A Comprehensive Study of Contemporary Tools and Techniques in the Realm of Cyber Security

Dhananjay*
Aishwarya Raman**
Sheetal Kaushik***

Abstract

The Inherent Weaknesses in the cyber space and ever escalating cyber-attacks tend to continuously threaten the National Security, economy and Privacy. More than fifty countries, around the world, have framed their Cyber Security Strategies to address the serious issues of National Cyber Security. A cyber security strategy is particularly meant to be securing the national cyberspace from malicious cyber threat courses, but due to the unpredictable threat background, considerable variations can be seen in the invasive and defensive actions and methods adopted by different country.

This research paper analysis and Compares Cyber Security tools and techniques, also discusses about developed and developing countries with their identified standards, aims and explanation of cyber awareness, characterization of the cyber threats, and legislative measures, capacity building programs etc. The majority of the strategies have described the need of assigning an official body for leading the cyber security tasks at the national level and establishment of Computer Emergency Response Teams (CERT) to fight cyber-attacks targeting national cyberspace.

Keywords: Cyber Security, Cyber Security Strategies, Cyber Security Measures

I. Introduction

In this digital age Everyone have the facility to send information from one part to the other within a fraction of second and that to with a click of a single button but only a fraction of those who click this button actually knows what is happening behind the scenes. "40 million People who were addicted to Ashley Madison a commercial website had no clue what nightmare they had to face after the cyber-attack by the impact group [1]. This is just one example out of the countless events that has happened in the previous year itself.

Cyber security has been there from quite some time but new and new ways of exchanging information has made older techniques used for securing confidential data obsolete. With crimes like these increasing day by day we need to come up with not just effective but intelligent solutions to safeguard confidential data. In this light we would like to take this opportunity to present our white paper on cyber security and threats. In simple terms cyber security means protecting the network, computer, programs or data from suspicious access. This paper brings forward the different cyber techniques and tools, strategies, ways of detection and the various kinds of cybercrimes. This paper shows a clear picture about various techniques being followed for eg: Authentication, encryption, firewall, digital signatures etc. and various tools such as Forensic Security tools, Vulnerability Scanner etc. This is the representation of the current condition of cyber-attacks in various places across the globe. The status clearly possesses an urgent need for the development of new cyber security techniques.

A. Worldwide Network Attacks Origin by Ranks

This information has been sourced from Symantec. This is a part of worldwide survey conducted in 2014, according to which China and United States remained in the top 2 positions in malicious activities. India

Dhananjay*
BCA Student, Institute of Information Technology and Management, Janakpuri, New Delhi
Aishwarya Raman**
BCA Student, Institute of Information Technology and Management, Janakpuri, New Delhi
Sheetal Kaushik***
Department of IT, Institute of Information Technology and Management, Janakpuri, New Delhi

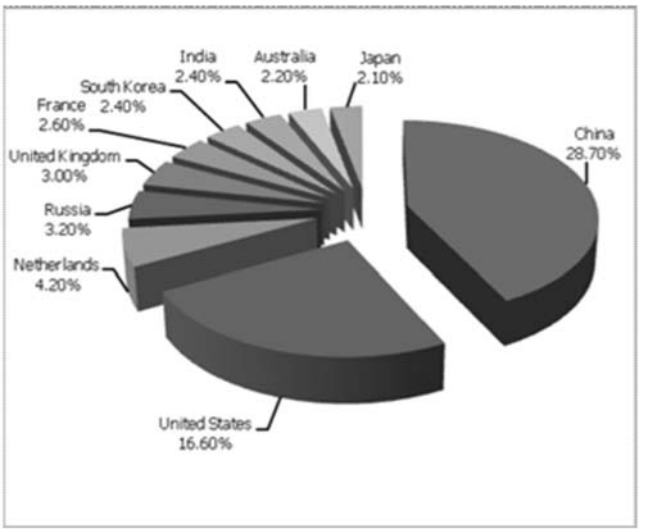


Fig. 1: Worldwide Survey conducted in 2014

remains in the 8th position with least malicious attacks.

B. Top 5 Sectors Breached by Number of Incidents:

The following graph shows the top 5 sectors breached by number of incidents. The maximum breaches happened in health sector while the least in Financial Sector.

C. Incidents of Breach:

The following chart shows the timeline of data breaches that happened globally in 2014. While the maximum incidents numbering 34 happened in march 2014, the maximum identities exposed were 147.62 million in the month of May 2014.

II. Literature Review

With a view to make this research titled "A Comprehensive Study of Contemporary Tools and Techniques in the Realm of Cyber Security" more effective; it is prepared after detailed study of various research papers and journals. Certain facts have been considered. The papers discuss about various cyber-attack detection strategies. In view of the current state of increasing cyber crimes this paper brings forward the need for the development of new cyber-attack detection strategies. This paper also demonstrates about various types of cyber-attacks for eg.:

(a) Denial of service attacks
Dos is basically a kind of cyber-attack where the attacker makes the memory resource too occupied or too heavy thereby limiting the user to use the machine. Here the network connection, or the computers or network may be targeted and prevents the user to legitimate commands [2].

(b) Remote to local(R2L)
In this kind of attack an attacker sends packets to machine over network so that he can illegally access the machine to gain the local access. The attacker usually doesn't have an account on the machine and is able to send the packets to the system. [3]

(c) User to root attacks (U2R)
In this class of attack, the attacker uses the machine normally and is able to exploit the system to gain the root access of machine (sniffing passwords, hacking) [4]

(d) Probing
Probing is a system of gaining access to the computer and files by knowing the weak point in the system i.e. mostly external to the network. [5]

A. Some of the Attack Detection Strategies Include

(a) Intrusion detection strategies: An Intrusion detection is a sort of device that checks the network

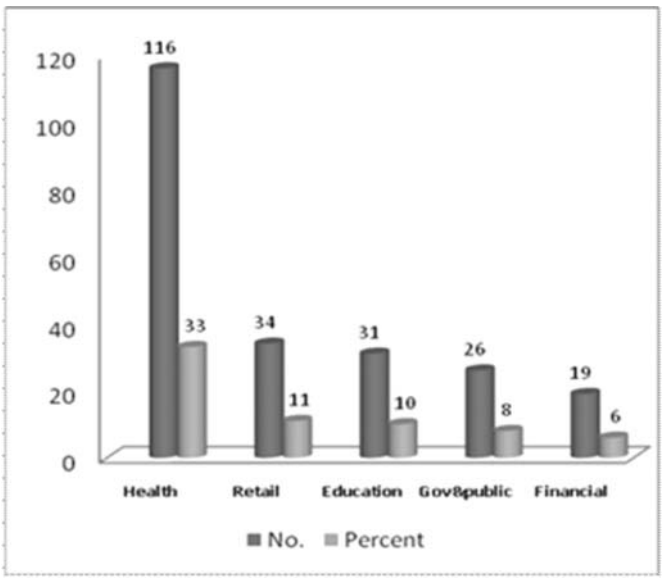


Fig. 2: Number & Percentage in Various Sectors

system for malicious or suspicious activities going in the computer and reports it to the supervision system.

(b) Signature based approach: in this system the server can use existing software like antivirus and firewall, use their properties, inherit them and use in attack signatures in such a way that those signatures that create log files directly saves in the machine [6].

As per the study the analytical view for detecting the cyber-attacks is also very important. One of the major examples is: artificial immune system.

Bio-inspired methods such as artificial immune system gives a new dynamical method to defend entire data network from malicious attacks. It detects the affected cell named as pathogens such as virus and mal virus. Artificial immune system only detects the reactive cell in the system that are affected and process them to protect system data [6]. As much as analytical view is important for detection it is also important to know the classification of cyber-attack and the possible solution to it:

For eg: (1) Cyber Wars in which different nations are involved with the aim of disrupting the network to gain military. (2) Cyber Crimes-it uses computers and internet to abuse the users for monetary gains. One of the Offered solutions to this kind of attacks includes: Agent based approach

III. Cyber Security Techniques and Tools

As per the survey it is founded that Cyber Security are gaining importance because of growing number of unauthorized attempts to rush into private data with the clear aim of stealing the same and forcing the users into information blackmailing. The tools and techniques [7]active to challenge cyber security concerns are:

A. Authentication

It proposes to verify the identity of user based on the credentials stored in the security domain of the system. The most common mode of governance is password technology; the main challenge encountered in authenticating process is when the unauthorized people try to spoil the attempts of authorized people only to listen to the authenticating message. The password transmitted over an insecure medium is responsible to be diverted by dishonest people who can use it to disguise as the original user. This problem is solved by encryption.

Techniques used for Authentication

1. Password and Pin Authentication

In this technique, privacy and confidentiality can be maintained up to some extent. User remember their passwords termed as Knowledge-based techniques. Passwords can be single words, numeric, phrases, any

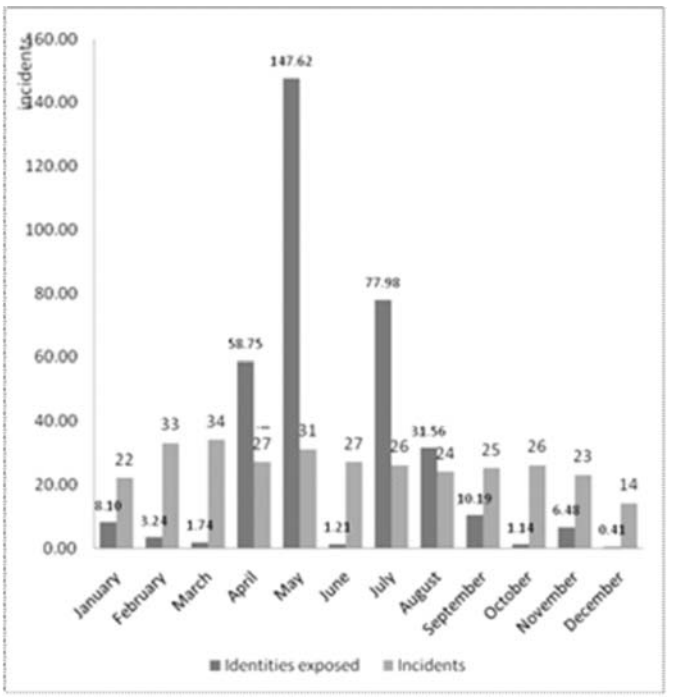


Fig. 3: Incident and Identities Exposed

grouping of these. But problem with this technique is that memorized passwords can be easily predicted or randomly explored by the hackers. The following fig.1 shows the working of authentication technique.

1. Biometric Authentication

As per the survey of previous year, detecting theft and loss or disclosure of data is increasing day by day. To overcome these security threats uses of different gestures come in the process such as:

(a) Fingerprints Authentication

As per the study of many years it is found that fingerprints are unique of every person in the world even twins also have different fingerprints and these are used for basic security in companies to access files and databases over the server. In this security it compares the pattern of rides and creases on the fingers. As per the survey record it is found that it is the worst security in Biometric. For eg. China stolen the fingerprints of 5.6 million US Federal Employees in Year 2013 [8].

(b) Voice Recognition Authentication

As per the record it is most widely use security in cyber world. It is different from speech recognition and it is basically recognized the way of person speaks and the pitch of the voice.

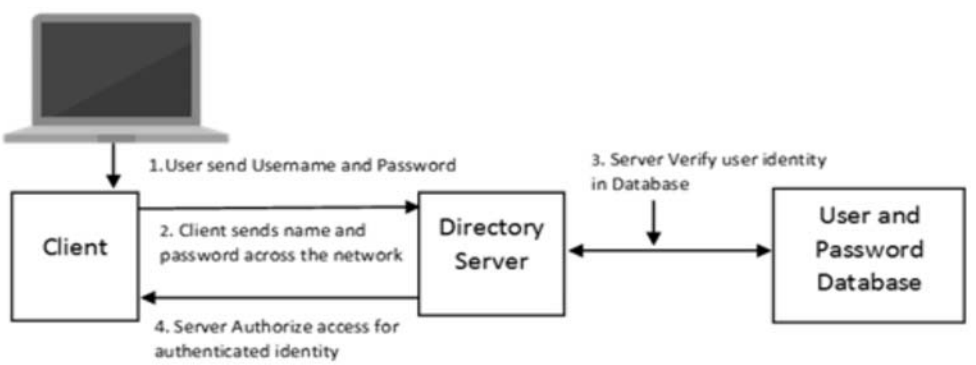


Fig. 4: Verification Process

	Fingerprint	Face	Iris	Voice
Uniqueness	High	Low	High	High
Durability	High	Medium	High	Low
How Well Trait can be Sensed	Medium	High	Medium	Medium
Speed and Cost Efficiency of System	High	Low	High	Low
Willingness of people to have trait used	Medium	High	Low	High
Difficulty of spoofing the trait	High	Low	High	Low
False Rejection Rate	0.4%	1-2.5%	1.1-1.4%	5-10%
False Acceptance Rate	0.1%	0.1%	0.1%	2-5%

(c) Iris Scanner Authentication

It is the latest technology used for authentication in different aspects and it recognizes the person by laser system that scan the retina of the eye that has unique pattern.

(d) Facial Recognition Authentication

This authentication application is capable to recognizing and confirming a person from the video sources and digital images. It recognizes the shape, size and pattern of the face of the person

This Table shows the pros and cons of Biometric Authentication and which is designed by analyzing different articles:

B. Encryption:

Encryption renders data crypt without application of a proper key to unlock the same. To decrypt an encrypted data, one would be required to undertake solving complicated mathematical problems like factoring large primes that would consume astronomical amount of computing resources and time.

(a) Symmetric encryption: It utilizes the same key for the purpose of message encoding and decoding, and the security level is similar to that of the key. The distribution of the key will be accompanied by potential security risks.

(b) Asymmetric encryption: It utilizes a public key to encrypt the message and a private key to decrypt the same. A majority of present day security protocols are using asymmetric encryption for distribution of keys.

Algorithm used for Encryption

1. Triple DES

Triple DES is designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

2. RSA

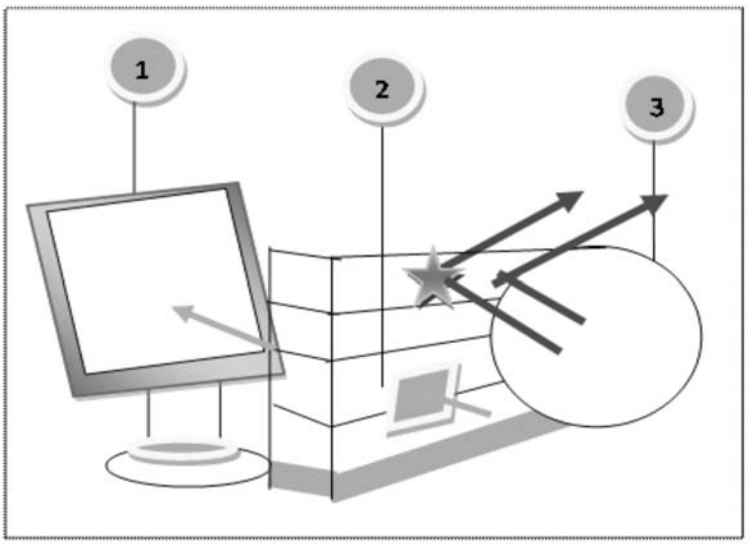
RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it.

3. Blowfish

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. It's definitely one of the more flexible encryption methods available.

4. Two fish

Computer security expert Bruce Schneider is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in



1. Your Computer
2. The Firewall
3. The Internet

Fig. 5: Working of Firewall

length and as a symmetric technique, only one key is needed. Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments.

Tools Used for Two Fish Encryption: Photo Encrypt, GPG, and the popular open source software True Crypt.

5. AES

The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

C. Digital Signatures

Digital signatures can be created out of the same mathematical algorithms that are used in asymmetric encryption. A user holds a private key for getting some information encoded with it. Anyone can get the same decrypted data by having the public key that will verify the person's credentials. This process is the core of the exact reciprocal of public key encryption

D. Anti-virus

The threats of computer viruses or undesirable short programs that trigger unwanted commands without the explicit permission of user have assumed monstrous proportions. Anti-virus software carries out two functions; it prevents the installation of virus in a system and scans the systems for viruses that are already installed.

E. Firewall

Firewalls [9,10] effectively hold back any attempt of unauthorized access to a computer when it is connected on the internet by hackers directly or via other network connections. Firewalls come pre-installed with most operating systems and are turned on as default. The help of commercial firewalls can be required if the security level of the default firewall is not strong enough or if it is posing interference to legitimate network activities.

Working of Firewall

There are various different methods firewalls use to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used in a number of ways

to add protection to user's home or business. Large organization or corporations often have very complex firewalls in their workplace to secure their networks. On the other side, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidential data outside the network. On the inbound side, firewalls can be programmed to stop access to certain websites like social networking sites. Moreover, firewalls can prevent outside computers from accessing computers inside the network

G) Some Cyber Security Tools

There are various tools used for cyber security such as:

1. Vulnerability Scanners

(a) Nmap- It is the Network Mapper and available as free and open source license utility for network discovery and security auditing.

(b) Nessus – For Security Practitioners who evaluate complex enterprise networks for security flaws and compliance issues, Nessus is the world's most widely Deployed vulnerability and configuration assessment product.

(c) Open VAS – Open VAS is a framework of several services and tools offering a wide-ranging and powerful vulnerability scanning and vulnerability management solution.

2. Forensic Security Tools

(a) FTK Imager - It is a court accepted digital investigations platform which is built for speed, analytics and enterprise-class scalability. It is known for its in-built interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with organization's needs.

(b) Sans Investigate Forensic Toolkit (SIFT) - The SIFT workstation is a VMware appliance, pre-configured with the necessary tools to perform detail digital forensic examination in the variety of settings. It is compatible with Expert Witness Format (E01), Advance Forensic Format (AFF), and raw(dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many new capabilities and tools such as log2 timeline that provides a timeline that can be of enormous value to investigator.

3. Penetration Testing

(a) Metasploit - Simplifies network discovery and vulnerability verification, Tool Used: Nexpose.

(b) Paros - Web Scanner

4. Reverse Engineering

(a) OllyDbg – It is an assembler level analyzing debugger for Microsoft® Windows®. Emphasis on binary code analysis.

5. Network and Security Traffic Analysis

(a) Silk - Silk, the System for Internet-Level Knowledge, is a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team (CERT NetSA) to facilitate security analysis of large networks.

IV. Review of Cyber Security Practices

This research study aims to highlight the conditions of Cyber Security in the world and the best cyber security practices. These are the countries that are top listed in the ITU'S cyber security ranking. This set of the particular countries contains a section of each of the following:

1. Developed Countries

This includes countries that lead the ITU's ranking which regards to cyber attentiveness [11] shown in Table 1. The analysis of these strategies will provide a notion of advance and secure cyberspace practices to be measured while expressing a cyber security strategy documents.

The Cyber Security practices of USA, UK, France, Netherlands and Germany are particularly recognized worldwide for mentioning dual aspects of cyber security that is both offensive and defensive cyber security action plans [12]. Japan, Spain, Australia and Canada [13] have been selected because they have the highest ICT usage and cybercrime rate in the world after US and Germany; they also reveal potentially secure approaches for combating cybercrimes in the country. [14] Besides These Countries Czech Republic and Estonia are amongst the few countries that have

Table 1: Developed Countries with High Cyber Security Ranking

Cyber Security Ranking	Country
1	USA
2	Canada
3	Australia
4	New Zealand
5	Estonia, Japan, UK, Germany
6	Austria, Israel, Netherland
8	Finland
9	France
12	Czech Republic

updated their first strategy draft. Netherlands has been selected as like the USA, it has two separate strategies one for Civil and other for military cyber defence. Finland and Israel are considered the prime example of cyber excellence according to many security researchers. [15] This is the reason why the strategies of these countries have been selected for the study.

2. Developing Countries

This includes countries which have high cyber security ranking, according to ITU, as shown in Table 2. Cross Comparison of Such Strategies will provide necessary information for developing nations development with such a quick step in cyber domain, Leave even many developed countries behind.

The Researchers regard Malaysia as the most cyber savvy country of Asia and hence, it is included in the set of countries for research [16]. India and Iran have extremely high cybercrimes rates, so the analysis of their strategies will provide considerable direction for protecting the cyberspace against miscellaneous threats and attacks.

3. Comparison Based on Identified standards

The Cyber Security strategies exist in various forms and length varying from nine pages (Netherlands Cyber Security Strategy of 2011) to ninety pages (Saudi Arabia's Cyber Strategy of 2013). Most of the countries under study have developed separate strategies for National Defense and Cyber Security, whereas few added a portion of "Cyber Security" in national security strategy or the defense strategy.

(a) Development of Cyber Security Strategy

The Development of cyber security strategies gradually gained momentum after 2008 when the trend of Cyber-attacks shifted to massive targeted state-sponsored attacks. Table 3 below gives a timeline of NCSS of Various National Cyber Security Strategies that have been selected from research study. With the Exception of Iran, Israel and Malaysia, all the countries have published their strategies online. The data for these three countries have been take out from public documents relating to the cyber security methods in the country.

Table 2: Developing Countries with High Cyber Security Ranking

Cyber Security Ranking	Country
3	Malaysia
5	India
7	Turkey
19	Iran

Table 3: Timeline of Cyber Security Strategies

Countries	Year Strategy/ Policy Issued
Australia	Strategy 2009, Revised strategy expected
Austria	Strategy 2013
Canada	Strategy 2010, Action Plan for Strategy 2013
Czech Republic	Strategy 2011, 2015
Estonia	Strategy 2008, 2014
Finland	Strategy 2013
France	Strategy 2011
Germany	Strategy 2011
India	Policy 2013
Iran	NCSS not Public
Israel	Official NCSS not Published
Japan	Strategy 2013
Malaysia	Policy 2006(Document not Public)NCSS expected in 2017
Netherlands	Strategy 2011, 2013
New Zealand	Strategy 2011
Saudia Arab	Strategy 2013
Spain	Strategy 2013
Turkey	Strategy 2013
UK	Strategy 2009, 2011
USA	Strategy 2003Strategy Review (2009)Policy 2011, Strategy for critical Infrastructure (2014), Dept. of Defence strategy 2015

The timeline infers that majority of the countries published their cyber security strategy in 2011. The United States of America, on the other hand, published the first strategy draft in 2003, when cyber-attacks were not very common. However, the continuously changing spectrum of cyber threats has made it imperative to update the cyber security strategy to encompass emerging threats and relevant countermeasures. Countries particularly the UK, USA, Netherlands, Czech Republic and Estonia have consequently published the subsequent versions of their strategy as well, with USA reviewing and updating their documents most frequently.

(b) Strategic Objectives outlined in NCSS

NCSS basically defines the vision of any country for addressing the cyber security challenges at the national level. Since all strategies are directed towards the ultimate goal of safeguarding the national cyberspace, they share many common themes and concerns. Except for Germany, which lists down some priority areas as the objectives, all other countries clearly state their strategic objectives in the document. The common objectives found in almost all NCSS are: [17]

1. To maintain a safe and resilient cyberspace,
2. To secure critical national cyber assets and infrastructures,
3. To define a cyber-security regulatory, legislative and assurance framework,
4. To raise cyber awareness amongst citizens, government officials, IT professionals etc.,
5. To develop cyber security incident detection and response capabilities e.g. Cyber-Security Incident Response Team (CSIRT) etc.,

6. To develop indigenous cyber-security technology,
7. To respect fundamental rights of citizens,
8. To promote public-private co-operation for enhancing the cyberspace security,
9. To stimulate international co-operation mainly with the neighboring and regional countries.

Beside the common ones, few strategies have also proposed objectives that are only specific to their country. For instance, France desires to become a world leader in cyber security domain in near future. Also, Japan desires for agile adaptation of evolving cyber threats and introduction of global outreach programs for cyber security, etc. The thorough study of the selected strategies also brings forward the fact, that with the passage of time, the scope of cyber security strategies is shifting from merely securing citizens or governments against cyber-attacks to securing the whole information society in general.

(c) Level of prioritization assigned to cyber security

In the last few years, besides terrorism, economic downturn, natural hazards, etc., cyber-attacks, cyber espionage and cyber terrorism have also become a global risk. The comparative analysis reveals that countries have now realized the importance of cyber security and, therefore, regard it as one of the top-tier national security issues. Countries especially USA, UK, Japan, Germany, Australia and France that have inflated rates of cybercrimes, have allocated significantly greater resources to cyber security measures than other countries under study. According to the publically available data, the UK spends £650m annually, India $500 million, France $1.2 billion, Canada $6 billion, and USA with the highest annual cyber security spending in the world amounting up to 10 billion dollars. [18] The facts indicate that despite same prioritization is assigned to cyber security in various documents, extensive variation lies in the budget allocated to national cyber security initiatives. [19]

(d) Characterization of Cyber Security Threats

For most of the countries, especially Canada, USA, UK, Germany, Netherlands etc. the potential risks and threats posed to the cyberspace revolve around organized cybercrimes, state sponsored attacks, cyber terrorism, unauthorized access to and interception of digital information, electronic forgery, damage and blackmail etc. For Germany and Netherlands, natural hazards and hardware/software failures too are regarded as the cyber threats. [20] In the cyber security strategies, there also exist some offenses that varies in terms of severity of the crime in different countries. Since Germany view cyber-attack as the attack on IT systems that compromises secrecy, availability and integrity of the information systems, USA considers it as an attack on the digital information, ICT devices and cyber networks. Hence, where probing is considered as a cybercrime in Germany, it is not an offense in USA. [21] Thus the varying observation of cyber security and the cyber threat landscape makes it difficult to adopt a holistic global approach to cyber threats and adversary. Apart from the traditional cyber-attacks, few countries have also taken account of emerging cyber risks in their strategies e.g. France, Japan and India have considered the risks of Cloud Computing, Japan mentions the need of addressing the security of Internet Protocol IPv6 and appliances attached to smart grids etc., in the document. Few countries such as Estonia, USA, Germany and Netherlands have also referred to cyber warfare in their documents. However, Finland and France have not defined any cyber threat topology explicitly in the strategy.

(e) Technical Measures:

(Threat Information Sharing/ Early Warning Approached)For a country to effectively deter targeted cyber threats and incidents, it is essential to have technical teams that efficiently spread threat information to the concerned authorities and provide cyber protection and resilience capabilities. Various forms of such teams include Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRT) and Information Sharing and Analysis Centre's (ISAC). The cross comparison of the selected NCSS reveals that all the countries hold their own national CERT/ CSIRT for effectively responding to cyber-attacks. However, the missions and efficiency of these units greatly vary for one another. Table 4 below provides a timeline of the establishment of CERT/ CSIRTS in the countries under study. [22]

Table 4: Timeline of Cyber Security Strategies

Countries	CERT Established
Australia	2010
Austria	2008
Canada	2003
Czech Republic	2011
Estonia	2006
Finland	2014
Malaysia	1997
Netherlands	2012
New Zealand	2011
Saudia Arab	2006
Spain	2008
Turkey	2007
UK	2014
France	2008
Germany	2012
India	2004
Israel	2014
Japan	1996
USA	2003

Few countries have also established coordinating bodies along with CERT/ CSIRTS for information threat sharing. For example, Integrated Government of Canada Response Systems by Canada, Cyber Security Strategy Head quarter by Japan, etc.

To ensure that all public and private entities can handle cyber security challenges, it is necessary to establish an appropriate policy framework to frequently evaluate the progress of the proposed objectives of the strategy and revise the strategy accordingly. The research reveals that except for Spain, most countries within the scope of study have mentioned review and evaluation processes for the strategy in the documents. Since, Malaysia has not formulated the complete strategy yet, it, therefore, lacks annual cyber security audits and policy reviews too. Countries such as Austria, Estonia and Germany have even specified the actors to be involved in reviewing mechanisms. However, in all instances, the details of review mechanisms have been provided as a separate act or in implementation scheme. Several strategies have also mentioned the frequency of the review cycle i.e. yearly for Netherlands and Slovakia and biannual for Austria and UK. [23]. While USA, UK, Estonia and few other countries update their cyber security strategy very frequently, there are countries that have not even updated their initial cyber security strategies once.

(f) Cyber Security Capacity Building

All cyber security strategies mention the need of creating cyber defensive and preventive capabilities to better defend the national cyberspace. This subsection throws light on various cyber security capacity building initiatives e.g. training, awareness, R&D initiatives etc., as documented in the selected strategies.

(1) Manpower Development and Cyber Awareness Programs:

All cyber security strategies emphasize the need of raising cyber awareness in general public especially businessmen, IT professionals, government officials and lawmakers. But countries especially, Australia, Spain, Japan and the UK pay special attention to the cyber training of children and parents too. [24] Countries particularly UK, India and Malaysia have mentioned the usage of social media for launching widespread awareness campaigns. However, Netherlands and Turkey highlight the need of teaching cyber security at all academic levels and have thus suggested making it a part of academic curriculum. All the nations under study, except for the Czech Republic, have defined nation-wide cyber-security outreach programs for their citizens, where they provide cyber security tools and practical education. The most notable programs amongst them are Stay Safe Online campaign of Australia, Malaysia's "Cyber Safe" Program, "Get Safe Online" program of UK, and organization of "Cyber Security Month" annually by Austria, UK, and US. [25] The study also reveals Japan's desire for establishing various cyber security support services for the capacity building. Moreover, countries especially UK, Netherlands, India, Saudi Arab, Malaysia, and Turkey emphasize the need of commercial security certifications/ trainings for professionals and experts in their NCSS. [26]

(2) Research and Development:

To prevent inherent vulnerabilities of the ICT devices from being exploited by adversaries, it is required to lay stress on the development of local security products, thereby enhancing cyberspace security. The comparative study shows that except for Australia, Saudia Arab, Czech Republic, UK and Finland, all other countries have officially recognized entities for promoting R&D work at the national level. The tasks of the R&D divisions as mentioned in the various strategies are to sponsor academic and industrial projects related to cyber security, develop indigenous cyber security products, promote security standards and best practices at the national level, etc.

(g) Latest on Cyber Security Practices

Privacy and data theft will be the top security issues that organizations need to focus. All are living in a world where all information is in digital form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. There will be new attacks on Android operating system based devices, but it will not be on a huge scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8 and Windows 10, so it will be possible to develop malicious applications like those for Android [27] and infected them using network and web.

V. Conclusion

In the recent years, Cyber Security has gained more attention than the issue of National Physical Security. Countries around the world are, therefore, framing cyber security strategies to address this serious issue. Almost all documented strategies, selected by different countries, have mentioned the need of establishing incident prevention capabilities at the national level, raising cyber awareness in general public, and promoting public-private partnership for better security of the cyberspace, etc. However, the majority of the countries have practically tried less to achieve the above stated objectives. Despite similar aims and objectives, the research has shown many differences in the scope and approach of the twenty strategies that were selected for the study. For instance, the establishment of CERT has been mentioned in all the strategies, but the tasks assigned to it vary from country to country. Similarly, all strategies urge the need of running various cyber awareness programs, but the approach of each country is different from the other. From a detailed research, it is obvious that the strategies of UK, USA and Germany are particularly better than the rest in terms of development and enforcement of action plans. Despite stating defensive missions in the strategy, they have also highlighted on utilizing their cyber capabilities to defend valuable assets offensively, and this gives them an edge over the other countries.

References

1. http://www.wired.com/2015/08/ashley-madison-hack-everything-you-need-to-know-your-questions-explained/
2. https://www.uscert.gov/ncas/tips/ST04-015
3. http://paper.ijcsns.org/07_book/200905/20090501.pdf
4. http://research.ijcaonline.org/volume60/number19/pxc3884306.pdf
5. http://www.ijcsit.com/docs/Volume%202/vol2issue3/ijcsit2011020309.pdf
6. http://arxiv.org/ftp/arxiv/papers/0803/0803.3912.pdf
7. Cross Domain Solutions http://www.crossdomainsolutions.com/cyber-security/tools-techniques/
8. Associate Press in Washington http://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints
9. Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000
10. Kuang Chu,network security and firewall technology, Chongqing university publishing house,2005
11. S. W. Lodin and C. L.Schuba, " irewalls fend off invasions from the net," IEEE Spectrum, vol. 35, no. 2, 1998.
12. Global Cybersecurity Index. ITU. 2014. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI101.pdf
13. Dunn, M. A Comparative Analysis of Cybersecurity Initiatives Worldwide. WSIS Thematic Meeting on Cybersecurity. 2005
14. Carmen Cristiana Cirlig. Cyber Defence in the EU- Preparing for cyber warfare? 2014. Retrieved Nov 29, 2015 from http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyberdefence-in-the-EU-FINAL.pdf
15. Sumo. Top 20 Countries Found to Have the Most Cybercrime. 2014. Retrieved Dec 5, 2015 from http://www.enigmasoftware.com/top-20countries-the-most-cybercrime/
16. Ashley Wheeler. The Best and Worst of Cyber Security. 2013. Retrieved Nov 4, 2015 from http://phoenixts.com/blog/best-and-worst-cybersecurity/
17. Nurjehan Mohamed. Malaysians are the most cyber-savvy among Asians. 2015. Retrieved Dec1, 2015 from http://www.therakyatpost.com/life/trends-life/2015/08/25/malaysiansare-the-most-cyber-savvy-among-asians/
18. Luiijf, H. Besseling, K. Spoelstra, M, Graaf, P. Ten National Cyber Security Strategies: A Comparison, Critical Information Infrastructure Security, Lecture Notes in Computer Science 2013. Volume 6983, pg 1-17
19. Hedborg, M. Comparing Security Strategies, UI Brief. 2012. Available: http://www.ui.se/upl/files/77897.pdf
20. Klimburg, A. National Cyber Security – Framework Manual. 2012. CCDCOE.
21. The Cyber Index International Security Trends and Realities. 2013. Retrieved Dec 3, 2015 from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en463.pdf
22. ITU. Cyber Wellness Profiles. 2015. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
23. OECD. Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy. 2012. Retreived from http://dx.doi.org/10.1787/5k8zq92vdgtl-en
24. ENISA. National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. May 2012.
25. Asia Pacific Cybersecurity Dashboard. 2015. Retrieved Dec 4, 2015 from http://cybersecurity.bsa.org/2015/apac/index.html
26. ITU. National CyberSecurity Strategy Guide. 2011.
27. Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012