IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL)
ISSN (P): 2347–4564; ISSN (E): 2321–8878
Vol. 9, Issue 6, Jun 2021, 39–52

THE CYBER-SECURITY CHALLENGES AND THE AMERICAN APPROACHES

Siva Priya Murugadoss

M.A International Studies, Women's Christian College, Chennai, India

Received: 05 May 2021 **Accepted:** 27 May 2021 **Published:** 15 Jun 2021

ABSTRACT

This article deals with one of the national security problems which is cyber-security. The main purpose of choosing cyber-security as a topic arises from few questions. Why did this technologically revolutionized concept have a part in the national security of states? What are the various strategies used by the states to tackle these threats? The article briefly answers these questions and discusses the actors involved in various types of cyber-security threats and the challenges evolving while making the policies. It also deals with the concept of Barry Buzan's vulnerability framework of non-traditional security threats to explain states strategies to suppress threats. The article comprehensively discusses the United States cyber-security strategies in different periods. Thus the article involves an analysis of the United States cyber-security strategies with the help of Buzan's framework and pillars of Global Cyber security Index. Thus the result of the analysis explains the complex nature of cyber-security threats and the challenges in creating and implementing the policies.

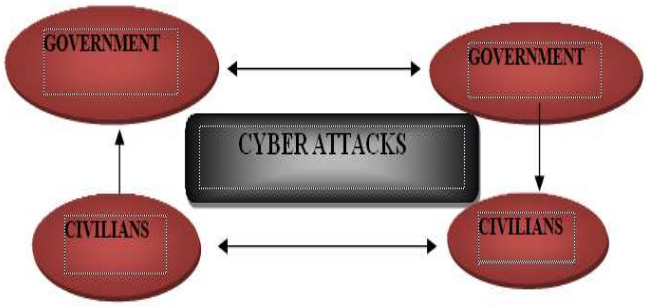
KEYWORDS: *Cyber-Security, Barry Buzan Framework, Global Cyber-Security Index, United States*

INTRODUCTION

The news statement published by Forbes magazine quoted that "*Cybercrime is expected to cost nearly $ 6 trillion worldwide in 2021"*, which explains the importance of cyber-security for the states. Many states have equal contribution of budget, developments in infrastructure and awareness to the area of cyber-security but some of them are still behind the basic requirements. This article discusses briefly about cyber-security and its challenges, approaches to developments and explains the cyber-security strategy of the United States of America.

Cyber-security is defined as the activity or process, ability or capability, or form whereby information & communications systems and the information contained therein are protected from and defended against damage, unauthorised use or modification, or exploitation[1]. Cyber-security is a debated concept because of its technical nature and difficulties in understanding the threats approached. So the cyber threats are malicious act that damages the information stored, networks of communication system or to steal data.

[1](2021), National Initiative for Cybersecurity Career and Studies, "Cyber-security Glossary." Retrieved from https://niccs.cisa.gov/about-niccs/Cybersecurity-glossary



Source: Author's Compilation

Figure 1: Classification of Cyber Threats.

Cyber threats are carried out in one of these ways: Cyber attacks, and Cyber espionage. Cyber attack cause damage to the data, which can be a communication system, information system or the electronics where information's are stored whereas Cyber espionage means obtaining secret and sensitive information of any entity to gain some strategic advantage. Some of the mode of cyber threats is through phishing, malware, ransom ware, data leakage, and DDOS.

The Cyber security threats are classified into four categories with respect to the actors like mentioned in the above Figure 1. The cyber attack happens in between states, the attack on civilians by state, a strike on state by civilian and finally, the attack on civilians by a civilian. However, the primary concerns of the state will be curtailing the citizens' attack on the state and other citizens. The management of cyberspace by all four means projects the capability of the state. In these article relations between state and cyber security was analysed through Barry Buzan vulnerability framework and compared with Global Cyber Security Index.

Barry Buzan's Framework

Buzan's framework exclusively describes non-traditional security threats that states find challenging to manage, which includes Cyber-security. Cyber security had become the rational part of national security, due to civilian's free accessibility of Cyberspace without restriction, which is convenient for all kinds of threats.

Barry Buzan's framework explained by analysing two factors such as power and socio-political cohesion, which decides states ability in managing threats.[2]The framework divides the states into four categories based on (weak or strong) power with (weak or strong) socio-political cohesion. The United States of America is analysed under the category of a state with strong power and socio-political cohesion. Power is analysed through robust military and economic supremacy in the international system. The socio-political cohesion primarily deals with the engagement of citizens and government of a state and the ability to manage domestic threats that have sparked to bring changes in domestic and international laws and policies.

Global Cyber-Security Index

The Global Cyber-security Index (GCI) is a multi-stakeholder initiative to raise Cyber-security awareness and measure countries' commitment to Cyber-security. It scrutinize across industries and sectors. The index helps countries to identify their potential in the field of Cyber-security and precautionary measures to prevent further cyber-attacks. The Global Cyber-security Index evaluates states performance under five categories such as Legal Measures, Technical Measures, Organisational Measures, Capacity Building and Cooperation.

[2]Czosseck .c (2010). *The cyber threat to national security: why can't we agree.* Retrieved from file:///D:/project/The%20Cyber%20Threat%20to%20National%20Security.pdf.

American Understanding of Cyber Security Challenges

Barry Buzan's framework and GCI are used to analyse the United States cyber security strategy. The most prominent aspect of American Cyberspace and a challenge is individuals' freedom in accessing cyberspace and inferred Cyber security threats due to proscribed actions. Freedom is also the most significant threat that enhances civilian attack on civilian. The America pre-eminence lies in identifying the challenges possessed in freedom of free access in cyberspace. However, the US and other states are facing challenges in technical nature, the degree of operational functionality intertwined in the design, and the involvement of human factors in Cyber-security.[3]Some of the challenges are listed below:

The Technical Challenges

The technical factors are the requirement of technical engineers in the decision making process and discussions, which are called as "system security engineers". System security engineering is a critical component in recognizing effects of Cyber-attacks by state and civilian. Other technical factor comprises integrated device with stable infrastructure and its interactions with other human operators.

Operational Functionality

The system security engineers are available at national level, but the general public still lacks proficient engineers, thus complicating policy implementation and making continuous cyber security monitoring difficult. In the US, Cyber-security management is a process-control loop that every country should consider.

Influence of Human Factor

The influence of the human factor also includes several Cyber assailants and the defender. The defender's influence in policymaking, which includes various interest groups, the policymakers, the engineers involved in the technicalities, states portrayal of its Cyber-security in media and other members like such as consumers, investors, law enforcement officer, businessman, Federal, State and Local government bodies. The contribution of human factor is an important factor of social cohesion[4] which makes citizens to be part of the decision making process. However, as each party seeks to optimize its own perceived interest or mission, thus giving rises to tensions between various interest groups. Consumers, investors, and companies, according to economists, would aim to optimize their position by growing profits and avoiding costs. Nevertheless, the US government has considered the interest of all the interest groups to an extent and enacted various laws like Presidential order, Presidential Policy directives and cyber security institutions to curtail cyber-attacks. The US cyber security measures and reforms are categorized under three period such as pre twin tower attack, post twin tower attack and cyber security policies under President Obama. The following two initiatives acted as an emergency plan for many national security issues of the US.

Presidential Policy Directive

A presidential directive is a written or oral instruction or resolution provided by the United States president that can rely on the president's powers conferred by the United States Constitution, statutory law, or, in some instances, legislative and judicial approval.

[3] Snyder Don et al. (2015). *"Improving the Cybersecurity of US Air Force military system throughout their cycles". Published by US Air force.* Retrieved from :file:///D:/project/read%20these/us%20airforce.pdf
[4]Trautman J. Lawrence.(2015). "*Cybersecurity: what about US policy*".
Retrieved from: file:///D:/project/read%20these/us%20Cyber%20policy.pdf

Pre Twin Tower Attack Measures:

In the pre Twin Tower period, the measures of cyber-security were generally an outline to implement their cyber-security.

The Initial Cyber-Security Act

The initial cyber security was concerned in protecting business and health care sector. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the 1999 Gramm-Leach-Bliley Act.[5]

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPPA is a United States federal legislation signed into law by President Bill Clinton on August 21, 1996, by the 104thUnited States Congress. Its key objectives were to modernize healthcare data flow, define how personally identifiable information owned by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations.[6]

Gramm-Leach-Bliley Act of 1999

Financial institutions, or organizations that provide consumers financial products or services such as loans, financial or investment advice, or insurance, are required by the Gramm-Leach-Bliley Act to clarify their information-sharing activities to their customers and safeguard confidential data.[7]

Presidential Executive Order 13681 - Improving the Security of Consumer Financial Transactions

Executive departments and agencies are transitioning payment processing terminals and credit, debit and other payment cards to use enhanced security features, such as chip-and-PIN technology, to improve data security and better protect people doing business with the government. Agencies must consider applicable voluntary consensus requirements and criteria, as appropriate, when deciding the enhanced security features to use in compliance with the National Technology Transfer and Advancement Act of 1995 and Office of Management and Budget Circular A-119.[8]

Post Twin Tower Period

During the post twin tower attack period, the US government enacted major Act such as Creation of Homeland Security Act, Federal Information Security Management Act (FISMA) and Bush's executive order 13231 and different initiatives.

Creation of the Office of Homeland Security

Executive Order 13228 created the Office of Homeland Security and required the protection of "energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; public and privately owned information systems; special events of national significance; transportation, including railways, highways, shipping

[5]Guillermo A. Francia Iii et al. (2007). "The Design and Implementation of an Automated Security Compliance Toolkit: A Pedagogical Exercise". Retrieved from: https://www.researchgate.net/publication/234787857_The_Design_and_Implementation_of_an_Automated_Security_Compliance_Toolkit_A_Pedagogical_Exercise

[6] GPO, (1996). "*Health Insurance Portability And Accountability Act Of 1996*". Retrieved from: https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

[7] Federal Trade Commission. "Gramm-Leach-Bliley Act". Retrieved from: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[8] The white house. "Improving the Security of Consumer Financial Transactions". Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

ports and waterways; airports and civilian aircraft; livestock, agriculture".[9]

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 requires that the Director of the Office of Management and Budget oversee Federal agency information security policies and practices, including requiring each Federal agency to define and enforce information security safeguards commensurate with the probability and magnitude of harm resulting from unauthorized use, disclosure, disturbance, alteration or destruction of information system. Senior officials in each agency must ensure the security of the information. The systems that sustain their activities, assets establish plans and procedures to ensure their continuity[10]. FISMA has brought Cyber-security to the federal government's attention, emphasizing a "risk-based approach for cost-effective defense". The law amended as the Federal Information Security Modernization Act of 2014. [11]

President Bush's Critical Infrastructure Protection Board by Executive Order 13231

Executive Order 13231 established by President Bush's Critical Infrastructure Protection Board. The USA PATRIOT Act of 2001 included a description of "sensitive infrastructure", and The National Plan for the Physical Protection of Critical Infrastructures and Key Assets outlines the Bush administration's homeland security strategy.[12]

Commission on Cyber-Security for the 44th Presidency

The Centre for Strategic and International Studies (CSIS), a nonpartisan, nonprofit research center located in Washington, D.C., created the Commission on Cyber-Security for the 44th President in 2007.[13] Members of the Commission have considerable government experience as well as skills in Cyber-security. The Commission outlines considerations such as "federal structure and strategy", "Cyber-security norms and authorities", "Investment and acquisition policy" and "government interaction with the private sector".

A forward-looking framework for coordinating and prioritizing government efforts to Secure Cyberspace in order to evaluate current and potential threats to federal structures and critical infrastructure, review authorities, strategies, and government organizations for Cyber-security, and identify critical infrastructure protection needs.

The Comprehensive National Cyber-Security Initiative

In January 2008, President George W. Bush released National Security Presidential Directive 54 and Homeland Security Presidential Directive 23, launched the Ambitious National Cyber-security Initiative (CNCI).[14] During Obama's presidency, CNCI and its related operations grew to become core elements of a wider, revised national US Cyber-security strategy. The Cyber Initiatives of the CNCI intended to achieve the following objectives:

---

[9] Homeland security. "Creation of the department of homeland security". Retrieved from: https://www.dhs.gov/creation-department-homeland-security

[10]Congress.(2002). "Federal Information Security Management Act".
Retrieved from:https://www.congress.gov/bill/107th-congress/house-bill/3844

[11] (2002). "Federal Information Security Management Act". Retrieved from: https://www.congress.gov/bill/107th-congress/house-bill/3844

[12] Department of Homeland Security. (2001). "Critical Infrastructure Protection in the Information Age". Retrieved from: https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf

[13]Center for strategic and international studies. "Commission on Cyber-Security for the 44th President in 2007". Retrieved from: https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-6

[14] The white house. "The Comprehensive National Cyber-security Initiative". Retrieved from: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

- To provide a front line of protection against today's immediate threats by establishing or improving mutual situational knowledge of network vulnerabilities, threats, and incidents within the Federal Government and eventually with national, local, and tribal governments and private sector partners, as well as the ability to respond rapidly to mitigate existing vulnerabilities and avoid intrusions.
- Enhance US counterintelligence capabilities and strengthen the supply chain's security for critical information technology to protect against a wide range of threats.
- Expanding Cyber education, organizing and redirecting research and development activities around the Federal Government, identifying and improving strategies to combat hostileor malicious activity in Cyberspace would reinforce the potential Cyber-security climate.

CYBER-SECURITY DURING OBAMA'S ADMINISTRATION

Presidential Executive Orders

EO 13556 - Controlled Unclassified Information

Except for information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended, the order provides an open and standardized programme for handling information that needs safeguarding or distribution controls in compliance with and consistent with legislation regulations and Government-wide policies.[15] To protect and manage the information, executive departments and agencies currently use ad hoc, agency-specific policies, procedures, and markings, such as information involving privacy, protection, proprietary business interests, and law enforcement investigations.

President Obama's 2013 Executive Order 13636: Improving Critical Infrastructure Cyber-Security

On February 12, 2013, President Obama signed Executive Order 13,636, "Improving Critical Infrastructure Cyber-security," which directs the Executive Branch to:

- Develop a technology-neutral voluntary Cyber-security framework;
- Promote and incentivize the adoption of Cyber-security practices;
- Increase the amount, timeliness, and consistency of Cyber threat data shared;
- Every effort to safeguard our vital infrastructure should provide robust privacy and civil liberties protections;
- Explore the efficiency of current legislation that can use to facilitate Cyber-security.[16]

EO 13800 - Strengthening the Cyber Security of Federal Networks and Critical Infrastructure.

In 2017, President Donald Trump signed Executive Order 13800, strengthening the Cyber-security of Federal Networks and Critical Infrastructure, to strengthen the nation's Cyber posture and capabilities in the face of growing Cyber threats. EO 13800 directs the federal government's efforts toward modernizing the information technology infrastructure, partnering with state and local governments and private sector partners to safeguard critical infrastructure and

[15] Federal Register. (2010). "Controlled Unclassified Information" Retrieved from: https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information
[16] Cybersecurity and infrastructure security agency. "CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE" Retrieved from: https://www.cisa.gov/publication/eo-13636-ppd-21-fact-sheet

collaborating with international allies'[17].

Presidential Policy Directive

- **President Obama's Presidential Policy Directive-21: Critical Infrastructure Security and Resilience**

The principles are guiding the Federal Government's response to any Cyber incident, whether involving government or private sector organizations, are outlined in the Presidential Policy Directive (PPD). The PPD also defines lead Federal agencies and an architecture for organizing the more comprehensive Federal Government response in major Cyber incidents. The PPD also needs the Departments of Justice and Homeland Security to keep their contact details up to date with the public's use to assist agencies impacted by Cyber-attacks in reporting them to the appropriate authorities.[18]

- **President Obama's Presidential Policy Directive-41: United States Cyber Incident Coordination.**

The directive defines the National Policy on Critical Infrastructure Protection and Resilience. The collaborative initiative involves the federal, state, local, tribal, and territorial (SLTT) governments and public and private critical infrastructure owners and operators.[19] The directive further improves overall teamwork and cooperation by refining and clarifying essential infrastructure-related functions, duties, and obligations across the Federal Government. The federal government is also responsible for enhancing the stability and resilience of its vital infrastructure.

The United States' policy is to strengthen its critical infrastructure's security and resilience against both physical and Cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. The federal government will also collaborate with foreign partners to enhance critical infrastructure protection and stability in the United States and critical infrastructure in other countries.

Congressional Actions

The National Cyber-Security Act of 2014

The National Cyber Security Protection Act of 2014, signed into law by President Obama on December 18, 2014, provides a much-needed amendment to the Homeland Security Act of 2002.[20] The law establishes within the Department of Homeland Security (DHS) and National Cyber-security and Communications Integration Centre (NCIC), responsible for sharing Cyber-security risks, incidents, analysis, and warnings for both federal and non-federal entities, overseeing critical infrastructure protection, Cyber-security, and related DHS programs.

[17] Cybersecurity and infrastructure security agency. " strengthening the cybersecurity of federal networks and critical infrastructure "retrieved from: https://us-cert.cisa.gov/eo13800

[18] Cybersecurity and infrastructure security agency.(2015). " strengthen the security and resilience of its critical infrastructure against threats and address cyber threats" retrieved from: https://www.cisa.gov/publication/isc-ppd-21-implementation-white-paper

[19] The white house. (2016). "cyber incident coordination". Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[20]Congress. (2014). "Department of Homeland Security Appropriations Act" retrieved from: https://www.congress.gov/bill/113th-congress/house-bill/2217.

The Federal Information Security Modernization Act

The Federal Information Security Modernization Act of 2014, signed into law by President Obama on December 18, 2014, provides amendments to the Federal Information Security Management Act of 2002 (FISMA) to " reestablish the oversight authority of the Director of the Office of Management and Budget (OMB).[21] It consists of information security policies and practices, and set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems."

The Cyber-security Workforce Assessment Act

The Cyber-security Workforce Assessment Act, signed into law by President Obama on December 18, 2014, requires "the Secretary of Homeland Security to assess the Department of Homeland Security's Cyber-security workforce and develop a comprehensive workforce strategy." The law assessment includes "(a) an assessment of the readiness and capacity of the workforce of the Department to meet its Cyber-security mission; (b) information on where Cyber-security workforce positions located within the Department; (c) information on which Cyber-security positions performed by [full-time employees, contractors, other agencies]." [22]

Besides, the law provides that within 120 days following enactment, a report will be submitted by the Secretary to appropriate Congressional committees as to "the feasibility, cost, and benefits of establishing a Cyber-security Fellowship Program to offer a tuition payment plan for individuals pursuing undergraduate and doctoral degrees who agree to work for the Department for an agreed-upon period".

The Homeland Security Workforce Assessment Act

Signed into law on December 18, 2014, the Homeland Security Workforce Assessment Act became law as an attachment to the Border Patrol Agent Pay Reform Act of 2014.[23] In the relevant part, the law designed to improve compensation rates, retention, and hiring procedures for Cyber-security positions at DHS. The law provides an enhanced process to identify critical department IT Cyber-security skills.

The Cyber-security Enhancement Act of 2014

The Cyber-security Enhancement Act of 2014 was signed into law by the President on December 18, 2014, and provides: in Title I, a Public-Private Collaboration on Cyber-security; Title II, Cyber-security Research and Development; Title III, Education and Workforce Development; Title IV, Cyber-security Awareness and Preparedness; and Title V: Advancement of Cyber-security Technical Standards. The Provisions of Title I "permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce Cyber risks to critical

[21] The white house. "Office of management and budget". Retrieved from: https://www.whitehouse.gov/omb/#:~:text=The%20Office%20of%20Management%20and%20Budget%20%28OMB%29%20serves,objectives%20and%20to%20fulfill%20the%20agency%E2%80%99s%20statutory%20responsibilities.

[22] OPM. (2015). " Federal Cybersecurity Workforce Assessment Act of 2015". Retrieved from: https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/#:~:text=The%20Federal%20Cybersecurity%20Workforce%20Assessment%20Act%20of%202015,National%20Initiative%20for%20Cybersecurity%20Education%20%28NICE%29%20Framework%3B%20and

[23] Congress. (2014). "Border Patrol Agent Pay Reform Act " retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/1691

infrastructure."[24]

Other Collateral Developments

Other initiatives are Commission on Cyber-security for the 44th Presidency, publication during 2011 of the DHS Blueprint for a Secure Cyber Future.[25] The Cyber-security Strategy for the Homeland Security Enterprise, NIST Framework for Improving Critical Infrastructure Cyber-security, and selected ongoing National Institute of Standards and Technology (NIST) initiatives.[26]

The Cyber-Security Strategy for the Homeland Security Enterprise

It intended to safeguard the United States' critical systems and properties, as well as to promote better, more robust information and communication technologies over time, allowing government, industry, and individuals to be safer online. "Protecting our Vital Information Infrastructure Today and Creating a Stronger Cyber Ecosystem tomorrow," according to the strategy.

National Institute of Standards and Technology (NIST) Initiatives

On a near-daily basis, the National Institute of Standards and Technology (NIST) publish Cyber-security notifications, resources, and initiatives. Those wishing to gain and retain a current understanding of Cyber-security technologies would likely benefit significantly from the NIST materials.[27]

NIST Framework for Improving Critical Infrastructure Cyber-Security

NIST is a voluntary risk-based Cyber-security Framework. A collection of industry guidelines and best practices to help organizations mitigate Cyber-security risks, according to Executive Order 13636.[28] The Framework that resulted from the cooperation of the public and private sectors uses a shared language to discuss and manage Cyber-security risk. According to the Framework, a clear understanding of the organization's business drivers and security concerns is specific to its use of information technology and industrial control systems. Since each organization's risk is different, the tools and approaches used to achieve the Framework's outcomes can differ.

Presidential 2015 Cyber-Security and Consumer Protection Summit

At a Cyber-security and Consumer Protection Summit held on February 13, 2015, at Stanford University, President Obama lists the following basic principles to consider while confronting Cyberthreats.[29]

[24]Congress. (2014). "*The Cyber-security Enhancement Act of 2014*" retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/1353
[25]Cybersecurity and infrastructure security agency. (2011). "Blueprint for a Secure Cyber Future". Retrieved from: https://www.cisa.gov/blueprint-secure-cyber-future#:~:text=The%20Blueprint%20for%20a%20Secure%20Cyber%20Future%20builds,resilient%20cyber%20environment%20for%20the%20homeland%20security%20enterprise.
[26]NIST. "cybersecurity framework". Retrieved from: https://www.nist.gov/cyberframework
[27]NIST. "Cyber security". Retrieved from: https://www.nist.gov/cybersecurity
[28]Cybersecurity and infrastructure security agency. "critical infrastructure security and resilience" Retrieved from: https://www.cisa.gov/publication/eo-13636-ppd-21-fact-sheet
[29]The white house.(2015). "White House Summit on Cybersecurity and Consumer Protection". Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection

Collaboration between Government and Industry

First, it has to be a shared mission. Since the private sector controls so much of our computer networks and vital infrastructure, the government cannot do it alone. However, the private sector cannot do it alone since it is always the government that provides the most up-to-date information on emerging threats. There is only one way to protect America from Cyberthreats: collaboration between government and industry, with sufficient knowledge and should be trusted partners. Second, we must reflect on our distinct advantages. Although the government has many capabilities, it is neither appropriate nor possible to secure private companies' computer networks. Many of the companies present today are cutting-edge, but the private sector does not always have the skills, situational awareness, or capacity to alert others required during a Cyberattack.

Cyber Scholarship Program

Given the increasing reliance on Cyber-security and information technology (IT), the Department of Defence (DOD) must safeguard itself. The Department of Defence (DOD) needs staffing with technically savvy personnel. The Cyber Scholarship Program (CYSP) created to assist in the effort. The National Security Agency administers the DOD CYSP, funded by the DOD Chief Information Office (NSA).[30] The program's goals are to encourage higher education in all areas of Cyber-security, improve the Department's ability to hire and retain Cyber and IT experts and increase the number of military and civilian staff with knowledge in the DOD

Global Cyber-Security Index

Apart from Barry Buzan Vulnerability Framework, Global Cyber-security Index also produced skeleton to analyze a state's Cyber-security standards. The five pillars of GCI explain the US's commitment level towards Cyber-security.

INTERPRETATION WITH GCI

Apart from the Cyber Security challenges, the Global Cyber-security Index had given five quantifying factors to mitigate Cyber-attacks, which helped to understand the American Cyber Security system. First, the legal measures which deals with the US's laws, including the presidential executive orders and policy directives, the legislation of congress. Secondly, Technical measures are the system security engineers and organizations, which are in the maintenance of Cyber-security. Thirdly, organizational measures include the incorporation of homeland security, comprehensive national Cyber-security initiative, US Cyber Command. Fourthly, Capacity-building includes the initiatives taken by an interest group to curtail Cyber threats. Finally, cooperation includes the American proposed summits and bilateral relation in mitigating Cyber Security.

The GCI has a way of calculating the commitment level of Cyber-security. It helps the states to observe the growth and fall of Cyber-security measures concerning the states, in the same way, the US policies and activities to improve Cyber-security worldwide.

[30]US DOD. "Cyber scholarship program". Retrieved from: https://public.cyber.mil/cysp/

Table 1: Analysis of the US Cyber-Security with GCI

Analysis of Global Cyber-Security Index Pillars with US Cyber-Security			
S. No	**Measurement**	**Year**	**Acts, Provinces, Directives.**
1	Legal Measures	1) 2001, 2009, 2013, 2014, 2017. 2) 2013, 2016 3) 2014 4) 2014 5) 2014	1) Presidential executive orders (E.O)-13231, 13556, 13636, 13681, 13800. 2) Presidential policy directives 21, 41. 3) The National Cyber-security Act 4) The Federal Information Security Modernization Act. 5) The Cyber-security Enhancement Act of 2014
2	Technical Measures	1) 2013 2) 2014 3) 2014	1) NIST Framework for Improving Critical Infrastructure Cyber-security. 2) The Cyber-security Workforce Assessment Act 3) The Homeland Security Workforce Assessment Act
3	Organizational Measures	1) 2002 2) 2002 3) 2008 4) 2010	1) Creation of the Office of Homeland Security. 2) Federal Information Security Management Act. 3) Comprehensive National Cyber-security Initiative. 4) The Cyber-security Strategy for the Homeland Security Enterprise.
4	Capacity Building	1) 1901 2) 2007	1) National Institute of Standard Technology. 2) Commission on Cyber-security for the 44th Presidency. 3) Cyber Scholarship Program.
5	Cooperation	1) 2015 2) 2019 3) 2019	1) Presidential Cyber-security and consumer protection summit. 2) Bilateral relation with Japan 3) Engagement with Estonia.

Source: Author's Compilation

It inferred that US satisfied all the necessary factors of GCI with exclusive arrangements to mitigate the threats. In each pillar, the US has established the requirements specific to the Cyber threat. The US government takes measures to deal with government agencies, private institutions and individual citizens concerning the situation. It shows the stability of the US towards strengthening Cyber-security.

The Table: 1 also projects the policies of the US concerning power and socio-politico cohesion which are resulted to be strong and have positive suggestions from policymakers. For example: after the data breach at the end of 2007, the US government reflexed with establishing CNCI through the presidential directive[31]. The CNCI established to spread awareness about Cyber threats among people, federal agencies and private institutions, enhance Cyber education, implementing R&D in the field.

The policies and reforms of the US are categorized above as pre Twin Tower attack, post Twin Tower attack and under Obama administration to explain the growth in the developments of cyber-security measures of the US and their ability to implement immediate policies to prevent future attacks.

[31]The white house. (2016). "cyber incident coordination". Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

With its rapidly growing Cyber-security power, the US also has a partnership with countries to provide assistance. Along with defence and countermeasures, the US tries to make a cooperative association with other states to have peaceful Cyberspace. Since the technical crew and products cost will be expensive, the developing countries depend on countries like the US and the EU which enhance economic benefits to the US.

Along with the foreign policies, policies related to trade, business and government the US government have a specialized center called IC3 to deal with daily Cyber-crimes that American people face. The center act as an interactive place for people to solve Cyber related problem.

In some cases, the US used counters Cyber-attacks with the state, because of severe Cyber damages faced by the US. These factors explain how the US maintaining its non-conventional security threats and adapting the changing nature of issues. The resilience of the US towards Cyber threats is more flexible. Notably in December 2014, the Obama administration's policies have centered on dealing with crisis environment near-term needs, such as "preventing Cyber-based disasters and espionage, minimizing the impacts of successful attacks, strengthening inter and intra-sector cooperation, clarifying federal agency roles and responsibilities, and combating Cybercrime."

Thus led to the conclusion that to tackle all the threats and protect the Cyberspace, the US has formulated various policies, Presidential policy directives, Presidential executive orders, and Cyber-security initiatives. Though there is a rapid increase in Cyber threats due to digitalization and accessibility to Cyberspace, the US has the complete Cyber environment and infrastructure to maintain Cyber-security despite the threats.

CONCLUSIONS

As a conclusion, it can be seen that the challenges and vulnerabilities occur due to cyber-security threats can be suppressed with preventive measures like developing infrastructure, effective policies and awareness but it is a difficult task to handle and put it in control. This clearly explains the necessity of cyber-security to be considered as a crucial part of national security.

REFERENCES

1. *CISA. (n.d.). (Accessed on: March, 2021) Retrieved from https://www.cisa.gov/about-cisa#:~:text=The%20Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29%20is,of%20meaning%20representing%20the%20Agency%20and%20its%20mission*
2. *US policy and the organization for security and cooperation in EUROPE: Report to the CONGRESS (2018) - United States Department of state. (2021, January 11). Retrieved from https://www.state.gov/u-s-policy-and-the-organization-for-security-and-cooperation-in-europe-report-to-the-congress-2018/*
3. *National archives and Records Administration. (n.d.). Retrieved from https://clintonwhitehouse4.archives.gov/WH/Work/021600.html*
4. *National archives and Records Administration. (n.d.). Retrieved from https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-Cybersecurity-strategy-15-years/*
5. *Joint statement on the Third US.-estonia Cyber dialogue - United States Department of state. (2020, December 01). Retrieved from https://2017-2021.state.gov/joint-statement-on-the-third-u-s-estonia-Cyber-dialogue/index.html*

6. *IC3 marks 20 years. (2020, May 08). Retrieved January, 2021, from https://www.fbi.gov/news/stories/ic3-20th-anniversary-050820*
7. *DOD's Cyber Strategy: 5 things to know. (n.d.). Retrieved from https://www.defence.gov/Explore/Features/story/Article/1648425/dods-Cyber-strategy-5-things-to-know/*
8. *Cyber security. (n.d.). Retrieved from https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf*
9. *Cyber security. (n.d.). Retrieved from https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0196.xmL*
10. *Cybersecurity planner guide. (n.d.). Retrieved from https://transition.fcc.gov/Cyber/Cyberplanner.pdf*