Paper Presentation

Cyber Security Issues and Challenges in India

Y.POORNIMA(Student),Y.NAVEENA(Student) Mr.V.HARSHA VARDHAN(KMM IPS)

Abstract:Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day.Cyber security can be a useful term but tends to defy precise definition. It is also sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance.In this paper the management of risk to information systems is considered fundamental to effective cyber security. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (how they are attacking), and impacts (what the attack does).The government role in cyber security involves both securing government systems and assisting in protecting non-government systems.

However, in the context of cyber security prevention it needs more attention to resolve difficult long-term challenges relating to design, incentives, consensus, and environment.

In this paper the Management of Cyber security Risks, government role and Long-Term Challenges are discussed.

Index Terms— Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1.INTRODUCTION

The information technology (IT) industry has evolved greatly over the last half century. Continued, exponential progress in processing power and memory capacity has made IT hardware not only faster, but also smaller, light, cheaper, and easier to use. The original IT industry has also increasingly converged with the communications industry into a combined sector commonly called information and communications technology (ICT). This technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others.

The act of protecting ICT systems and their contents has come to be known as cybersecurity. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It is also sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. However, cybersecurity can be an important tool in protecting privacy and preventing unauthorized surveillance, and information sharing and intelligence gathering can be useful tools for effecting cybersecurity.
The management of risk to information systems is considered fundamental to effective cybersecurity. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts.
The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on cybersecurity.

1.1 The Concept of Cyber security:

Over the past several years, experts and policy makers have expressed increasing concerns about protecting ICT systems from cyberattacks—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years 1. The act of protecting ICT systems and their contents has come to be known as cyber security. A broad and arguably somewhat fuzzy concept, cyber security can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:

- A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software, and the information they contain and

communicate, including software and data, as well as other elements of cyberspace.

- The state or quality of being protected from such threats.
- The broad field of endeavor aimed at implementing and improving those activities and quality.

It is related to but not generally regarded as identical to the concept of information security, which is defined in government law as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-

A. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

B. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information**;**

C. Availability, which means ensuring timely and reliable access to and use of information.

Cyber security is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gath ering, and surveillance. Privacy is associated with the ability of an individual person to control access by others to information about that person. Thus, good cyber security can help protect privacy in an electronic environment, but information that is shared to assist in cyber security efforts might sometimes contain personal information that at least some observers would regard as private. Cyber security can be a means of protecting against undesired surveillance of and gathering of intelligence from an information system. However, when aimed at potential sources of cyberattacks, such activities can also be useful to help effect cyber security. In addition, surveillance in the form of monitoring of information flow within a system can be an important

component of cyber security.

2. MANAGEMENT OF CYBER SECURITY RISKS

The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (how they are attacking), and impacts (what the attack does). The management of risk to information systems is considered fundamental to effective cyber security.

2.1 What Are the Threats?

People who perform cyberattacks generally fall into one or more of five categories: criminals intent on monetary gain from crimes such as theft or extortion; spies intent on stealing classified or proprietary information used by government or private entities; nation-state warriors who develop capabilities and undertake cyberattacks in support of a country's strategic objectives; ―hacktivists who perform cyberattacks for nonmonetary reasons; and terrorists who engage in cyberattacks as a form of non-state or state-sponsored warfare. 2.2 Final Stage.

2.2 What Are the Vulnerabilities?

Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix.

2.3 What Are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. Cyber theft or cyber espionage can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system for use in cyberattacks on other systems. Attacks on industrial control systems can result in the destruction of the equipment they control, such as generators, pumps, and centrifuges.

Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.

Reducing the risks from cyberattacks usually involves (1) removing the threat source (e.g., by closing down botnets or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) lessening impacts bymitigating damage and restoring functions (e.g., by having back-up resources available for continuity of operations in response to an attack).

3.GOVERNMENT ROLE

The government role in cyber security involves both securing government systems and assisting in protecting non government systems. Under current law, all government departments have cyber security responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (Deity), Ministry of Communication and Information Technology, Government of India. It aims at protecting the public and private

infrastructure from cyber attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

The National Cyber Security Policy of India 2013 is suffering from various shortcomings and limitations as per various studies and researches. Despite the declaration of the policy, India is still not cyber prepared. The policy has also not been implemented till the month of November 2014 (till 21 November 2014). The cyber security challenges in India would increase further and immediate action is required in this regard. The proposed initiatives like National Cyber Coordination Centre and National Critical Information Infrastructure Protection Centre (NCIIPC) of India could prove useful in strengthening Indian cyber security and critical infrastructure protection in India.

3.1The Indian Cyber Space:

The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of Online attacks In India National Informatics Centre's were setup in year 1975 to provide various IT related solutions to the government. There were three major networks were setup at that time.

(a) INDONET:- It connects IBM mainframes that made up India's computer infrastructure

(b) NIC NET: It a NIC Network for public organizations that connects Central government with the state, and district administrations.

(c) ERNET: - It is an Education Research Network to serve the academic and research communities. who perform cyberattacks for nonmonetary reasons; and terrorists who engage in cyberattacks as a form of non-state or state-sponsored warfare.

3.2 National Security Policy 2013

India had no Cyber security policy before 2013. In 2013, The Hindu newspaper, citing documents leaked by NSA whistleblower Edward Snowden, has alleged that much of the NSA surveillance was focused on India's domestic politics and its strategic and commercial interests. This leads to spark furor among people. Under pressure, Government unveiled a National Cyber Security Policy 2013 on 2 July 2013.

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
- To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.
- To create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training.
- To provide fiscal benefit to businesses for adoption of standard security practices and processes.
- To enable Protection of information while in process, handling, storage & transit so as to safeguard privacycitizen's data and reducing economic losses due to cybercrime or data theft.
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

3.2 What Are the Vulnerabilities?

Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix.

3.3 Existing Counter Cyber Security Initiatives

On the recommendations of ISTF the following initiatives have been taken:

1) Indian Computer Emergency Response Team (CERT-In) has been established to respond to the cyber security incidents and take steps to prevent recurrence of the same.
2) Public Key Infrastructure (PKI) has been set up to support implementation of Information Technology Act and promotes use of Digital signatures.
3) Government has been supporting R&D activities through premier Academic and Public Sector Institutions in the country.

Some of the other initiatives that can be taken:

a. National Informatics Centre (NIC).

A premier organization providing network backbone and e-governance support to the Central Government, State Governments, Union Territories, Districts and other Governments bodies. It provides wide range of information and communication technology services including nationwide communication Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

b. Indian Computer Emergency Response Team (Cert-In)

Cert-In is the most important constituent of India's cyber community. Its mandate states, 'ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance

c. National Information Security Assurance Program (NISAP).

This is for Government and critical infrastructures, Highlights are:

(a) Government and critical infrastructures should have a security policy and create a point of contact.
(b) Mandatory for organizations to implement security control and report any security incident to Cert-In.
(c) Cert-In to create a panel of auditor for IT security.
(d) All organizations to be subject to a third party audit from this panel once a year.
(e) Cert-In to be reported about security compliance on periodic basis by the organizations.

4.LONG-TERM CHALLENGES

The executive-branch actions and proposed legislation are largely designed to address several well-established near-term needs in cyber security: preventing cyber-based disasters and espionage, reducing impacts of successful attacks, improving inter- and intrasector collaboration, clarifying federal agency roles and responsibilities, and fighting cybercrime. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment (DICE):

Design: Experts often say that effective security needs to be an integral part of ICT design. Yet, developers have traditionally focused more on features than security, for economic reasons. Also, many future security needs cannot be predicted, posing a difficult challenge for designers.

Incentives: The structure of economic incentives for cyber security has been called distorted or even perverse. Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cyber security can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure.

Consensus: Cyber security means different things to different stakeholders, with little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations.

Environment: Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics.

5.Fedaral role:

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity.

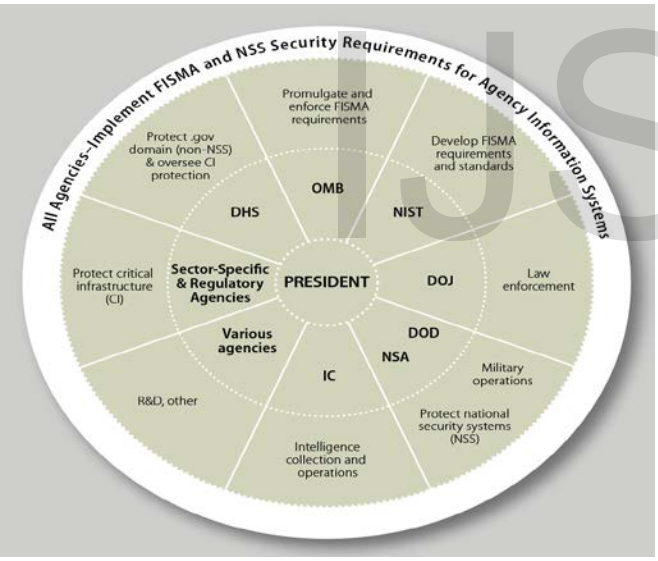
The following diagramis a simplified schematic diagram of major agency responsibilities in cybersecurity. In general, the National Institute of Standards and Technology (NIST) develops standards that apply to federal civilian ICT under the Federal Information Security Modernization Act (FISMA), and the Office of Management and Budget (OMB) is responsible for overseeing their implementation. The Department of Defense (DOD) is responsible for military ICT, defense of the nation in cyberspace, and, through the National Security Agency (NSA), security of national security systems (NSS), which handle classified information. NSA is also part of the Intelligence Community (IC). The Department of Homeland Security (DHS) has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting CI assets. It is also the main federal focus of information sharing for civilian systems through its National Cybersecurity and Communications Integration Center (NCCIC). The Department of Justice (DOJ) is the lead agency for enforcement of relevant laws.

5.Federal Role

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity.

Figure 1 is a simplified schematic diagram of major agency responsibilities in cybersecurity. In general, the National Institute of Standards and Technology (NIST) develops standards that apply to federal civilian ICT under the Federal Information Security Modernization Act (FISMA), and the Office of Management and Budget (OMB) is responsible for overseeing their implementation. The Department of Defense (DOD) is responsible for military ICT, defense of the nation in cyberspace, and, through the National Security Agency (NSA), security of national security systems (NSS), which handle classified information. NSA is also part of the Intelligence Community (IC). The Department of Homeland Security (DHS) has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting CI assets. It is also the main federal focus of information sharing for civilian systems through its National Cybersecurity and Communications Integration Center (NCCIC). The Department of Justice (DOJ) is the lead agency for enforcement of relevant laws.

5.1 Simplified schematic diagram for federal agency cyber security role's.



In February 2015, the Obama Administration also established, via presidential memorandum, the Cyber Threat Intelligence Integration Center (CTIIC) under the Director of National Intelligence (DNI). Its purposes are to provide integrated analysis on cybersecurity threats and incidents affecting national interests across the federal government entities, including the NCCIC and others at DOD and DOJ.

6.CONCLUSIONS

Although the government has ambitious plans to raise cyber connectivity. There has a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily life activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility. The cyberspace holds the fifth place in common space and it is vital to have co ordinations and cooperation among all nations regarding cyberspace. The need of cyberspace and its exploitation is growing rapidly. The cyberspace is becoming important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cybercrimes and, thus urging a need to modify the existing laws through which these activities can be put on a check. There is a need of international cooperation of nations to crack down the efficiency on cybercrime, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

7.REFERENCES:

[1] "National Cyber Security Policy-2013". Department Of Electronics & Information Technology, Government Of India. 1 July 2013. Retrieved 21 November 2014.

[2] "Amid spying saga, India unveils cyber security policy". Times of India. INDIA. 3 July 2013.

[3] "National Cyber Security Policy 2013: An Assessment". Institute for Defense Studies and Analyses. August 26, 2013.

[4] "For a unified cyber and telecom security policy". The Economic Times. 24 Sep 2013.

[5] "Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity". Stanford Journal of International Law, Vol. 50, p. 119, Winter 2014 Indiana Legal Studies Research Paper No. 290. 15 July 2014.

[6] "Analysis Of National Cyber Security Policy Of India 2013 (NCSP-2013) And Indian Cyber Security Infrastructure". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 21 November 2014.

[7] "Ten things you should know about India's Cyber Security Policy". CXO Today.

[8] "Analysis of National Cyber Security Policy (NCSP–2013)". Data Security Council of India. 15 July 2013.

[9] "The National Cyber Security Policy: Not a Real Policy". ORF Cyber Security Monitor, Volume I Issue 1. 1 August 2013.

[10] "Cyber Security Breaches Are Increasing World Over And India Must Be Cyber Prepared". Perry4Law Organization. 22 May 2014.

[11] "Cyber Security Challenges In India Would Increase". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 18 November 2014.

[12] "National Cyber Coordination Centre (NCCC) Of India May Become Functional". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 20 January 2014.

[13] B. B. Gupta, R. C. Joshi, ManojMisra, ―ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack, International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

[14] Institute for Defense Studies and Analyses, India's cyber security Challenge, First Edition, March 2012.
[15] http://ncrb.nic.in/, ―Cyber Crimes
[16] R. M. Johri Principal Director (information Systems) Office of CAG of India, ―Cyber Security – Indian Perspective‖
[17] ids.nic.in,SS Raghav ―Cyber Security in India's Counter Terrorism Strategy‖, Col, [accessed on 10 Feb 2015].