[2] The Morris worm was the first recognised worms to affect the world's nascent cyber infrastructure -spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris (http://www.nato.int/docu/review/2013/cyber/Cyberwar-does-it-exist/EN/index.htm)

[3] http://searchsecurity.techtarget.com/definition/cyberwarfare.

threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. Today, cyber security threats pose one of the most serious economic and national security challenges[4].

**Ecosystem of Cyber warfare:**

a) *Cyber terrorism*- can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

*b) Cyber Fraud-* Cyber attacks that are generally aimed at getting monetary or related gains for the perpetrators. Phishing attacks combined with fake websites to steal user's personal details and, with these, steal money from their account.

*c) Cyber Spying*- Cyber attacks aimed at gaining information from the perpetrators. Related to cyber fraud in that one aim of cyber spying may be to sell the information gained.

d) *Cyber stalking or Bullying*- Cyber attacks which are designed to frightened and intimidate individuals rather than business or Government. Usually they are social media based- Facebook or Twitter.

[4] http://meity.gov.in/Plan_Report_on_Cyber_Security.pdf

e) *Cyber Assault*- Cyber attacks[5] aimed at causing damage to information or equipment that is being attacked. Damage may be physical damage or deletion of important file or information.

India ranks among the top 5 countries at risk for cyber attacks in 2016.

| **Cyber Attacks-Most vulnerable countries 2016** | | | |
|---|---|---|---|
| *Top Five Countries with High risk of Cyber Attacks* | | *Top Five Countries with Low risk of Cyber Attacks* | |
| *Countries* | *Risk %* | *Countries* | *Risk%* |
| Algeria | 30.7 | France | 5.2 |
| Bolivia | 20.3 | Canada | 4.6 |
| Pakistan | 19.9 | Australia | 4.1 |
| China | 18.5 | United States | 3 |
| **India** | **16.9** | Britain | 2.8 |

*www.businessinsider.in*

### Cyber warfare Threat to Indian Defence Sector and challenges

The Minister of Defence, Shri Manohar Parrikar in a reply to a starred Question in Lok Sabha stateed that Cyber-crime has emerged as one of the foremost security threats at global level including at the national level. Since armed forces function on exclusive private networks, these establishments have not witnessed institutional attacks. Cyber attacks are largely faced by internet connected Personal Computers (PCs) and these relates to unauthorized data access, malware infestation, denial of service, etc[6].

[5] Annexure-I Major cyber attacks events around the world

[6] Lok Sabha, Starred Question No. 400, 12 August 2016

Cyber threats like espionage and Denial of Service (DoS) attacks to offensive actions by adversarial State and Non-State actors. Several countries are developing sophisticated malicious codes as lethal cyber weapons. Large scale mapping of SCADA (Supervisory Control and Data Acquisition) devices using specialized tools, pose major challenge for any country.

## Cyber related Crimes in India

i) Cyber crime data by **National Crime Records Bureau** (NCRB)[7]

| Year | Cases | Cyber Crime |
|---|---|---|
| 2013 | 5,693 | *Identity theft, phishing, obscene publication/ transmission in electronic form, cyber forgery and cyber frauds.*<br>A total of 95 persons have been convicted for Cyber Crimes during 2014 |
| 2014 | 9,622 (69% rise) | |
| 2015 | 11,592 (20% rise) | |

ii) Information reported to and tracked by, ***Indian Computer Emergency Response Team (CERTIn)***

| *Year* | *Cases* | Types of Cyber Crime |
|---|---|---|
| 2014 | 44679 | Including phishing, Scanning, Malicious code, Website intrusion, Denial of Service etc |
| 2015 | 49455 | |
| 2016 | 50362 | |
| *Year* | *Cases* | |
| 2014 | 85659 | Unsolicited e-mails |
| 2015 | 61628 | |
| | | |
| 2014 | 155 | Government websites were hacked |
| 2015 | 164 | |

[7] Rajya Sabha, Unstarred Question- Q No.244, 3 February 2017

iii) Data made available by ***Reserve Bank of India (RBI)***,

| *Year* | *Cases* | Types of Cyber Crime |
|---|---|---|
| 2013-14 | *9500* | |
| 2014-15 | 13083 | Cases related to ATM/ Credit/ Debit Cards & Net Banking frauds were reported by the banks. |
| 2015-16 | 16468 | |
| 2016-17 upto December 2016 | 8689 | |

**Cyber Security Challenges-** *Outlined By the Department of Electronics & Information Technology (DeitY)*[8]

The Department of Electronics & Information Technology (DeitY) has outlined the following as the main issues and challenges observed in the cyber space:-

- Lack of adequate human resource to tackle the challenge (Auditors, Experts, Skill development in IT)
- Infrastructure and Research and Development to secure Cyber Space
- Budgetary allocations to tackle the Cyber threats
- Threat emerging from servers hosted outside India
- Challenge posed by imported electronics/IT products
- Upcoming technology viz. Cloud Computing, Big data, Internet of Things(IoT) etc.
- Balance between Cyber Security and Right to Privacy

[8] Op.cit., 52nd Report on Cyber Crime. P.13

- Expanding role and implementation of Information Technology across all sectors in the country
- Growth in volume and complexity of Information Technology ecosystem in the country
- Growth in volume of transactions and sensitive data exchange
- Rapidly changing security and threat landscape
- Difficulty in tracing origin of attack
- Need for reducing cyber security risk exposure of IT infrastructure and ecosystem in the country
- Responsibility to ensure that proper processes, technology, governance structure and compliance to laws and regulatory requirements are followed in a borderless environment

Defending borderless environment poses challenges which are dynamic in nature.

## Cyber Security Measures taken by the Indian Government[9]

India is gearing up to bring in new encryption and privacy policies to take on growing cyber security challenges. It may also amend the existing laws to make cyberspace more secure. India has taken steps in establishing institutions and released the National Cyber Policy in 2013 to deal with cyber security issues. In recent times, India has launched a series of cyber security initiatives to digitally empower its citizens and safeguard cyberspace. In the wake of increasing cyber threats, India appointed its first chief information security officer (CISO). The appointment underlines India's commitment to combating cyber attacks. It will help India develop the vision and policy to fight cybercrime and manage cyber security more effectively.

[9] Rajya Sabha- Q. No. 3454 (16-12-2016)

(a) Government has taken a number of legal, technical and administrative policy measures for addressing cyber security. This includes National Cyber Security policy (2013), Framework for enhancing Cyber Security (2013), enactment of Information Technology (IT) Act, 2000 and setting up of Indian Computer Emergency Response Team[10] (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, 2000.

(b) Government has taken various steps in the form of legal framework, emergency response, awareness, training and implementation of best practices to tackle cyber security. Such steps include

i) The Information Technology (IT) Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

ii) Government is implementing a Framework for Enhancing Cyber Security, with a multilayered approach for ensuring defence-in-depth and clear demarcation of responsibilities among the stakeholder organizations in the country.

iii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the IT Act, 2000 for protection of Critical Information Infrastructure in the country.

iv) With respect to the banking sector, in order to focus more attention on IT related matters, Reserve Bank of India has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. The Bank has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of

[10] The constituency of CERT-In is the Indian Cyber Community. It's a nodal agency for responding the computer security incidents as and when they occur. CERT-In is operational since January 2014.

cyber security. The circular requires banks to have among other things, a cyber-security policy, cyber crisis management plan, a gap assessment vis-à-vis the baseline requirements indicated in the circular, monitoring certain risk indicators in the area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

v) RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents. Department of Banking Supervision also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.

vi) RBI also has set up an IT subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities. The subsidiary is in the process of recruiting the experts.

vii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out. CERT-In has issued 372, 402 and 432 advisories during 2014, 2015 and 2016 respectively.

viii) Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

ix) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 11 such drills have so far been conducted by CERT-In where 110 organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Spaces and IT/ITeS participated.

x) Government is setting up of National Cyber Coordination Centre (NCCC)[11] to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

xi) Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.

xii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

xiii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

[11] NCCC- The Expert Group constituted in the Ministry of Home Affairs to prepare a roadmap for effectively tackling cyber crimes in the country has recommended to set up an Indian Cyber Crime Coordination Centre (I4C) to fight against cyber crimes in the country.

xiv) Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. In Academia National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

xv) A number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.

xvi) CERT-In and Centre for Development of Advanced Computing (C-DAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

xvii) Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.500 Crores has been allocated for Ministry of Electronics and Information Technology (MeitY) in the 12th Plan period (2012-17) for Cyber Security Programme including Cyber Safety, Security and Surveillance, Cyber Crime Investigations and Cyber Forensics

xviii) National Cyber Security policy (NCSP, 2013) provides for creation of a workforce of 5 lakh cyber security professionals in the next five years through capacity building, skill development and training

xix) To protect important and confidential data of Defence Sector from cyber attack threat, the operational networks of the Armed Forces are air gapped from internet. Further, Defence Services have established Cyber Emergency Response Teams (CERTs) to prevent and react to cyber attacks. Safeguards have been instituted in the form of audits and physical checks. Policies, guidelines and procedures have been laid down and periodic cyber security advisories are issued[12].

xx) Government is implementing "Information Security Education and Awareness (ISEA)' project to train professionals / government officials and create mass information security awareness among citizens. The Project is implemented by 51 institutions across the country. 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security till 2016.

xxi) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 18 such training programs were conducted covering 580 participants during the year 2016. In addition a workshop on security of digital payments systems has been conducted for stakeholder organisations covering 110 participants.

xxii) Currently 24 security auditing organizations are empanelled to support and audit implementation of Information Security Best Practices. NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place.

xxiii) NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems and anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardening.

[12] Lok Sabha, Starred Question.No. 400, 12 August 2016

These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently. A 24x7 security monitoring centre is in place at NIC for detecting and responding to security incidents. Restoration is done after detected incident is analysed and necessary remedial measures are taken.

### *International Collaboration on Cyber Security*[13]

i. India and the U.S. agreed to cooperate on cyber security issues. As a part of the U.S.-India Cyber Relationship Framework, both countries agreed to share cyber security best practices, share threat information on a real-time basis, promote cooperation between law enforcement agencies and encourage collaboration in the field of cyber security research. India and the U.S. will also establish joint mechanisms to mitigate cyber threats and protect internet infrastructure and information.

ii. In 2015, India and the U.K. made a joint statement about cooperation in the cyber security space. The two countries agreed to work together to provide professional development and establish a Cyber Security Training Centre of Excellence. The U.K. also agreed to help launch the proposed National Cyber Crime Coordination Centre in India.

iii. India has entered into cyber security cooperation with European Union and Malaysia

iv. India and Japan are collaborating on cyber security in the form of Memorandum of Understanding (MoU) signed between CERT-In and Japan-CERT in 2015 for exchange of information on latest threats and vulnerabilities and mitigation strategies to cyber-attacks.

[13] Ministry of Electronics & Information Technology

There is a strong case for India to collaborate with more countries, but in the meantime, these partnerships are a great foundation.

### UN cyber security index 2017:

India has been ranked ***23rd*** among 165 countries by United Nations global cyber security index – measuring country's commitment to cybersecurity – in the "maturing" category between the 50th and 89th percentile. The "maturing stage" refers to the 77 countries that have developed complex commitments, and engage in cybersecurity programmes and initiatives. With higher score 0.683 India ranks one stop higher than Germany, which has scored 0.679 while China is nine spots below India.

**Conclusion**

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. The day is not far when terrorists themselves will cause large-scale cyber incidents as they have already graduated from defacing websites to causing real damage to their "enemies," especially their critical infrastructure. This will change the entire landscape of terrorism. A common vision is required to work internationally to ensure cyber security and prevent cyber war and cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy.

### Cyber Europe 2016

*On 14th October,2016, EUROPE concluded six months long 'Biggest ever' pan-European cyber-security exercise on. Engaging 28 EU Member States plus Switzerland and Norway, the fourth annual exercise involved thousands of cyber-security experts. It was was inspired by threats to critical national infrastructure (CNI), the internet of things (IoT) and cloud computing, using threat vectors as diverse as drones, innovative ex filtration methods, mobile malware and ransomware. The motto of the exercise is "Stronger Together" and the key to success is cooperation at all levels to stymie transnational threats.*

## *Ransomware attack*

*On 16th May 2017 the WannaCry ransomware attack hit about 150 countries globally, including Russia and the US. In India, five or six isolated instances were reported in States like Gujarat, Kerala and West Bengal; though any substantial disruption to country's IT backbone was denied by the IT Secretary Aruna Sundararajan.*

## ***Events of Cyber Attacks***

- In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world.
- In October 2010, "*Stunext"* a complex piece of malware designed to interfere with Siemens industrial control systems was discovered in Iran and Indonesia leading to speculation that it was a government cyber weapon aimed at Iranian Nuclear programme
- July 2011, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.
- In October 2012, the Russian firm Kaspersky discovered a worldwide cyber-attack dubbed “Red October,” that had been operating since at least 2007.The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.
- In a major Cyber-attack in 2012, hackers advertised details of 117 million LinkedIn users on darknet.
- In 2016 Maharashtra Government claimed that railways IRCTC website has been hacked.
- On 2nd January,2017 India's elite National Security Guard (NSG) website claimed to be hacked by the Suspected Pakistan-affiliated operatives.

## Glossary of cyber security terms

***Cyber Space*** is a space created not in nature but by human beings, but has the potential for tremendous benefits as well as unknown risks due to the rapid growth in the fields of computing and communications and the ongoing improvement in the performance of computerized systems have created this type of new space in the world.

"***Cyber attack"*** is a relatively recent term that can refer to a range of activities conducted through the use of information and communications technology (ICT). Recent international events have raised questions on when a cyber attack could be considered an act of war, and what sorts of response options are available to victim nations.

***Cyber terrorism*** can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

**"Cyber warfare"** Although there is no clear doctrinal definition of "cyberwarfare," it is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response.

**"Cyber warriors"** are agents or quasi-agents of nation-states who develop capabilities and undertake cyber attacks in support of a country's strategic objectives. These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyber attack and are often blamed by the host country when accusations are levied by the nation that has been attacked.

**"Cyber activists"** are individuals who perform cyber attacks for pleasure, philosophical, political, or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist" such as a member of the cyber-group Anonymous who undertakes an attack for political reasons.