

**U.S. SEARCH FOR CYBERSECURITY: DOMESTIC
AND INTERNATIONAL DIMENSIONS**

*Dissertation submitted to Jawaharlal Nehru University
in partial fulfillment of the requirements for
the award of the degree of*

MASTER OF PHILOSOPHY

SACHIN TIWARI



**United States Studies Program,
Centre for Canadian, US and Latin American Studies
School of International Studies
Jawaharlal Nehru University
New-Delhi-110067**

2018



CENTRE FOR CANADIAN, US AND LATIN AMERICAN STUDIES
SCHOOL OF INTERNATIONAL STUDIES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI - 110067, INDIA

Date: 23 July 2018

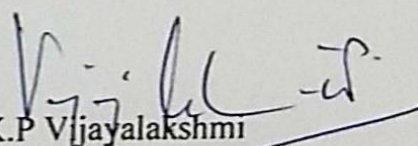
DECLARATION

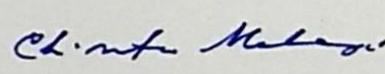
I declare that the dissertation entitled "U.S. Search for Cybersecurity: Domestic and International Dimensions" submitted by me in partial fulfillment of the requirements for the award of the degree of Master of Philosophy of Jawaharlal Nehru University is my own work. The dissertation has not been submitted for any other degree of this University or any other university.

Sachin Tiwari

CERTIFICATE

We recommend that this dissertation be placed before the examiners for evaluation.


Prof. K.P. Vijayalakshmi
(Chairperson/CCUSLAS)


Prof. Chintamani Mahapatra
(Supervisor)

*Dedicated to Maa, Papa, Rishi and Jenni for always supporting
me...*

Acknowledgements

The inspiration for this research work came from a call I received from my brother, expressing his displeasure over a cancelled shipment. It appeared that the Danish Shipping giant had been hit by the computer malware Petya Virus, which affected computers in 150 countries. The virtual effect on the real world was clear, so was the threat associated with sophisticated technology.

I'm grateful to my supervisor Professor Chintamani Mahapatra who patiently listened, improved and helped me to build the base for this research. His ability to take out time for me, irrespective of his demanding schedule, continuously reminded me of how fortunate I am. The strong foundational coursework on the U.S security, politics and society as part of my curriculum was crucial while forming the debates around the Cybersecurity. I'm thankful to Prof. KP Vijayalakshmi for helping me understand the research details of the primary sources originating from the US government. I am grateful to Dr. Saumyajit Ray for expanding my knowledge about the American society. Furthermore, academic engagement like CyFy (Cyber conference) and Raisina Dialog helped me to grasp the contemporary perspectives in the field of Cybersecurity while giving me the opportunity to acquaint various academicians and policy makers associated with this field.

This unique academic moment also gives me the opportunity to show my indebtedness to my family. I thank my family, especially my parents for having mountainous faith in me and all my life choices. Finally, I'm grateful to my friends in JNU especially Rashi, Aakriti, Blandina and Pradipto for helping me in my final drafting process.

TABLE OF CONTENTS

List of Abbreviations

Preface

Chapter 1: Introduction	1
Cybersecurity: Conceptual Framework	4
Major Themes in the Cybersecurity Debates	10
Development of Cybersecurity : National Security Issue	20
Chapter 2: The Politics of Cybersecurity: Cyber Debates in the U.S ..	25
Construction of Cyber Threat in the U.S	27
9/11 Attacks and the Internet Age	34
Global Cyber-attacks and Political Debates in the U.S	41
Privacy , Intelligence and National Security Debates	45
Strengthening US Cybersecurity: Nuclear as Response to Cyber-Attack....	49
Chapter 3: Transnational Cyber Security Threats and the U.S.	
Response	52
International Cooperation in Cyberspace	54
Threats to U.S in the International Cyberspace.....	60
The U.S Efforts for Cooperation Towards International Cybersecurity	70
Information Security: Issue of EU-US Data Transfer	70
U.S Legislation on Emerging Cybersecurity Environment.....	75

Chapter 4: U.S Response to Cyber-Attacks: Select Case Studies	78
Economic Espionage : Case of Cyber Attack on Google.....	80
State Attributed Attack: Case of Sony Pictures.....	87
Insider’s Threat: Case of NSA leaks	86
DDoS Attack: Case of Petya and WannaCry Malware	90
Case of Russia Involvement in the U.S Elections	96
Chapter 5 Conclusion	105
References	113

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
APT	Advanced Persistent Threat
CIPWG	Critical Infrastructure Working Group
CISPA	Cyber Intelligence And Sharing Protecting Act
CNCI	Comprehensive National Cybersecurity Initiative
CSIS	Centre for Strategic And International Studies
DARPA	Defense Advanced Research Project Agency
DoD	Department of Defense
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOJ	Department of Justice
EU	European Union
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for assigned names and numbers
ISP	Internet Service Provider
MILNET	Military Network
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NMS	National Military Strategy
NSA	National Security Agency
NSPD	National Security Presidential Directive
NSS	National Security Strategy
PATRIOT	Providing Appropriate Tools Required To Intercept And Obstruct Terrorism ACT
PDD	Presidential Decisions Directives
PRISM	Personal Record Information System Methodology

SCADA	Supervisory Control And Data Acquisition
TCP	Transmission Control Protocol
US	United States
US CERT	United States – Computer Emergency Readiness Team
USCYBERCOM	United States Cyber Command
USSSTARTCOM	United States Strategic Command

LIST OF FIGURES

Figure-1	Dimensions of the Cyberspace.....	7
Figure-2	Growth of Cyber Attacks.....	9
Figure -3	Organizations Associated with Cyber Security.....	49
Figure-4	Cost of Data Breach.....	94
Figure -5	Petya Virus Screenshot for Ransomware from a User.....	96
Figure-6	Example of Russia Disinformation Campaign.....	102

PREFACE

The Cyberspace is considered as a domain with its own separate sphere where the interconnection of electronic and computer networks allows for information communication. The creation and control of information via networked connections have exploited information to a new level and, thus, created vulnerabilities. The U.S. has used digital technology superiority to project power and propagate its interests. However, the characteristics of cyberspace i.e. low cost and open global network have allowed for threats to emanate ranging from individual(s) to the state(s). Cyberattacks, in case of formidable defense, have targeted the U.S private companies and civilian sector. The growth of ransomware industry is the outcome of it, with sophisticated cyber tools being employed to gain financial resources and disruption. In this context, America faces new transnational security threats due to open access to malicious cyber tools through the Cyber domain with serious implications on the its National Security.

In wake of the Cyber threats appearing at a much higher scale, the paradox of security and freedom mounts to concerns for privacy. These debates are also reflected in cyber threats where, for instance, individuals like Edward Snowden disclosed classified files of the National Security Agency have tremendously shaped the outlook of Cyberspace, and the emerging ‘paradox’ of striking a balance between the security and the Freedom. Yet, the mounting attacks have fueled the demand for more active Cyber policies. Overall analyses of the threats, their changing nature and the response of the U.S government would provide the framework for protecting national security interests.

The dissertation is divided into five chapters:

Cybersecurity represents the integration of technical structure of the internet along with political considerations. Chapter 1 covers the conceptual understanding of Cyberspace and its related aspects. The diffusion of technology and power has impacted the power relations between new actors and major powers. The major debates concerning the behavior of states and actors are discussed in the chapter. Laying down the basic framework, this study answers the questions and assumptions.

The general perception of American policy makers with regard to security threats have been highly influenced by events like 9/11. This is reflected in the formation of Cyber security policies in the US. Chapter 2 (**Politics of Cybersecurity: Cyber Debates in the U.S**) covers the major debates in the US throughout spectrum ranging from the executive, legislature, experts, private sectors and the public. The elevation of Cybersecurity as an important aspect of national security has also led to massive surveillance programs raising concerns for privacy. Maintaining a balance between active cyber policy and privacy has been given much emphasis.

Chapter 3 (**Transnational Cyber Security Threats and the U.S. Response**) discusses the transnational nature of Cyberspace and the emerging threats from it with regards to the US. Interconnectedness of internet has allowed for formation of a digital economy. The same phenomenon has also led to the emergence of Cyber threats. In the American context, states including China, Russia and North Korea have employed Cyber weapons to acquire technology and disrupt critical infrastructures. The mutual distrust has moved for militarization of the cyberspace and has limited consensus on international agreements on cybersecurity.

Based on domestic and international debates on Cyber security, select cases on the varied themes are analyzed in chapter 4 (**U.S Response to Cyber-attacks: Select Case Studies**). The US' response to cyber-threats has differed vastly as economic espionage has become a priority issue. For instance, China's attack on Google attack, North Korea's cyber-attack on Sony Pictures and political disruptions caused by Russia's interference during the election of 2016, were not dealt with in similar ways.

These concerns are discussed in the chapter where taking action(s) against the perpetrator remains a challenge even for a superpower such as the U.S. The search for cybersecurity has been dealt with in the dissertation.

Chapter 1

Introduction

“It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy”- Barack Obama, 44th U.S President

Diffusion of technology and power is an important element of cyberspace, which has decisively put the non-state actors and even individuals in a challenging position which only states could earlier afford as a privilege. The emergence of cyberspace has changed the way power is propagated and its diffusion takes place across time and space. For the United States, being a global power, the impact is quite meaningful. The U.S is vulnerable to attack through the low-cost entry, attribution, and open network used by the small nation-states and non-state actors in compromise for their resources and means of warfare.

The U.S developed the internet as a part of the secure communication amidst the threat of nuclear attack during the Cold War; it was only after the commercialization of the internet in the 90's that the true impact of it could be harnessed. Internet that began in the form of a secured connection between few institutions has emerged as an open global network. It has unleashed the force on all the domains especially the economy forming the information highway. In the words of former Vice-president Al Gore, “Electronic is to our age what coal and iron were to the industrial revolution”¹, defining it as a form of power. Setting the tone for the digital domain, *National High-Performance Computing Act of 1991*, U.S leadership in the electronic age was too secured.

The debates surrounding the usage of word cyber coincided with the U.S power in the form of economic benefits. The open unsecured network with the expanding user base of different motivations exposed the vulnerability in subsequent years. The usage was diversified with the individual, companies and the states all connected to the open global network. The relations were altered when hacking into the computer network resulted in a series of disruptions. In the wake of 9/11, serious debate about the security of the internet was discussed, with an individual ability to disrupt the global power. The emergence of the Patriot Hackers brought to the debate a new angle with the Chinese hackers attacking

¹ Speech delivered in U.S Congress on 18th May, 1989, “National High Performance Computing Act” establishing for development of national information infrastructure.

the US computing system and defacing the White House website, which later New York Times published it as, “the world's first hacker war”² (Smith, 2001). Expansion of the cybersecurity in the Department of Homeland Security paved its way during the Bush Administration including protection of the critical infrastructure.

The intensity of the cyberattacks has not been limited and rather has expanded with the harnessing of the interconnection of nodes to achieve the means. So-called ‘political violence’ was inflicted in the case of Estonia a member of NATO in 2007, leading to the question of the state targeted attacks. In another instance, the government of Georgia in 2008 was targeted with major services defunct for a period of time. The state use of the domain as a warfare added to the setting up of a separate Cyber command under *USSTRATCOM* in 2009. Yet, the actions of some individuals (insider’s threat) leaked the major classified files of government including personal emails in support of the freedom of information. The intricate links are complex where the classification of the action varies, and the response to the threats also varies accordingly. Efficiency and production which were the earlier goals to harness the power of the internet exist today also, but the increasing frequency of the cyberattacks especially of the threats emanating across boundaries makes it a major threat.

These disruptions in the post-Cold War globalized period were to phrase an important debate regarding the US Cybersecurity and its position in the world in an emerging information age. Former President Barack Obama’s consideration of the digital infrastructure as the National strategic asset has been dominating the government policy since 2009. Yet, the tenure was full of cyber-attacks in varying propensity on all fronts including political, social and economic with transnational origins. Internal leaks with the Bradley Manning’s case in 2010 culminating in Wikileaks and Edward Snowden Breach of NSA documents in 2014 exposed the vulnerability within the U.S establishment. On the other hand, major American private companies were cyber attacked resulting in severe economic losses and intellectual property theft. These conditions have deepened over the course and brought the question of the intricate balance between the civilian

² The attacks were in response to the U.S plane colliding with Chinese fighter jet in 2001 over Chinese airspace, leading to death of a Chinese pilot. The standoff saw Cyberattacks in form of intrusion including defacing Whitehouse website from May 6 – 13, 2001. (The New York Times , 2001)

security, private sector security and the overall national security of the U.S. Bringing an important question of the lack of clear perspective as to what contributes cyber threats and how the public-private integration can counter the threats to the US national security.

Cyberspace is a transitional domain for information and economic exchange; the offensive capabilities by the states make the international norm difficult. In case of the U.S, the possibility of “Electronic Cyber Pearl Harbor” was evident when Robert Gates, Obama’s first Defense Secretary created a dedicated Cyber command in 2009. The intrusive nature of cyber across boundaries has placed it on a different scale from other domain in the national security strategy of the U.S.

The chapter begins with a theoretical framework for understanding cyber as a domain and a detailed literature review on cybersecurity. The second part, discusses the major themes in cybersecurity debates with a review of the literature understanding the cybersecurity and its various typologies, connecting the idea of security to cyberspace. The third part of the chapter lays out the research question, research methodology for the research study to understand the context of cybersecurity for the United States which are further discussed in the subsequent chapters.

Cybersecurity: Conceptual Framework

The Cyberspace is the ‘fifth domain’ apart from land, sea, air, and space. It has its own space and the laws that are applied to it. Defining the characteristic of the Cyberspace includes various attributes such as; diffusion of power, ease of accessibility, low cost of entry, attribution i.e. anonymity (Choucri 2012; Nye 2010; Clark 2007; Castells 2014). The cyber domain position is characterized as a “transnational domain for information and economic exchange which contemplates the transnational nature of the internet and the problem of global governance” (Riggins, 2013). Definition of cybersecurity has constantly shifted to reveal the growing number of threats and new areas affected by the attacks. The case of UNGA resolution 53/70 where the definition modification from the phrase ‘may adversely affect the security of the state’ in 1999 to ‘may adversely affect States in both civil and military fields’ reflects the change in definition due to evolving nature and increased threats. In 2002 it was again replaced with “may adversely affect the

integrity of the infrastructure of States to the determination of their security in both civilian and military fields” (Radu, 2014).

The context of the cyberspace can be found in the science fiction novel *Neuromancer* by William Gibson (1984) where cyberspace is defined as, “A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system” (Gibson, 1984). Consensual hallucination here is the world of the virtual reality represented by the millions of interconnected computers containing endless data and the ability of the artificial intelligence changing lives. Though a work of fiction, the defining contours undeniably exists in the contemporary context with technology integration into the daily life with emerging concepts such as the virtual identity, virtual state.

The definition of the prefix Cyber and its associated terminology Cyberspace, Cybersecurity, Cyberattack, and Cybercrime are a challenge to define. The contours of the definition formed in the 1990’s have changed due to the evolving nature of technology; the definitions which are present in the domain have been extended to include the emerging threats. One of the comprehensive definitions by the International Telecommunication Union (ITU, 2008) defines Cybersecurity as,

“collection of tools, policies, security concepts, safeguards, guidelines, risk management approach, actors, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user assets.”

The security objectives recognized by ITU are:

1. Availability (of the data without any hindrance)
2. Integrity (Authenticity and non-repudiation)
3. Confidentiality (Information for the concerned user only)

The security aspects depend on the objectives which directly affect the intensity, access, and trustworthiness of the data key to security. In this perspective, “Cyber-attack” is further defined as an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a

computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.

According to another definition by Department of Homeland Security (2009),

“includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure”.

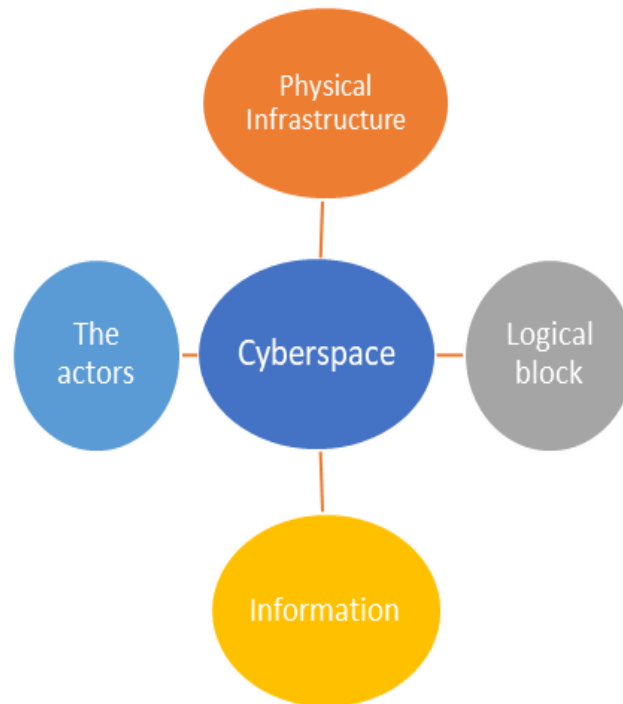
Yet, the disruption which has been experienced in recent times has remained more rudimentary where the securing of the information assets and collaboration remains a priority for the states, ignoring the civilian arena where the issue of privacy and securing information has emerged. The definition of the cybersecurity focuses more on technology aspect with securing assets, thus limiting the assessment of its impact on society.

Formation of Cyberspace

Cyberspace with its own space, environment, and boundaries is recognized as a domain. It is defined by the use of the automated systems that process information and disseminate information. Its composition can be understood by the way of the layered model where the four layers form the cyberspace.

- Physical Infrastructure composes hardware which includes; servers, computers, optical fiber cables, routers.
- Logical Block includes the building block as data format, transport structure on which various applications such as Word, Java are built.
- Information compromises in form of text generated, graphics, videos etc.
- The Actors are the users depending on the usage include; States, Non-states actors, Individuals, Private Organizations.

Figure 1: Dimensions of Cyberspace



Source: Layered Model of Cyberspace: Physical and Virtual Physical and Dimensions (Source: Clarke: 2010; Choucri: 2012)

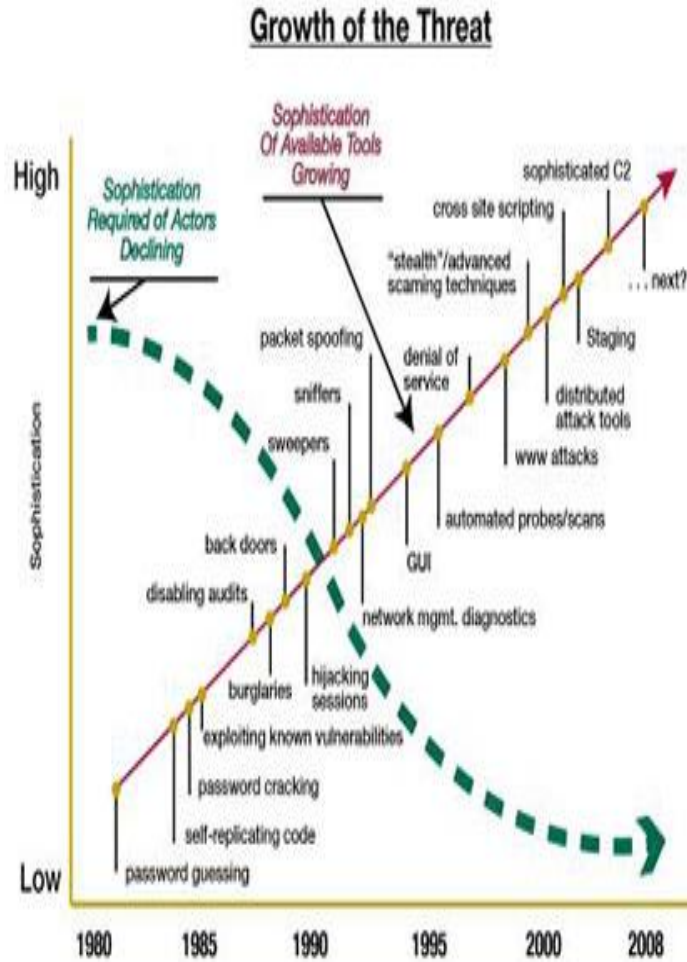
The interaction of the layered model produces the environment of interaction under which the cyberspace operates. Cyberspace is not a virtual world only transcending boundaries; rather it is also limited by the geographic constraints. Servers, internet connections are bounded by the sovereign rule of the state they are located in. The integrated network connection allows for the possibility to mount attacks on the computing infrastructure systems though it can be limited by the states in form of “regulatory mechanisms” such the “Great Firewall” of China. The international bodies as the International Telecom Union with consultation of states decide the format and structure under which Internet operates. Under this framework, various actors use the interconnection system represented by cyberspace utilizing it for the innovation purpose or for malign activities causing disruption and damage. (Choucri, 2012).

The Growth of Cyber Threats

The vitality of the critical infrastructure to the actors has resulted in the equation of the cybersecurity with the conventional domain, representing the strategic importance of cyberspace comparable with other domains. The case of NATO presents preponderance on the decision to target the adversaries waging Cyber-attack on Estonia in 2007 equating it with the physical armed attack. The applicability of the war to the cyber domain represents a fundamental change, where the malign actions are to be considered for retaliation via cyberspace or conventional armed attack. The anarchical behavior of a state's cybersecurity policy has shifted to a more conscious policy regarding other states. It would determine whether the agreement over the international law and behavior in the Cyber domain has limited agreement over the course of time. The concepts developed during the cold war are an important tool to examine the cybersecurity aspect, though limited in several aspects and criticized for being narrowly focused on power rivalry (Friedman, Singer 2013).

The objective and the subjective nature of security i.e. the real and the perceived threat may be underestimated or overestimated by the state (Baldwin, 1997). The states perceive the threat in both the manner, virtual in form of formations such as cyber catastrophe scenario which is yet to occur and real in form of cybercrime attacks which occurs on regular basis. The development of cyberspace into a critical domain of information and economic exchange, the capability to control information stored on the internet through pricing, altering, or securitizing information has become a point of contention among cyber actors of all stripes including states and non-state actors (Kiggins,2014). The condition arises from the fact that globalization has generated an increased interdependency, placing limits on what a single state actor can accomplish in cyberspace to ensure security (Nye, 2011).

Figure 2: Growth of Cyber Attacks



Source: The Growth of Cyberattacks in sophistication and means from 1980-2008 (Source: NATO Review: Changing Gear on Cyber Defense: Neil Robinson)

Information in the Age of Cyberspace

The vitality of the information has remained for societies to function and its development has also been the cause of conflict. The age of cyberspace can be described in terms of the information revolution, where the ability to disseminate the information is within fractions of second with the low cost of entry. The power projection has also changed with the multiple actors in the arena and the relations between the actors with control and action in cyberspace growing. Information can be categorized majorly into three types:

1. Free Information: The information which is free to disseminate to the audience depending on the no barrier, usually includes the scientific information available in the domain or via other sources.
2. Commercial Information: The information is available to the audience not free of cost, usually the intellectual property rights are covered in the form of the software licenses by major firms.
3. Strategic Information: The vital information of importance to the national security is protected under the encrypted information, it is vital for the maintenance of the asset against the competitor and the function of the critical infrastructure.

The information in the three categories in the cyber-age has largely provided the opportunity in the form of the Unlinking. “Unlinking allows thoughts to have a “life” of their own; thoughts gain separation from the person. Ideas and concepts flow from person to person without necessarily tying themselves to any one person.”(Abelson and Lessig, 1998). The attribution is an important aspect where the thought and ideas could be freely disseminated. Cyberspace has allowed the users to remain anonymous, post the information, and the creation of the digital community where the ideas related to the stand in favor or against the government can be shared. From the security perspective, it has emerged as a challenge where the difference between the information and misinformation has been narrow and the impact leading to “false memory” of the events. The very idea of information warfare has placed the data infrastructure and its integrity at apparent risk. Russia’s alleged involvement in the U.S Presidential Elections of 2016 placed the myriad of cyber attacks for disrupting the election of highest official position in the US.³ Information disseminated especially via social media has produced the emerging security concerns ranging from individual to the states. Dissemination of the “fake news” alter the facts from myth and turns events into via potential weapon to achieve interest, as Hillary Clinton on Russia alleged role in 2016 US elections puts it, “we were in the dark about the weaponization of social media”,(Clinton, 2016) highlighting the changing context of information in a digital age, and therefore, the study

³ Russian alleged involvement relates to hacking of the political parties database, tampering voting machines and creating fake advertisements to divide voters on key issues.

analyses the security issues, not just limited to the technical or commercial perspective but rather the information as a weapon leading to the online extremism and the political stability of the states.

Major Themes in the Cybersecurity Debates: Literature Review

The theoretical framework in International relations has linked the notion of power to the states. However, the presented framework is limited due to the complexities which cyber as domain presents. The nature of the cyber domain with evolving technology is shaping the balance of power and sovereignty, which are being regularly challenged by multiple actors. The contentious nature of cyberspace can be captured in political debates where the expansion of national security is promoted for threats emerging in cyberspace, and on the other hand legislating for the privacy and civil liberties (Carr, 2016). Joseph Nye Jr. (2011) in *CyberPower* considers the diffusion of power in cyberspace where the individuals and non-state actors can inflict tremendous harm. The U.S formed major new initiatives such as dedicated cyber command reshaping power domain; The emerging domain is 'imperfect commons', where the issue of effective cooperation and attribution are major challenges. The challenges present in the international arena, and cooperation on cyber norms among states, especially when cyber-attacks are transnational in nature has increased the vulnerability in cyberspace. In this perspective, the state control of information remains vital to its sovereignty and its power. The state-centric approach which has dominated international relations, now in the context of cyber development has to be accompanied by other actors (Kshetri, 2009). In other words, the power relations though still in favor of state are shifting with other actors in a challenging position and a leading example is of the private sector which has a significant control in the development and delivery of the digital technology including content in Cyberspace.

The politics of cybersecurity is represented by the security dilemma where the actions of one actor lead to the security buildup by another. In cyberspace, it is represented by the **offensive-defensive balance** i.e. the position that technology favors the ability to wage attacks leading states to develop offensive cyber tools to counter it. According to realist thinker Robert Jervis, anarchy reigns in an international environment and encourages the behavior of the states to noncooperation even if the state's share a common interest.

(Jervis, 1978). Variables such as the control of resources, values, leadership decision, new opportunities, and dangers change over time. The development of offensive weapons in Cyberspace exemplifies the state of Cybersecurity in the international arena, marked by limited cooperation among states and the failure to reach understanding regarding the norms for the security. One of the prominent factors is the low cost of entry, wherein the individual, non-state actors had the access to the interconnected global system. Clarke (2010) captured the need for the international cooperation where its salience and seriousness are beyond the single state capability.

Deterrence Debate in the Cyberspace

The deterrence i.e. signaling and credibility as espoused in the deterrence theory of Thomas Schelling (1960), “that the best way to deter is usually to commit yourself to retaliate in ways that will hurt your attacker.” The credible threats that would make the adversary to refrain him from doing something and making him compelling to do something are often utilized in the cyber domain. States and non-states actors push for the disruption in the critical infrastructure as the case of an attack on National Health Service (NHS) of UK exposed the greater vulnerability to the threats. One of the major problems in the cyber domain is the problem of attribution i.e. the identification of the attackers involved in the attack. Largely, the absence of any credible authority from the realist perspective is complemented by the attribution where the identity remains concealed. Also, the distinction between the offensive and the defensive weapons are often blurred as the same program information designed for defense purpose could be used for the cyber-attacks on the adversary. Author Fred Kaplan and Simon Schuster (2010) in their book, *Dark Territory: The Secret History of the Cyber Warfare* brought forward the perspectives of cyberdomain in war. The US utilized the Cyberspace in the operations starting from the Gulf war under Desert Storm (1991), Haiti attack, and Iraq war (2003). The development of the Stuxnet virus (2010) against Iranian Nuclear program saw the expanded capacity to wage a sophisticated cyber-attack. The disparate use of the cyberspace to inflict harm in cyberspace has developed leading to the proclamation of the security vulnerability and the emerging cyber strategies of states reflecting it.

The theoretical conception of Security Dilemma brings to the ‘Spiral of Mistrust’ which is more likely to take place when the offensive capability prevails over the defensive measures. The architecture of the internet was designed for the ease of usage, communication and hardly related to the security issues which would emerge in the later period. The utilization of the cyberspace for the offensive was the creation of the larger mistrust which had emerged and likely to continue in greater balance over the offensive capacity in favor for greater gains, which in other domains as the air, land, sea is much more difficult to achieve. Due to the architecture of the cyberspace, the attacker identity can be concealed by changing the address of the origin, using hacked computers for attacks. This represents fundamentally a new challenge as opposed to the cold war rivalry where the adversary was clearly identified and the tactics to counter it was developed. The concept changed in the 21st century with increased risk in cyber domain with the diffusion of technology allowing multiple actors with varied interest. The diffusion of technology is not a linear progression with the technical means but the structural trickle with the technology and the actors both associated have a greater role. In other words, the cost and the risks associated with fulfillment of the party making the threat are ascending. (Nye, 2011)

Critical Infrastructure Protection and the National Security in Cyberspace

Fundamentally, the debates surrounding the cyber as a security assessment largely stems from the perception of the technology itself i.e. the treatment of the technology as the means and the ends for achieving the objectives. Integration of critical Infrastructure with an automated system has developed dependency accompanied by the security threats. Due to the vital importance of the critical infrastructure as the electric grid, the state response had prioritized it as a national security. Edward Amoroso (2010) *Cyber Attacks: Protecting National Infrastructure*; Ralph Bendrath (2001), *The Cyber debate: Perception and Politics in US Critical Infrastructure Protection* focus on the critical infrastructure which remains most important for the U.S security and economy. Often the issue of critical infrastructure is added with other issues becoming highly politicized and a security challenge. The vulnerabilities as the ‘zero-day effect’ remain an important question as attempts to attack computer systems are increasing in number. Yet, the

premise of the government role in protection of critical infrastructure is limited due to the essential services provided by the private sector which accounts for over 80 percent services in the U.S. The information leaks by the contractors in form of “insider’s threat” also remains a major concern for securing the infrastructure where the vulnerabilities leaked in case of NSA leaks exposed the intelligence tools of National security Agency (NSA) which were later used in WannaCry and Petya ransomware attacks.

Similarly, Michael Krauz, *The True cost of the information security breaches and Cybercrime* discussed the growing vulnerabilities from the viewpoint of the nation’s security and the economy. The most important among them is the critical infrastructure on which the attack could be waged by State-sponsored groups or individuals. Raising an alarm on the vulnerability preparedness by the experts, it recommended a more proactive cyber response with a robust public-private partnership for the U.S national security. The question of the internal leaks especially contractors has been not dwelled into the problem of protection of national critical infrastructure.

The increased vulnerability of the critical infrastructure has pushed for the strong cybersecurity measures. Clinton administration pushed for major legislation in form of the Presidential Directive-63 for the protection of critical infrastructure. The defense measures are unable to cope with the incoming attacks, compromising sensitive data and critical infrastructure has led to the consideration of the active defense policy measures. In the research article by Angelyn Flowers, “*US policy on the Active Cyber defense*” analyzes the US policy of the active policy defense. Apparently, the passive defense is inadequate in wake of the massive attacks; the author outlines the Presidential directive (PDD-20)⁴ which lays out measures for the active cyber defense. Premising on the self-defense and the state sovereignty, the active cyber defense includes the offensive strategy including the first strike in case of the attack. The perspective of the active Cyber defense also has been brought in the article ‘*Defending America against Chinese cyber espionage through the use of active defenses*’, recognizing the digital espionage as the most important emerging threat. The Chinese hackers have penetrated the secure system of

⁴ In wake of massive Cyber-attacks and data leaks, PDD-20 was the Presidential directive by former President Barack Obama signed on 10th Oct, 2012. It changed the focused on the active cyber measures instead of passive defense.

several U.S government departments and acquired the sensitive data ranging from intellectual property to the national security plans. Determining it in the case of the Cyberwar, the article builds an approach to an armed attack (Alexander Melnitzky, 2012). However, the response in cyberspace is limited to attacks due to three premises; the anonymity, placelessness, and the ubiquity to identify the attacker. US private sector in recent times has been most vulnerable to the Cyberattacks, propagating the emphasis on the public-private partnership.

Information Security, Surveillance, and Data Privacy

The question of surveillance and privacy had forged new security implications for the citizens and its relationship with the state. In the book *“No Place to Hide: Edward Snowden, the NSA, and the U.S surveillance state”* analyzed the excessive government power which far stretches security concerns and developed in the form of “U.S surveillance state” where the citizens are being constantly monitored (Greenwald, 2014). Similarly, *Black Ice: The invisible threat of Cyber Terrorism* identifies that the terrorist not just inflicts harm, but manipulates information to change the outcomes of views and the opinion of the target. Its trajectory opened the discussion for the openness of the internet and the government capability to keep the radar on the citizens. It forms one of the prominent issues in the policymaking where the relations between of state and individual are redefining meanings amid the cyber terrorism (Dan Verton, 2003).

In this aspect, *“Google and the twisted Cyber affair”* discusses the case of the state mounted attacks on the private firms. Private firms are highly vulnerable to the cyberattacks as with the case of Google targeted in China along with cyber-attacks on other U.S firms. Similarly, *“The Cyber Threat to National Security: Why Can’t we agree?”*, explores the evolving nature of the cyber in shaping the way information is created, as a destructive force with states, non-state actors globally are able to influence the information. The devolution probably has risen especially considering the nature is transnational and the need for international cooperation. (Forrest Hare, 2010).

This leads to the creation of a new reality with almost two parallel worlds of real and virtual worlds. Thereby, changing the context of identity and the way we exercise our

behavior including all the actors. The prominence of the cyber as the national security threat proclaimed in the National Cyber Strategy Review of 2009,

“Ensuring that cyberspace is sufficiently resilient and trustworthy to support U.S. goals of economic growth, civil liberties and privacy protections, national security, and the continued advancement of democratic institutions requires making Cybersecurity a national priority”(Cyberspace Policy Review, 2009).

The linking of the security with the civil liberties, privacy has placed the prominence of the societal security along with the political and economic. Debates for the privacy, surveillance have been emphasized by the civil society, legislators. The protection of privacy is not to be seen outside the purview of security rather it is part of the cybersecurity and the debates on the stronger measure for privacy protection has strengthened the necessity of strong measures for it.

The Assessment of the National Security and the Cyber domain

“Security”, as a concept produced by Baldwin can be ambiguous, especially in reference to the roles concerning it i.e. what to protect and whom to protect. The state-centric model has dominated the security conceptualization. In “*Redefining Security 83*” Richard Ullman broadened the view with defining National Security as, “anything that interferes with the autonomy of states and the degradation of the human life” (Ullman, 1983). The human component forms the vital part of the security and the emergence of the policies in defining the security aspects of the states. Cyber attacks are leveraged not just by the states but rather by non-state actors and individuals, thus affecting the humans and state autonomy.

Security as defined by Wolfers (1953), “*the absence of the threats to acquired values*”. Later the definition of security was further elaborated by Baldwin (1997) to include perspectives of society such as security “for whom”. An important aspect of the understanding security is the Copenhagen School of Thought, which perceives the threats through the process of securitization, which defined as, “the process of state actors transforming subjects into matters of “security” an extreme version of politicization that

enables extraordinary means to be used in the name of security.”(Buzan et al. 1998). There had been an underestimation of the security policy approached in a narrow view concerning military security and the emergence of cyberspace as a threat reflects the new approach required to study it.

Approaching with the wider application of the concept of the security, Barry Buzan et al. (1998), considers the emerging threats as the economic, environment, human security in the purview of the security. Threats and vulnerabilities can arise in many different areas, military and nonmilitary, but to count as security issues they have to meet strictly defined criteria that distinguish them from the normal run of the merely political. They have to be staged as existential threats to a referent object by a securitizing actor who thereby generates endorsement of emergency measures beyond rules that would otherwise bind. (ibid, 1998)

The process of defining the securitization process is:

1. A Speech Act (The political language of the topic of importance putting it as a national security issue)
2. Identifying a threat frame (Language, Symbols, Virtuality)
3. Actions (In the form of policies, National Security Strategy (NSS), and institutions that are framed to tackle the threat).
4. Audience

Constructivism provides an important perspective on the process of an issue becoming a major national security issue. The Dilemma of the legislator while posing the problem of the cyber as security issues arise from the threat perceived not only from cyber-attacks but rather from other sectors also such as the rise of Terrorism. Cyberspace is also a sector as it is currently being securitized by state and non-state actors; it is a site of contention (Kasab, 2014)

The actors involved in the Cyber domain are not only limited to states rather they include non-state actors and individuals, who play an important role in the domain. Certainly, it is unique in the case of the cyber domain as the field is an entirely human-created domain,

unlike the other domains as the land, air, and water. The line of communication which is used for securing the nuclear reactors are also the same lines for disruption and can cause damages as in form of Distributed Denial of Service attacks (DDoS). Cyber is unique in this sense, as compared to the other technology which developed earlier is that: it combines fluidity and speed cutting across time and space. In another perspective, the information being created, stored and delivered is creating new avenues where the vulnerability is being exposed apart from the vast knowledge expanse it is being delivered. The form of alternative can be captured in works of terrorist outfits as Al-Qaeda, ISIS providing content to the created spaces where consumer's footprint is there for the fulfillment of the extremist propaganda.

Nazli Choucri, a cyber-expert at MIT in her book, *Cyberpolitics* puts forward the effect of cyber on politics, "the cyberspace is now a venue for competition among interest groups, and as an arena for conflicts and contention surrounding the increasing visible hand of the government" (Choucri, 2012). The state-centric views dominating the international relations are facing the new reality of cyberpolitics where the venues for interacting are rapidly shaping the environment with other actors. The problem of International cooperation in the cyber domain is limited due to the factors which separated from the traditional security (Bendrath, 2001), "No clearly identifiable actor; Lack of getting verifiable information; the capabilities of the enemy to wage an attack." The precedence of the Cyber as the 'threat politics' had been considered in works as (Nissenbaum, 2002; 2007) where the consideration of the language reflects and constructs the issues as threats.

The language of the cybersecurity refers to the cold war rhetoric and reflected in the political language. Peter Swinger (2014), *Cybersecurity and Cyberwar: What everyone needs to Know*; Steve Winterfield (2013), *The basic of the Cyberwarfare: Understanding the fundamentals of Cyberwarfare in theory and practice* outlined that, 'Swap in the words "conventional" and "nuclear" for "cyber" and "kinetic" and the new doctrine is actually revealed to essentially be the old 1960s deterrence doctrine of "flexible response," where a conventional attack might be met with either a conventional and/or nuclear response, the usage of the digital pearl harbor emphasizes the cold war rhetoric in

the political debates referring to the potential vulnerability of the critical infrastructure as the banking, electric grid, nuclear plant to the potential dangers. This brings the vital question of trust and mistrust in cyber age and cooperation within and among states which can be looked from the liberal perspective.

Framework and Cooperation in Cyberspace

The liberal theory has focused on the institution based order created after the World War II. These institutions have formed the bedrock of the modern government and economies today. Theory of Complex Interdependence (Keohane and Nye 1977) forms an important understanding of the growth of the digital technology across time and space. Interdependence as defined refers to “*mutual dependence*”, and in the world politics refers to “*the situations characterized by reciprocal effect among countries or among actors in different countries*”. The situation of interdependence is not the balance of power rather there is an existence of an asymmetry. Similarly, in *Cyber Power* (2011), Joseph Nye Jr. considers the diffusion of power in cyberspace where the individuals and non-state actors can inflict tremendous harm. The U.S has major new initiatives such as dedicated cyber command reshaping power domain. The emerging domain is ‘imperfect commons’, where the issue of effective cooperation and attribution are major challenges. The challenges present in the international arena, and cooperation on cyber norms among states, especially when cyber-attacks are transnational in nature has increased the vulnerability in cyberspace. In this perspective, the attack on the private sector of the US has caused ineffective cooperation especially with states like China and Russia. The attacks range from the cyber espionage including the stealing of the intellectual property, intrusion and using servers for malicious attack, financial losses, as the major security of the US government are with the private firms.

In the book *Private Sector Cyber: Can Active measure Help stabilize Cyberspace?*” Ariel Levite and Wyatt Hoffman (2007), makes an assessment of the defense measure employed by the private firms where the states have been unable to fulfill the security (pg3.). From the low intensity active cyber measure to the aggressive, the companies have started to resort to the threat emanating depending upon the changing nature of the private entities in the state (pg. 14.). It is a critical issue where the complexity of the state

legislation, ethics, and the security provisions are at risk from the foreign states and sponsored attackers. The industry-driven offensive measure may take place, presenting the question of the security compliance of the private sector in wake of a cyber-threat by the U.S government (Hoffman; Levite, 2007).

In the cyberspace, technology has leveraged the actors including national states, non-states actors to reap the benefits with the political, economic and social interaction leading to a more complex dependence structure. Development of the major protocols on the internet including the HTTP, ISP, and ICANN ensures a common connectivity to all actors despite the power propagation. International Cooperation on the Cybersecurity presents a picture of power and interdependence and the treaties between the U.S and China represents the complexity of interdependence and power in the age of Cyber. cyberspace does not operate in isolation; rather the international structure shapes the environment under which the norms are formed. States with different motivations perceive the cyberspace accordingly with several using the information as a form of cyber weapon to gain an advantage. The dilemma had led to limited cooperation in cyberspace among actors which is strictly based on a voluntary basis.

Development of Cybersecurity: National Security Issue

During the 1950 and 1960s, the most important gathering for the computer practitioner was the twice held Joint Computer Conferences (JCCs) and later the two were renamed as the Fall JCC and Spring JCC. These developed into the American Federation of Information Processing Societies (AFIPS). From this advent, the topic of computer security also called information security system and contemporary referred to national infrastructure system paved its way into the public view for the first time. (Ware, H. (2008), RAND and the Information Evolution: A History of Essays and Vignettes, RAND Corporation).

The control of the information is seen as an important proposition by the political scientist of the state control over the sovereignty and the national security. With the development of the information technology, the multiplicity of the interconnectedness, the control of the information flow is seen. The conference which laid an early disposition of the information related to the public view. In combination, the political,

economic and the societal views are also being framed having a physiological impact. From the technical perspective, the complexity of the system prompted the creation of the critical infrastructure system. The interdependence of the units produced various loopholes which are used as a vulnerability. The terrorist attacks on the U.S especially 9/11 attacks presented the vulnerabilities amidst the interdependence of the system which could be attacked. The actions of the U.S administration, thereby, have been marked with the decisions keeping in view of the defense structure of the information system.

The actions which commanded from the past decade is illustrative of such designs, most publicized being the Estonia cyber-attacks in 2007, Georgia disruptions in 2008. Consideration of the cyber as war has pushed for ‘militarization’, as a former cybersecurity adviser to U.S President Clarke (2010) puts it, “states are capable of doing in a cyberwar that could devastate the modern nation”. The similar proposition has been forwarded by the U.S officials and other intelligence officers. The military disruptions will rank always high, but it is the social disruptions which are occurring in prominence. This includes the recruitment of the terrorist fighters online, the rallying of the crowd with malicious intent, disruption of the democracy itself. The question of the privacy, intelligence in the age of cyber is under scrutiny as debates over the true impact of it are still being framed.

The case of cybersecurity presents an important step towards securitization where the subjective i.e. the perceived threats are the basis for the formulation of the security strategy. Due to the evolving nature of cyberspace, the prediction of future forms the basis represented in the language, policies of the government. UK National Strategy 2010 outline the damages can be inflicted on the military, industrial and economic targets. Emphasis is on the ‘age of uncertainty’ towards the emerging security environment and of which internet is a vital link of the global network.

The uncertainty is also promoted by the non-state actors, individuals ability to the treatment of the whole idea of the security can be captured in the inter-relationship of the states, non-state actors, and citizens which has an increased role in digital development owing to the diffusion of information. In treatment of the security effects of the cyber, the available studies concern with the notion of war as in case of cyberwar, cyberattacks the

most important aspect which this study forwards is that the *“Cyber domain is not in isolation to other domains , rather the online effect on offline is what matters the most.”*

The changes occurring in the digital world ranges from the kind of actors participating to the level of influence exerted by them. From the initial acts of the cybertheft, the states have realized the potential of the ‘Offensive’ i.e. the ability to attack in the cyberdomain.

This leads to the creation of a new reality with almost two parallel worlds: real and virtual. Thereby, changing the context of identity and the way we exercise our behavior. The prominence of the Cyber as the National security threats proclaimed in the National Security Strategy(NSS) released in December 2017,

“America’s response to the challenges and opportunities of the cyber era will determine our future prosperity and security...A, strong defensible cyber infrastructure fosters economic growth, protect our liberties, and advances our national security.”(National Security Strategy, 2017)

The integration of cyberspace in form of “internet of things” in all aspects of life has pushed for the creation of more security measures as attacks in the domain increases in number and intensity. Constantly evolving nature has produced more interdependence with the artificial intelligence integrating machines with human. The security risks in the cyberspace is a combination of the varied factors, including the threats from the arising from the internet architecture, intention of users, lack of cooperation of among states and human factors. The literature on the cybersecurity is more dispersed in the nature of threats emanating from the states to the non-state actors and the individual. The treatment of the subject of the cyber per se from a single perspective limits the focus of the threats which the U.S is approaching; there is a need for a pragmatic approach to the treatment of the Cyber threats. In this perspective, the study will analyze the changing nature of the threats and its implication on the U.S national security taking into consideration both the domestic as well as International dimensions.

Based on the above theoretical framework with literature analysis, the research answers the following questions:

Research Questions

- How have evolving Cyber threats changed the U.S. perception of national security?
- What are the major U.S policy perspectives on Cybersecurity issues?
- What has been the role of the U.S. in promoting international cooperation for developing cyber laws?
- How have Cyberattacks on private sector affected the US national security?
- How has the U.S. government responded to the involvement of foreign countries in cyber data breaches?
- How has U.S government dealt with the issue of internal leaks of documents and other related government data?

Hypotheses

The major Hypotheses raised in the study are,

A. The technological diffusion in the cyber domain has led to increased risks for the U.S. national security.

B. The transnational nature of Cyberspace makes it hard to arrive at international agreements and renders the U.S. response ineffective in wake of the Cyber Attacks.

Research Methodology

The evolving nature of the cyberspace and its interconnectedness present a complex picture of the security issues. On the theory, Erikson (2006) identified that the distance between the theory and the practice is distant. Second, is that the IR theories were developed during or before the time of cold war and contains most terms to deterrence, the balance of power, security dilemma, where the complexities of the evolving technology space as cyberdomain makes it difficult for analysis and application. Pragmatism as an approach bridges the gap between the theory and practice. Instead of the conflicting content of IR theories, the study uses the approach to bridge the gap. One of the core assumptions of pragmatism is that “we cannot flee from interacting with our environment and as the world keeps interfering with our beliefs, we have to readjust. In

such "problematic situations," a (very practical) form of "inquiry" helps us to find appropriate ways of coping with respective problems at hand”(Hellman; 2009). The identity is formed in a digital world and transcends boundaries with continuous change, therefore the synthesis of the theories and the practices followed are an important step to understanding the complexities of the digital age.

Therefore, the study analyzes various practices in the cybersecurity including policy making, actor’s behavior, and answer the research questions from a theoretical perspective. It is substantiated by the Case Study approach of specific Cyber-attacks and the U.S government response to them. The analysis is based on an interdisciplinary approach and examines data from political, law, technology, economic and other relevant fields. Research materials and data have been examined and collected from sources such as the Presidential Directives, Congressional Hearings, and the archival materials at the website of the U.S. Department of State, U.S. Department of Defense, Homeland Security, and U.S. Cyber Command.

The secondary sources include books, journal articles, newspaper reports and other information available on the internet. The reports from the major think tanks including RAND, CSIS, Brookings, Carnegie Endowment, and Chatham House on cyberspace have been used for analyzing the issue.

The design of the presented research covers the critical aspects of the security such as securitization, active defense policy, privacy in relation to the power structure in the cyber domain. The emergence of cyber as a domain with its own environment and boundaries is unique in the way it provides fluidity across other domains. The development of cyber as a secure network to the commercialization has also produced vulnerabilities, which are largely fixed in the history, technology, politics, and perception shaping the cyber environment. Interconnectedness had been used by states to conduct offensive cyberattacks with the advantage of attribution, low cost which was difficult to achieve in other domains. Separation of the civilian and the military sector has faded in cyberspace and it had allowed multiple actors to inflict harm. The uncertainties were combined with the cold war narrative of espionage, deterrence represented in the

cyberspace debates. U.S search for cybersecurity represents these embedded factors which have been discussed in the subsequent chapters.

Chapter 2

Politics of Cybersecurity: Cyber Debates in the U.S

The cyberspace underpins all the aspects of life today including economic, political and social. The increasing dependency has added to the threats emerging from cyber domain which are growing in number and sophistication. The perceived cybersecurity threats affecting the state, private industry and non-state actors vary in degree and intensity. Therefore, the various actors including the politicians, policymakers, technical experts, individuals hold divergent views of the cyberspace. The private industry strives for the innovation and growth of the technology, while the state sets the regulatory practices and the economic conditions for its expansion. Citizens are concerned for the security of personal information online.

The constantly evolving nature of the cyberspace places challenges the way the policy-making, law enforcement, and the technical standards for security are to be placed. The debate on cyber-threats is therefore not only about predicting the future, but also about how to prepare for possible contingencies in the present. As there have been no major destructive attacks at the cyber-level, decisions have to be made based on scenarios and assumptions (Cavelty, 2008). The protection of the cyber infrastructure has emerged as an important issue and directly influences the national interest. Major critical infrastructure, military installations, communication facilities are embedded with automated technology.

The private industry leads the cyber domain with 85 percent share in the cyberspace development. There is a substantive gap between government practice and policy regarding cybersecurity. Director of FBI until 2001 did not have a computer in his office, the very same year of the creation of the Homeland Security Department amidst increasing Cyberattacks. As Peter Singer and Alan Freidman (2014) put, “The field is becoming crucial to areas as intimate as your privacy and as weighty as the future of world politics. But it is a domain only well known by “the IT Crowd.” It touches every major area of public and private-sector concern, but only the young and the computers savvy are well engaged with it.” It is often reflected in debates among leaders, legislators, and technical experts.

The chapter analyzes the political debate among the US leadership in relation to the cybersecurity. The various aspects of the political, economic to the societal effects would

be analyzed in light of various legislation, congressional hearings, academic papers and media reports. The first section deals with the early history of the cyber in the context of the political debates. Then, the second section would analyze the important primary data such as Congressional documents, presidential directives etc. The third section covers the privacy versus security issue in light of surveillance, data collection by states, the role of foreign actors and the private sector. The fourth section examines the debates of offensive and defensive measures for security and the search for deterrence in wake of major cyber-attacks.

Rhetoric of Cyber-Politics in the U.S

Massive electric grid failure and electricity outages and loss of civilian lives due to the hacking of traffic computer systems are the perceived scenarios of cyber-attack; termed as cyber doom. Potential devastating cyber-attacks have been central to the framing of the cyber threats in politics. The vulnerability of the networked computer system remains high with the sophistication of threats emanating from cyberspace. The cyber threats in politics are framed in combination with the inclusion of the facts, future scenarios and including the past scenarios notably the cold war. The evolving cyber domain has brought challenges as to what constitutes an attack in cyberspace. This is reflected in the debates on the U.S national security with difficulty in defining cyber as a domain and the distinction between different types of attacks as cyberwar, cyber-attack, and cybercrime. Diffusion of technology has provided non-state actors such as terrorist groups with capabilities to inflict severe harm. Cyberspace is underpinned in all other domains like land, air, sea, space and has a direct impact on their security. The politicians remain mindful of the harm terrorism can inflict and the possibility of the destruction it can cause in the cyber domain.

The U.S Cyber policy rests on the maintenance of the internet as an open interoperable network accessible to all. The huge increase in the number of cyber-attacks has produced national security challenges including the protection of critical infrastructure, military assets, economic and social security need to be assured. Also, the online space has led to the citizen data being compromised and surveillance by the state and the non-state actors.

The position of the political leaders, private organization, and academia position on cybersecurity has emerged from the protection of the national security assets and the protection of privacy and civil liberties of the citizens. The framing of the cyber policies has been placed to secure the nation from various cyber threats emerging on one hand and the protection of the privacy of the individual on the other. The emerging paradox is reflected in the policy legislation with conflicting decisions among the US leadership.

Development of Cyberspace in the U.S

The launch of the ICBM (Intercontinental Ballistic Missile) in 1957 and Sputnik satellite by former the Soviet Union in 1958 had a tremendous effect on the U.S policy for technology development in space and Computer field. The Soviet Union was framed as a threat and the launch was a sudden shock with Senate Majority leader Lyndon Baines Johnson expressed “the profound shock of realizing that it might be possible for another nation to achieve technological superiority over this great nation of ours,”(DARPA, 2015). ARPA (Advanced Research Project Agency) was created by Congress in 1958 for rapid technology development in wake of the launch of Sputnik satellite. To establish the U.S leadership in technology domain the development of cyber was pursued facilitated by the provisions of the National Security Act of 1947.⁵ John F. Kennedy administration played a crucial role in expanding the technology field especially the space program.

The origins of Cyber in the available literature are marked with a difference of Cyber for communication (Carr 2016; Choucri 2012) and for defense (Erickson: 2001; Castells 1996; Clarke). An official paper by DARPA (Defense Advanced Research Project Agency)⁶ sheds light on the early development of Internet-initiated in form of Project Lincoln by the US Air Force in 1951 against the former Soviet Union in the form of the computer defense network for the coordinated action against the threats. The semi-automatic ground system paved the way forward for the interconnection system build across the U.S. Professor Joseph Licklider of Massachusetts Institute of Technology

⁵ Development of the interconnection system across the U.S was initiated for the secure communication by Department of Defense Directive 5105.5 . (1953)

⁶ Report released by DARPA details the initial history of Internet containing internal memos and files. *DARPA and the Internet Revolution Report* , 2015

(MIT) headed the way for internet development envisioning it for research and education purpose.

“In place of the 23 air-defense centers, he imagined a nationwide network of “thinking centers,” with responsive, real-time computers that contained vast libraries covering every subject imaginable. And in place of the radar consoles, he imagined a multitude of interactive terminals, each capable of displaying text, equations, pictures, diagrams, or any other form of information” (DARPA, 2015)

Initially, the internet was the secure networked connection between the academics for scientific development, information sharing supported by the US government. It expanded with the development of email in 1972 and distribution of more networked connection in the U.K, Germany, and the former Soviet Union. Federal computer systems were compromised in cases like ‘414s’ a group of seven teenager hackers. Senator Dan Glickman (D-Kan) called for congressional hearings to examine attacks on computer system. Similarly, FBI deputy director Floyd Clarke described that “a computer can be used like a gun, a knife or a forger’s pen” (Washington Post, 2003). Movies like War Games introduced the world of hacking to the audience. Even President Reagan watched the movie and inquired about the possibility of threats from the new arena (Clarke, 2010). Foreign intelligence threats were the most important until the commercialization of the internet in the 1990s. The sophisticated Cyber-attacks began with the expansion of the internet in the 1990’s leading to the intensified debates on its security.

Construction of Cyber Threat in the U.S

The early security threats emerging in the 1980s were incidents of hacking by technical experts and computer programmers mostly from universities such as Harvard and MIT. Hacking by the groups most notably 414s (a group of teenage hackers) increased in number leading to the call for examining and regulating cyber policy. Also, the threat from the Soviet Union of espionage and intelligence gathering pushed the measures for the security of computers. In response, White House issued the first directive NSDD-145 “*National Policy on Telecommunications and Automated Information Systems Security*”. NSDD-145 is an important legislation regarding the U.S stands on the cybersecurity recognizing the threats during its inception in the 1980’s. The vulnerability of the

networked system was recognized, “Telecommunications and Automated Information Processing Systems” are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements.” (White House, 1984)

The important points of legislation include the expanding responsibilities of NSA for the telecommunication and information. Also, it included the establishment of NIST steering group for overlooking the information security. The institutionalization of the security in the information technology paved the way for the creation of various departments supporting cybersecurity. This included the state control over the information in the digital domain with more military authority. The power provided to NSA was “contentious” as noted in General Stilwell and Linc Faurer letter to Secretary of Defense was not in full agreement regarding the “nature and extent of authority under NSA”(Burnham, 1985). It is important to note that the division of authority among the agencies remained contended especially over the civilian control and privacy issues. In 1987 Congressional Hearing House Government Operations Committee, Chairman Jack Brooks (D-TX), critiqued the role of NSA as “an unprecedented and ill-advised expansion of the military’s influence in our society,”⁷ and provided to the need for the civil-military balance. Congress balanced the civilian control over the information system with the *Computer Security Act of 1987*(H.R 145) and identified “computer system containing the sensitive information”.

The National Bureau of Standards (NSB) was formed with the task of developing computer standards program, training for the Federal computers and protects national networks along with NSA.”⁸ The development of the information technology and the institution related to security were important in the Gulf war. The Gulf war ushered in a

⁷ Cited in Michael Warner (2012), *Cybersecurity : A Pre-History*

⁸ The split of the responsibility between NSB and NSA was tilted again in favor of NSA under Directive-42 authorized in 1990 under George H. Bush administration restoring primacy over the protection of Information systems. *Computer Security Act of 1987* for computer standard program.

new era of modern technology with information warfare headed by the U.S planned for the dysfunctioning of the Iraq air defense system before the ground attacks. (Clarke and Knake, 2010). The making of Terminator movie series where the machines had taken control of the world revealed technology impact in form of highly developed AI (Artificial Intelligence system). Not just limited to novels or movies, the real-life acts such as Australian man opening up the sewer system in 1998 by taking control of the Supervisory Control and Design Automation (SCADA) system, emerged in the language citing the necessity for the protection of the critical infrastructure system. That very same year, the most important Presidential Directive PDD-63 was authorized by the Clinton administration. The Critical infrastructure is defined in the Executive Order (EO) PDD-63 as, “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” (NIST, 1997)⁹

The idea is that the image perceived in the popular media does have an effect on the framing of the view of the legislators, which in turn has an effect on the legislation on the larger question of the cybersecurity. In other words, the securitization of the Cyber domain with the ‘Speech Act’ governing the issues and moving into issues of the national security. The U.S legislators under the cold war environment legislated for the advanced technology development with the U.S leadership in the digital domain. The same voice was resonating by the former Vice President Al-Gore who pushed forwards for the Internet development and its commercialization, which would be discussed below.

Commercialization of the Internet: Clinton Administration

The effort’s for the rapid development of the Internet was pushed by Democratic Senator Al Gore, along with the ‘Atari democrat’¹⁰ who proposed for progressive legislation on the expansion of information technology. They viewed the Internet as a power for the US

⁹ NIST under Department of Commerce advances the development of Information Technology in the U.S. URL; <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

¹⁰ Atari Democrat was term introduced by Christopher Matthews and referred to the issue oriented politics focusing on the growth of American economy along with private sector and the technology industry. Lily Geismer (2016)

leadership in the digital age. The Atari Democrats pushed forward the politics for the commercialization of the internet and focused on stimulating entrepreneurship and private sector growth (Geismer 2016). The first major legislation for expansion of Internet was introduced by Rep. Al-Gore; the bill was cited as '*High-Performance National computing Act*' 1991 popularly known as the 'Gore Bill'. The bill changed the way internet was perceived mainly from the security aspect mostly limited to the government sector. It opened avenues for the growth of the private industry and building of the "back-bone" of the internet infrastructure backed by the US government.

The important consideration of the bill was:

- High-performance computing and associated technologies are critical to the United States economy (Section 208).
- It is appropriate for Federal agencies and departments to use the funds authorized for the Program in a manner which most effectively fosters the maintenance and development of United States leadership in high-performance computers and associated technologies in and for the benefit of the United States.

In the words of Al-Gore, "National Information Infrastructure will be built and maintained by the private sector. It will consist of hundreds of different networks, run by different companies and using different technologies, all connected together in a giant "network of networks," providing telephone and interactive digital video to almost every American." (Information Superhighways Speech, Al Gore, 1994)

"The information highway was placed with the federal budget of \$600 million for the expansion of the highway, leading to the development of several companies as the Bell Atlantic. The Clinton administration pushed for providing the access to all, the Administration not only wants to keep the goal of universal service but possibly expand it to include expensive services like video conferencing and swift access to databases, like a digital Library of Congress". (White House, 1994)

Moving forward, the interlinking of the security and commercialization appeared during the same time period. The administration pushed for the open free internet for the economic propagation of the U.S, leading the digital age. On the other hand, an initial

measure for securing critical infrastructure was placed amidst security concerns. The vulnerability of the internet was due to the architecture of the internet with huge expanse, as noted in a 1988 article on the design of the internet,

“No one can keep track of how many people use the Internet, how many machines it can reach or even how many sub- and sub-sub-networks form a part of it. The "backbone" of the network -- major electronic corridors established by the Department of Defense, the National Science Foundation, and others -- is obvious enough, but like the interstate highway system, it leads to successively smaller local byways and obscure private roads.”(Gellman, 2013)

Yet, the inevitability of the information highway was not deemed to be risk-free rather with was accompanied by threats. One of the earliest viruses was the Morris worm released in 1988 by one of the students at MIT, as evident other similar attacks by the university students became the mark of experiment and sometimes dissent. However, the sophistication to use the internet for the attacks grew with the commercialization and rapid adoption by all the actors. The early incidents of the Cyberattacks are merged with the notion of the Terrorism, as in the case of the 1994 attack by terrorists on World Trade Center in New York. The efforts for securing the physical security was accompanied by the network systems security which at the time was fast developing its embeddedness into the other sectors working including offices, homes and the potential for an attack on them were fast increasing. The result was the commission to study the impact on the critical infrastructure titled, “Commission on Critical Infrastructure Protection” (PCCIP) in 1996 for the designation of the critical infrastructure and its protection. The whole notion of the protection of the critical infrastructure stems from the urgency which is intertwined with the notion of the past, present and the future. The threat frame including the national security, state security, network security and human security are applied in the understanding of the threats.

Emergence of Cyberthreats: Clinton Administration and the Politics of Cybersecurity

Clinton administration was the first administration which witnessed and legislated on the Cyber-attacks, most of its origin lies in the other domains such as terrorism. The outcome was the executive order PDD-63 which defined the policy and the vision of the course of the cybersecurity.

Presidential directive 63 laid the Cybersecurity policy comprehensively and defined the major assets to be protected:

- Layout the attack from an adversary, “Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States”.
- Institutionalization of the federal with the creation of the office of National Coordinator for Security, Infrastructure Protection, and Counter-terrorism.
- The primacy of the role of the Public Private Partnership Government institutionalization which includes the resource allocation from \$250 million in 1998 to \$2.01 Billion in 2001. (White House, 1998)

The national effort to develop the critical infrastructure system in the U.S with the directives lacked a comprehensive approach and the several gaps revealed in the review report by Gaston Gianni and Barry Snyder regarding the implementation of the Presidential Directive 63. The report highlighted the lapse of security and the effective implementation of the directives by security agencies,

- Many agency infrastructure plans were incomplete.
- Most agencies had not identified their mission-essential infrastructure assets.
- Almost none of the agencies had completed vulnerability assessments of their MEI assets or developed remediation plans. (White House, 2001)

It provided for the lack on the part of the agencies even to identify their respective cyber critical infrastructure and, the very notion as to what is critical for the national security. The review was published on March 21, 2001, and provides an important glimpse into the

legislative enactment and its implementation by the government and security agencies for strengthening cybersecurity in the US.

9/11 attacks in the Internet Age

Attacks of 9/11 waged a new debate over the use of the Cybersecurity, as the 9/11 commission reported to the unpreparedness of the U.S citing President Clinton speech in 1998 that states,

“As we approach the 21st century, our foes have extended the fields of battle - from physical space to cyberspace... Rather than invading our beaches or launching bombers, these adversaries may attempt cyber-attacks against our critical military systems and our economic base... If our children are to grow up safe and free, we must approach these new 21st century threats with the same rigor and determination we applied to the toughest security challenge of this century.”(White House 1998)

The concerns for the security of the information security especially with the expansion of internet during Clinton administration with stronger policies pushed for the security of the development of cyberspace. Securitization in the form of the ‘Speech Act’ by political leaders and computer experts over emerging cyberthreats was legitimized by the government in the form of the legislation which led the way for the cybersecurity becoming one of the top priorities for the U.S administration. It was reinforced by the 9/11 attacks, where the vulnerability of the U.S from the attack in cyberspace by the terrorist could lead to the devastating effects. The referent objects were the state and the individual and the collective security was the national security from the cyber-attack.

Creation of the office of the President’s Special advisor for Cybersecurity after 9/11 attacks marks an important quotient in the institutionalization of the cybersecurity efforts by the U.S under Bush administration. This was deemed in the form of the interdependence among the U.S agencies such as FBI, CIA, and Department of Homeland security for the information sharing and in the form of the Joint Task Force-Computer defense under the command of the Department of Defense.

Patriot Act 2001 and *FISMA Act, 2002* were the outcome of the commission on 9/11 reports, though they were not directly related to the cybersecurity. Indeed, the question

of surveillance was rated high in the reports, where the agencies were provided a free hand in conducting the inquiry. This security aspect in the coming years will find strong resistance to the balance of privacy and an open, interoperable system.

The title –II of the Patriot Act provided with the enhanced surveillance procedures to the agencies. These included:

- Sec. 220 provided for nationwide service of search warrants for electronic evidence.
- Sec. 204 of FISA lays out the exclusive means by which electronic surveillance and the interception of domestic wire and oral (current law) and electronic communications may be conducted.

Along with it the records of the citizens including the banking transaction, credit card to resemble for a longer duration with the federal agencies. Creation of the Department of Homeland security was an important measure for the National security of the U.S and the handling of the Cyberstrategy. The National Strategy paper of 2002 by Bush administration mentions the changing security environment with emphasis on terrorism, “Terrorists are organized to penetrate open societies and to turn the power of modern technologies against us” (NSS, 2002). The extensive power granted under the Patriot Act led to the concern especially the surveillance measure’s curtailing privacy of US citizens.

Strengthening the Cybersecurity in the Digital Age: Bush Administration

National Cyber Strategy to Secure Cyberspace in 2003 was one of the most comprehensive national strategies by the U.S Congress released by the Bush administration after the 9/11 attacks and outlines the security format including the individual, private to the public in the web of national security. It's important to note the instance on the counterterrorism as one of the major factors driving the policy legislation. Constituted just after the 9/11 attacks, the impetus of the events in other domains has a considerable effect on policy formation. The language, rhetoric and the stance changed from there on and the cyberspace is not an exception to it. Looking at the debates during the formation of the National strategy provides a glimpse of the security component of

the cyber and how it came to be regarded as one of the national security priorities (Etzioni, 2011).

The *National Strategy to Secure Cyberspace* (2003) identified five levels to address the cybersecurity problem. These included: Home User/ Small Business, Large enterprises, Critical Infrastructure, National Issues, Global level were identified as a priority. Also, the role of the Department of Homeland Security in preparation and securing national comprehensive plan was expanded. A major part of the cyber defense was the funding on the research and development initiated under the Office of Budget and Management (OMB) with the director of Science and Technology for preparation of Annual Federal Cybersecurity government agenda.

Several components of security were passed to the Private Sector in the Bush administration which was earlier in-house. The preeminence of the private sector will develop as the most important critical component, as the major services handling and the research development are managed by the private sector. Many authors have implied cyberspace as the domain of private (Carr 2016; Nye 2011), with the development of Public-Private partnership and an enhanced role of the private sector. Under Clinton administration, the pretense for the strategy was to avoid the governance led rules and regulations that would hinder the development of the private sector and realize the full potential in the innovation, development, and compete on the global scale (Cavelty, 2008).

The federal role is mentioned in the effort to identify, prioritize and coordinate the protection of the critical infrastructure and key resources to deter, prevent and mitigate the risks (HSPD-7, 2003). The private sector is best equipped and structured to respond to an evolving cyber threat. A federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs. Yet, the case of Titan Rain series of disruption from 2003 allegedly by China led to the low rate of disclosure from private companies.

The number of the incidents reporting an attack has gradually grown with the number of actors involved. The diffusion of technology played an important role in the Estonia attacks of 2007 and the Georgia where patriot hackers supported by Russian state

launched cyber-attack. These are reflected in widely publicized articles as by Colonel Charles Williamson of US Airforce for putting the military botnets on unclassified networks and later Richard Clarke (2010) former cybersecurity adviser to Bush administration. Daniel Lungren Chairman on the Subcommittee Emergency Preparedness, Science, and Technology describes the increasing cyber attacks as the ‘Soft underbelly’ of the U.S (Lungren, 2005).

Reference to the war imagery has been an important component, especially the usage of the word Electronic Pearl Harbor. The construction of the threats in the form of the worst threat scenarios has been divisive in the form of the speeches by the leaders, policymakers, and defense experts and accepts by the audience. The term associated with the historical trauma suffered from the unforeseen attack has been deeply embedded with the policymakers rushing for the new threats emerging from the cyberspace.

The reference to the security can be placed in the manner of the “collective images of security” (Krauser, 1986). The collective images of security were placed when the images of China shooting the weather satellite in 2008 led to the questioning of the U.S capabilities in the response to the growing cyberthreats. The sophistication of world affairs in wake of globalization had led to the government, policy experts center their attention on the capacity of the adversaries, leaving the major question of intent (Bendrath, 2001). The auto-satellite tests led to the conclusion of the “wake-up call” for the U.S, with the Congress stating, “[i]t is the Sense of Congress that the United States should place greater priority on the protection of national security space systems.”(Ambassador Mahley, Space Policy Institute,2008). Bush administration called for the Comprehensive National Cybersecurity Initiative (CNCI) in 2008 in the National Presidential Directive 54 especially for protecting the federal network and the counterintelligence for threats from foreign states and hackers.

Obama Administration and Cyber Policy Review 2009

The Cyber Policy review of 2009 referring to as the *Clean –Slate Review* was issued after the Presidential order to review the Cybersecurity policy of U.S. It is an important consequence of the rhetoric of the cold war in the leadership tone published in the paper. The Cyber policy review puts,

“After the launch of the Sputnik satellite in October 1957, the United States is in a global race that depends on mathematics and science skills. While we continue to boast the most positive environment for information technology firms in the world, the Nation should develop a workforce of U.S. citizens necessary to compete on a global level and sustain that position of leadership”(Cyber Policy Review, 2009).

The effect is double fold where on one hand the maintenance of the technical superiority is leading to the creation of new vulnerabilities which are exposed time and again. On the other hand, the massive buildup in the cyber infrastructure is pushing the structures of the other states in the quest for the greater edge in the mutable field. Realist thinker’s conception of the credible deterrence which involves the use of force as a threat to adversary can be put in the context where the attack capability in cyberspace is pushing for other states to militarize cyberspace. In the case of cybersecurity, it becomes more challenging where the offensive is easier than the defensive to conduct. The buildup of the whole system architecture is such that the new vulnerabilities would continue to risk the emerging threats. Zero-day exploit i.e. new vulnerabilities in the network system are used by adversaries to mount cyber-attack.

In view of this security review, the key recommendation which formed of the Cybersecurity policy 2009:

1. Appointment of cybersecurity policy official for coordinating cyber policies.
2. Designate Cybersecurity as one of the Presidents key management priorities.
3. Designation of a Privacy and Civil liberties official to NSC cybersecurity directorate.
4. Development of the U.S government position for an international cybersecurity framework policy.
5. Enhancing the Public-Private partnership.
6. Issuing of a strategy that addresses privacy and civil liberties interest.

The analysis of the document delves into three important themes which it addresses:

- Official
- International Cooperation Framework

- Privacy, Surveillance

President Obama on broadening the scope of the consideration of the asset moved, “From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient.” (White House, 2009)

Yet, the question of the overlapping structure with responsibilities issue of the greater federal control ‘over who is in charge’ remained. The incoherence in the policy structure continues with the categorization of cyber-attacks, where the Mike McConnell puts it as cyber as a domain of warfare and develop the offensive’, while Howard Schmidt White House Security advisor during Obama administration denies that the U.S is facing a cyber-war pointing to the exaggeration of threats. The continued primacy of the cyber threats in the political debates owes to the growing number of cyber-attacks which are reflected in the offensive-defensive debates.

Militarization of Cyberspace and the Political Debates

Development of the cyber weapons is twofold with the defense on one hand and the ability to retaliate in case of cyber-attack is other. Technology diffusion had led to various states utilize the cyberspace for waging attacks as a major issue for the balance of security and marinating an open internet with privacy safeguards. The intensity regarding the Cybersecurity during the Obama administration provided an impetus where the Cybersecurity was placed at the top of the National security of the U.S. This stemmed from the number of increased attacks not only including the major attacks occurring such as the Estonia 2007 DDOS attacks, Georgia attacks in 2008, but also cyber espionage against U.S multinational corporations such as Google in 2010. The attacks not only compromised sensitive data but also included the daily attempts to intrude the main servers to gain access to the central system. The view can be held in the manner that as the technology grows more sophisticated the nature and trajectory of the attacks has also increased which will continue in the future. In an Op-ed published in the Wall Street Journal, President Barack Obama presented a scenario of the failure of the critical infrastructure system as,

“Across the country, trains had derailed, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several states had shut down, contaminating drinking water and causing Americans to fall ill. Our nation, it appeared, was under cyber-attack. Unknown hackers, perhaps a world away, had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water, and other critical infrastructure systems.” (Obama, 2012)

In light of the emergence of the threats, “The United States needs to do more to develop an offensive cyber war capability rather than just focus on defending its networks from attack, says the chairman of the House Cybersecurity subcommittee.” (Rep. Jim Langevin (D-R.I.). These worst-case cyber scenarios reflected the concern of the Obama administration and the efforts to pass the Cybersecurity Act 2012 through Congress, which faced resistance on basis of the privacy. Politicizing the issue on basis of the critical infrastructure ranged from Clinton administration and forms the basis for more aggressive Cybersecurity policies.

Global Cyber-attacks and Domestic Debates in the U.S

The year 2010 was marked by the serious confrontation in the field of the Cyber-attacks with the question of the espionage by China leading the front of the U.S multinational companies including Google and involved the serious question of the Intellectual Property Rights. The edge that the U.S has as a leading power rests on the innovative development that took place in various fields and now the leading technology has been passed into the hands of adversary countries which itself have a leading computer technology. Obama administration emphasized the economic benefits from the digital trade which far exceeded the security issues emerging in the cyberspace. Digital Trade grows over 44 percent from 2010 to 2016 forming 6 percent of US GDP. What emerged is the maintenance of technological superiority with technological innovation, the safeguard of intellectual property. Followed by the same time were multiple attacks from foreign states including China for making gains with trade secrets and the latest technology.

The militarization of the cyberspace has been taking a form of dedicated cyber military commands with the development of the offensive cyber weapons. The U.S created the dedicated cyber military command in 2009 in the wake of emerging cyber threats. The creation of the ' Stuxnet' virus in 2010 forms a leading debate on the offensive use of cyber as a weapon which attacked the Iran centrifuge system reaching to the sophistication of technology created and the deployment by the administration against the state (Sanger:2012). The usage of cyber weapon was also discussed in Libya operations in 2011, where the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyber-offensive to disrupt and even disable the Qaddafi government's air-defense system, which threatened allied warplanes (New York Times, 2012). The offensive side of the cyber is well recognized within the U.S political circles and the use of it was put in the legislation.

From the realist perspective, the power propagation is essential to the conduct as well as the national interest. In the case of the Cyber, both are at stake considering the situation of the myriad attacks by countries involving China, Russia, Iran and North Korea as principal actors recognized. The innovation especially in the field of the defense, economic and technology have placed at the forefront of the world power in the post-cold war period. The U.S leadership in internet development ensured the economic development which paved the way for the Gore-Clinton an essential ingredient to fuel the new thriving development of U.S and leading forward.

Questions poised for the U.S national security included the sophisticated attacks which were taking place. The International Strategy for Cyberspace (2011) aptly mentions two important points, *“The offline challenges of crime and aggression have made to the digital world.”*

The nature of the participation was particularly set in the cyberspace in the defense department strategy document in the treatment of the Cyber as a domain and the conduct of the U.S.

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace potential in its military, intelligence, and business operations;

- Employ new defense operating concepts, including active cyber defense, to protect DOD networks and systems.
- International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e., sea, air, land, and space), also apply to the cyberspace domain. (DOD, 2015).

The strategy came out amidst the increasing cyber-attacks, expanding the scope of intelligence collection for the concerned authorities. During the time the U.S suffered cyber-attacks from states including Iran on the banking institutions. The maintenance of the credible deterrence cannot take place without arbitrary threshold i.e. punitive punishment. Iran's actions did not cross the threshold for the offensive action of the U.S, highlighting the difficulties of deterrence in cyberspace and the reason why cyber attacks are on the rise over the years.

The realm of the cyberspace poses from the challenges that the *Cybersecurity Act of 2012* introduced by Senator Joseph Lieberman, failed to move through the Congress, particularly on the cost to the private sector and the privacy issues from the civil advocate groups. Negotiation of the boundaries between the public and the private and between the economic and the political thus couples the network-fragmentation implied by "cyber" with an understanding of business and government as sharing the same goal. (Nissenbaum, 2009)

Obama administration signed a classified document in 2012 under directive PDD-20, paving the course for the development of Offensive and Defensive capabilities, militarizing the nature of Cyber operations with active engagement,

"Offensive Cyber effect operations can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging".(White House, 2012)

One of the major purposes was to identify potential targets of national importance, where offensive operations could leverage the U.S position. The strategy was to provide a favorable balance of effective response and low risk associated with different instruments

of national power, establishing and maintaining offensive capabilities which are integrated suitably with other U.S military capabilities in other domain (PDD-20, 2012). The case of the Stuxnet virus in 2010 which destroyed the Iranian centrifuge elaborates the offensive capacities which integrated the action plan supported by capabilities in other domains.

Regulation Debates: Private Sector and Cybersecurity

The background was the mounting attacks especially from China which included the cyber espionage activities against U.S companies like Google and against the federal executive branch department as Department of Defense. It involved the disclosure of the information from the private companies to the federal agencies and the selection of the NIST for the development of the security standards. The information sharing debate tends to put the “top-down approach” as stated by McAfee Vice President, on private firms where ‘the rapid pace of innovation in the private sector is sensitive to the stringent cybersecurity requirements’. The use of the cyber as technology to achieve the political means has gained the momentum with the attacks on Estonia and the regular intrusion on the system is not confined to gain economic or military gains but rather achieve the political means.

Executive order 13636 was passed for the strengthening the protection of critical infrastructure by working to strengthen incentive system for the private sector due to the increasing number of attacks. The similar goal was iterated in Republican Task Force in 2011 for the incentives to the private sector. However, the protection of the critical infrastructure put in the threat framework of legislators have vulnerabilities in the design of the SCADA which were breached earlier in 2000 by the Australia at Maroochy Water service with the attempt to enter the critical infrastructure as mention in report, *Making the Nation Safer: The role of Science and Technology in Counterterrorism*(2011). The proposition was that “the design of today’s supervisory control and the data acquisition (SCADA) systems has been designed with little or no attention to security”. For example, data in SCADA systems are often sent “in the clear.” Protocols for accepting commands are open, with no authentication required. Control channels are often wireless or leased

lines that pass through commercial telecommunications facilities (National Research Council, 2011).

The major concern of the Obama administration pointing from the, “In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home.” The scenario of the U.S Cybersecurity in form of the government efforts has been effectively captured in the report: ‘*National Strategy, Roles, and Responsibilities*’ need to be better defined and more effectively implemented.

The Government Accountability Office (GAO) report outlined that the government issued number strategy-related documents with wide topics over the last decade, many of which address aspects of the cybersecurity and protection of critical infrastructure. The information sharing between the federal system and the private organization have remained a challenge in detecting and sharing of threats. “However, no overarching Cybersecurity strategy has been developed that articulates priority actions, assigns responsibilities for performing them, and sets timeframes for their completion” (GAO-13-187). The tussle between the federal government efforts for the regulation has limited effect on the lack of coordination among the agencies and the gap between the private industries.

Privacy, Intelligence, and National Security

The narratives of the political debates on the question of privacy and National security are intermittently connected. 1974 Privacy Act enacted by Congress paved the way for regulating databases, and considered “the right to privacy is a fundamental right protected by the constitution of the United States”. Similarly, States of California passed the 2003 Data protection mandating the companies to notify the citizens of the data being collected by them. Since then, 47 States, District of Columbia, and other U.S jurisdiction including federal agencies to protect the sensitive personal information (Charles, R. et al. , 2014). In the wake of the 9/11, the PATRIOT ACT was passed by Congress which gave greater power to federal agencies for data collection including surveillance and some sections allowed for the bulk collection program of the U.S citizens.

Data collection and sharing have remained a complex topic, especially concerning National security. Private sector which holds the majority of data has remained skeptical of sharing with a federal agency, seeing it an impingement on their freedom. The *Cybersecurity ACT of 2012* failed to pass through Congress on the question of the handling and sharing of the private information. Eventually, Cyber Intelligence and Sharing Protection Act (CISPA) was passed, which legislated for the voluntary framework agreement between the private sector and his federal agencies. The question of privacy of the data in the information age is considered especially in wake of the espionage attacks, terrorist usage if the social media sites, fraudulent banking.

Another perspective on the question of privacy can be looked at in the manner of 'Psychology Politics' where the technology has narrowed the boundary between the private and public. More and more citizens have revealed their private life on the social media sites willingly. Holding similar stand on the issue, Supreme Court in United States v. Miller, "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed" (Mund, 2018). NSA leaks by Edward Snowden revealed a vast amount of data being collected by the National security agency and these included the data collection via from U.S citizens apart from the foreign states. In wake of the pressing demand for the protection of privacy, Congress passed the *US Freedom Act* in 2015. The Act curtails the power of federal agencies in bulk data collection of the U.S citizens amending the various section of the Patriot Act.

Net Neutrality and Freedom of Internet Debates

Net Neutrality has been a major issue of debate for consumer protection and privacy. FCC (Federal Communications Commission) decision to amend the Open Internet order 2015 changed the treatment of the broadband providers from 'information carriers' to simply carriers. Broadband Carriers are required by law to treat all data equally and the storage of the ISP i.e. a user internet address data. There are apprehensions about the intention of the user privacy online and the data being used by the third parties without their consent. There are dissenting voices with several individuals, grass organization,

political parties in open opposition to it. Political leaders from both Democratic and several Republicans are of the opinion that ending Net Neutrality would end “equal access” to all, advocating the internet as a public good available to all. Industry companies as AT&T opined that the policy-making had been inconsistent with constant changes and recommends for “Internet Bill of Rights” by Congress ensuring neutrality, transparency, openness, and privacy for all citizens,” which lacks in the current situation(Stephenson, 2018). The primary argument of FCC is that it regulates the broadband companies while the larger IT companies as Facebook use the same connection for the greater control of the market, restricting the small carriers and startups. The state had acquired position for the Net Neutrality under “Restoring Internet Freedom”, states including Washington, Oregon had enacted Net Neutrality Bill and 29 states are pushing the Net Neutrality bills. One of the major positions of the bills is the protection of the “personally identifiable information” and restricting the providers from misusing it. (Greenberg, 2018).

The debates on the privacy are two-fold with the consideration of the privacy, civil liberties and the protection of personal information online, financial fraud and terrorist attacks. Civil rights organization Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) have strongly advocated for the data protection laws. NSA had been sued for conducting unwarranted mass surveillance and several court cases have been filed by these organizations. However, “the cases were dismissed in the courts because plaintiffs could not prove they had been the target of surveillance because the surveillance was secret” (Purba, 2016). Public perception has remained in favor of the information sharing by security agencies. Recent assessment has shown that the cyber-threats considered being top security concerns. The rise in the number of cyber-attacks especially the low profile as cybercrime involving personal information leaks has put privacy at stake.

Internal Leaks: The Human Factor in Cybersecurity

National Strategy document mentions the Cybersecurity in line with the other domains as space, air, and oceans, where the rise of a cyber-attack is preminent. Explicitly the document mentions the aggression by Russia. Another important dimension which has

marked its presence in the security is the Human factor, the role of the contractors is important in understanding the Cyberattacks as Government Accountability Report 2017, *Cybersecurity: Actions Needed to strengthen US capabilities* layout for, “strengthen oversight of contractors providing IT services.” The case of WikiLeaks would be discussed in Chapter 4.

The blurring of the line between the information and misinformation is one of the critical aspects under which the perspectives for the National security are taking shape. President Barack Obama (2016),

“Because in an age where there's so much active misinformation, and it's packaged very well, and it looks the same when you see it on a Facebook page or you turn on your television, wheresome overzealousness on the part of a U.S. official is equated with constant and severe repression elsewhere, if everything seems to be the same and no distinctions are made, then we won't know what to protect. We won't know what to fight for.” (White House, 2016)

Terrorism is also well paced in the rhetoric of the cyberpolitics, where the diffusion of technically allows the non-state actors to equate harm and the continuation of its program. “They [ISIS] still pose a significant threat to us in the cyber domain,” Sen. Gary Peters (D-Mich.). “Probably the most significant threat we face as a country comes from the cyber threat that we must deal with especially when placing the context of the social media in recruiting of the fighters of which several hailed from the U.S”. (Hill, 2017)

The disruption of the U.S elections in 2016 by Russia emerged as a critical issue of the cyber usage by an adversary in an offensive manner. Effectively, information is being used as a weapon to gain the political and economic means. Similar, reports of the disruption have been carried in the western democracies including France, Germany, Sweden, and Ukraine. Admiral Mike Rogers NSA chief and Cybersecurity commander responded that,

“This was not something that was done casually, this was not something that was done by chance, and this was not a target that was selected purely arbitrarily. This was a conscious effort by the nation-state to attempt to achieve a specific effect.”(Rogers, 2016)

In response, the U.S Congress passed the, “*Countering Foreign propaganda and Misinformation Act*”, in the light of the allegation of the disruption of the U.S election in 2016 by Russia’s sponsored hackers. The information used to inflict harm is not new, but the expanse of it using cyberspace has led to its “weaponization” and its usage for strategic gains.

Strengthening US Cybersecurity: Nuclear as a Response to Cyber Attack

The Congressional hearings and the various memos passed in the wake of the disruption in 2016 presidential elections have risen to the use of the cyber domain by the actors especially states and non-state actors. As put, “the candidates fought not about increasing the number of troops and tanks on the ground, but about how to enhance the country’s cybersecurity” (Wired: 2016). The mounting attacks such as the Equifax attacks related to the insurance record of millions of American citizens in compromised accounts have led to sensitive information breach. Russia alleged role in disrupting the U.S presidential elections via email leaks, misinformation equally, the ISIS cyber capabilities and North Korea nuclear proliferation are additions to the narrative of the politics surrounding cyber.

Current political rhetoric continues with the militarization of cyber domain with the other states and the notable emergence of Artificial intelligence (AI). The search for credible deterrence i.e. the where the cost of inflicting harm is more than rather than the reward (Schilling, 1960), has gained ground which was limited by the issue of the arbitrary threshold. Despite Obama administration use of Offensive as cyberstrategy is continued under the Trump administration with more militarization of the domain. The recent addition of the Pentagon countering cyberattacks with the nuclear is a way front with the recognition of the nonstrategic forces, “global threat conditions have worsened markedly since the 2010 Nuclear Posture Review(NPR). Now there exists an unprecedented range

and mix of threats, including major conventional, chemical, biological, nuclear, space, and cyber threats, and violent non-state actors’.

The nuclear posture 2018 states, “Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities. In addition, it states, “Given the potential of significant non-nuclear strategic attacks, the United States reserves the right to make any adjustment in the assurance that may be warranted by the evolution and proliferation of non-nuclear strategic attack technologies and U.S. capabilities to counter that threat” (Nuclear Posture Review, 2017).

The extension of the nuclear to the non–nuclear strategic attacks includes cyber in form of the credible deterrence will have a significant impact on the very definition of the constitution of cyber-attack as the case was of Estonia cyber attacks in 2007 which led to serious disruption. Academician as Dr. Lisbeth Grounlund at Union of Concerned Scientists said, "President Trump is embarking on a reckless path — one that will reduce US security both now and in the longer term," The administration is blurring the line between nuclear and conventional war-fighting. Reciprocity has emerged as the important component in the U.S administration policy for the cyber-attacks against the U.S.

The major concern driving the security aspects from the view of the leadership is the advantage that the cyberspace has provided to the U.S. As noted, “America's economic prosperity in the 21st century will depend on cybersecurity. And this is also a matter of public safety and national security.” The words evolve from the dangers coming from the domain which cannot be subdued due to the entire reliability. The scenarios presented by the failing of the National grid, terrorist attacks have been resonated. Cyber domain poses a unique challenge where the political narrative reflects the concern for cyber-attacks challenging national security and the privacy, civil rights. These factors are at constant interplay in shaping the narratives on cyberspace and the U.S cybersecurity policy. The advantage provided by the technology to the offensive side of Cyber capabilities of the

U.S is turned against due to the decentralized nature of cyber technology. Actors as a foreign state, non-state actors and individuals are in a challenging position, where the case of the states offending on each other, and non-state actors use cyber to disseminate the harm. Diffusion as in the political narratives has leveraged other actor's especially state capabilities, the relative gains of the U.S.

Cyber as a domain and its open, interoperability across boundaries have brought to the forefront of the advantages forms including the political, economic, social and also the advantage of disruption i.e. offensive. Politics of Cybersecurity has been driven by the security concerns emerging from the developing technology and the political structure in which it is embedded. The dilemma is reflected in the international relations with limited cooperation and development of the offensive. The next chapter analysis the international relations in cyberspace marked with the dilemma of the cooperation and the militarization of the cyberdomain.

Chapter 3

Transnational Cyber Security Threats and the U.S. Response

The Internet is a transnational medium and an increasingly important platform for the delivery of products and services globally. It is regarded as the 'Global Commons' i.e. a common resource which cannot be excluded and is treated as a duty-free zone under WTO agreements. The provision of online news and connections across geographic borders via social networking tools has been described by American leaders, 'as an essential human right. By contrast, the very same free flow has been described by leaders in Russia and China not as a human right but as an "information attack" designed to undermine state stability. As a result, in international exchanges US officials have talked about Cyber-attacks in terms of "assaults on an intrusion of cyber systems and critical infrastructure," while their counterparts, from places like Russia, have discussed them as part of a Western "information war "to undermine regimes "in the name of democratic reform."(Singer et al., 2014).

Cyber espionage networks like GhostNet malware stole political, economic and media information from over 1,200 computers in 103 countries. Ronald Deibert, the Canadian computer security expert, states the limitation of deterrence: "Attacks can be 'crowdsourced' by the nation-state such as the attack on Sony picture sponsored by North Korea or arise from acts of spontaneous participation or both. In such an environment, it complicates the task of assigning accusation to a state and forming an appropriate response. This is potentially destabilizing to the global order." Global structure of the cyberspace has been changing rapidly covering the major part of the world. The chapter examines the international dimensions of cyberspace from the perspectives of security challenges in the form of the militarization of domain with cyber-attacks on the rise, protection of data and intellectual property. Cooperation occurs in the cyberspace in the form of the multistakeholder arrangement such as UN GGE apart from the bilateral agreements between States. The U.S response to the emerging international cybersecurity scenario would be analyzed in form of the security measures and collaboration on cybersecurity measures.

Cyberspace in International Relations

The nature of the cyberspace due to its interconnectedness of the information systems has transcended national boundaries. The harnessing of the internet for the economic benefits and communication have made it vital to global economies. The commercialization of the internet accompanied by the development of the private sector led to the harnessing of the internet for economic gains. Along with gains, the vulnerability was espoused with the increasing number of Cyber-attacks ranging from individual to state-led. Most important characteristics of the Cyber domain are attribution, diffusion, and interconnectedness allowing multiple actors crossing national boundaries. In this perspective, the international relations have developed with hacking initially to contemporary sophisticated Denial of service attacks(DDoS). The offensive advantage over the defensive has developed over years with the development of the separate military Cyber command by the nation-states.

International Cyber Environment

The definition of the meaning of the cybersecurity remains contested at the global level. The United Nations Security Council (the most powerful body on security decisions) failed to mention the cyber aspect of security with none of the Security Council resolutions have so far mentioned the Cyber aspect of security. It had been limited to the use of the internet by terrorist groups through the Working Group on Countering Use of the Internet for Terrorist Purposes (CTITF), (Radu, 2014). The first UNGA resolution was proposed by Russia in 1998 in the field of International security. The U.S proposed and passed a resolution in 2002 at United Nations General Assembly (57/239), “prioritizing cybersecurity planning and management” for the adoption of the cybersecurity leading to the ,culture of the global Cybersecurity. The debate over the information security versus cybersecurity has been profound between the states holding a divergent position on it. Political contestation, a compromise was reached for a wording that is less compelling and reduces the overall effectiveness of the resolution (Radu, 2012). The failure to form the binding resolution on Estonia and Georgia attacks are reminiscent on the part of the International organization functionality.

The International Telecom Union (ITU) resolution 64/211 passed in 2010 explicitly mentions the increasingly transnational nature of cyber threats. Efforts to develop rules of the road for cyberspace focus on the applicability of existing international law, potential gaps, and the development of norms, confidence-building measures, and postulating deterrence posture.

The international relations effects range from the international law, development of norms such as the UN GGE (United Nations Group of Governmental Experts), Budapest Convention on Crime, Bilateral agreement and developing deterrence policies in the wake of the development of the attack capabilities. The broad range of international institutions has developed for the construction of facilitating and promoting responsible behavior in Cyberspace. This organization operates from the global level to the regional level, ensuring standard operations on the internet and ensuring its security.

Figure 3: Organizations Associated with Cyber Security

Asia-Pacific economic cooperation	International Electrotechnical Commission	Meridian
Association of South East Asian Nations (ASEAN)	International Organization for Standardization	North Atlantic Treaty Organization
Council of Europe	International Telecommunication Union (ITU)	Organization of American States
European Union	Internet Corporation for Assigned Names and Numbers (ICANN)	Organization for Economic Cooperation and Development
Forum of Incident Response and Security Teams	Internet Engineering Task Force	United Nations
Group of Eight (G8)	Internet Governance Forum	
Institute of Electrical and Electronic Engineers	Interpol	

Source: Key Entities and Efforts with Significant Influence on International Cyberspace Security and Governance (Source: GAO, 2010)

- The International Telecom Union (ITU): emerged as part of developing the common standards related to the telecommunication
- NATO Cybercommand (CCDCOE) developed in 2007 in response to Estonia attacks. It facilitates the development, the retaliatory capabilities against cyber-attack and information sharing among the partner states for effective cybersecurity.
- Computer Emergency Response Team (CERT's) serves as the first line of defense informing of the computer vulnerability and patches for the malware. US-CERT in the U.S function to measures for the cybersecurity including guidelines and advisory for incoming threats.
- ICANN (Internet Corporation for assigned names and Numbers) distributes the unique IP providing identity to each internet connection.

The international organizations provide a multi-stakeholder platform for the Cybersecurity related issues, ranging on the matters of the consensus on global norms for cyberspace and effective coordination over transnational issues.

Emergence of the U.S Position on International Cooperation in Cyberspace

The first White House directive for the attacks via cyberspace came in the form of the 1984 Presidential directive NSDD-145 (National Policy on Telecommunications and Automated Information Security Systems) which states that, “the technology to exploit the electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation” (White House, 1984). Formation of the Computer Emergency Readiness System (CERT) in 1988 paved the way for emergency measures in collaboration.

The Clinton administration saw the commercialization of the internet and harnessing economic gains from it. Growing network structure and the security aspects led to the foundation of ICANN (Internet Corporation for Assigned Names and Numbers) a private non-profit organization founded in 1998 led to the wider distribution termed as the

‘Internet community. In its proclamation, “Internet is an international network of networks, owned by no single nation, individual or organization” (ICANN, 1998). The distribution of the assigned names and numbers on a universal basis ensured internet as a public good available to all parties despite the size and its power points to the nature of the information system which was decentralized. A large part of the development of the cyberspace was due to the efforts by Clinton administration envisioning in the form of “open and free internet” paving the way for the development of the private sector with the rapid expansion of the economy. The U.S also recognized the internet as a truly global medium to deliver products, services and advocated for the Duty-free zone in the electronic transmissions across the globe.

During the same period, the U.S witnessed a terrorist attack on world trade center in 1994. The vulnerability exposed by the terrorist attack led to the securing of the networked systems. The 1998 *Presidential Directive 63* recognized the urgent need for the protection of the critical infrastructure systems and the need for the international cooperation to help manage this increasingly global problem. 9/11 terrorist attacks represented the way attacks could be directed in an asymmetric manner with the actors having relatively less capacity to inflict huge damage. The *National Strategy to Secure Cyberspace 2003* recognizes that the vast majority of cyber-attacks originates or passes through systems abroad, crosses several borders, and requires international investigative cooperation to be stopped. It outlined working with international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global “culture of security” (White House, 2003). In response, the Collaboration working such as multilateral institutions has been pushed forward APEC, EU, and OAS by designating a committee responsible for the cybersecurity.

U.S response in the international cyber environment has emerged from the multilateral order created by it in the aftermath of World War II, where the market-based economy and interdependence between states formed a major part. Internet, in the same way, has been designated as the open, interoperable medium. However, the cooperation in the international arena is limited by the strategic interest of the allies, partners, and adversary.

The interconnected network provided by the cyberspace provided the opportunity to harness the offensive side to achieve gains, and various actors as terrorist groups, Non-governmental organizations and individuals to propagate influence.

9/11 attacks on the U.S were an important reminder of the emerging capabilities of non-state actors as terrorist groups to inflict severe damage. When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. Former Secretary of Defense Leon Panetta highlighted the threats from cyberdomain, “The greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber-attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation...Cyber Pearl Harbor” (Department of Defense Archives, 2012). U.S Cyber policy has changed with the rapid number of cyberattacks leading to the recognition of the “Cyberwarfare” as the emerging concept in the Information System (National Military strategy, 2006). The cyber policies were revised with the Comprehensive Cyber review of 2008 and 2009. The Military component was developed with the creation of the Cyber command in 2009 at Fort Meade under Strategic Command of NSA.

The International Strategy of the U.S Cyber policy witnessed major Chinese attacks in the form of the commercial espionage with a massive transfer of critical data for commercial and strategic benefits in 2010 with Google attacks. Due to the changes in international cybersecurity environment, the Obama administration released the *International Cyberstrategy in 2011* which changed the U.S outlook to the treatment of a major cyber-attack as an armed attack. Similar to other domains, the U.S could initiate Article 51 of U.N that “the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations.”(UN Charter) The U.S position has been the maintenance of an open, interoperable network in view of the commercial benefits along with the military superiority.

Politics of Cyber-attacks in the Transnational Domain

The action in the cyber domain had been dominated by the use of the political goals. The usage of the political means throughout the period of cold war was marked by hostilities between states leading to espionage by the foreign states. The same trend continues in the cyberdomain with the states and non-states actors using the cyberspace with perceptions of the era of the cold war remains preeminent, now that we are witnessing a trend of the disruption, destroys for the political means. The forms of attack witnessed are two-fold with the online offensive causing the physical damage ranging from the network infrastructure, critical infrastructure, to the mobilization for achieving political ends. On the other end, the physical offense such as the removal of the Bronze Soviet-era statue in Estonia or Iran attacks on the U.S in relation exhibit the use of the cyber domain from the vulnerability perspective As revealed in the attack on Sony pictures, DoD 2015 Cyber strategy put it,

“The North Korean attack on Sony was one of the most destructive cyber-attacks on a U.S. entity to date. The attack further spurred an already ongoing national discussion about the nature of the cyber threat and the need for improved Cybersecurity. The increased use of cyber-attacks as a political instrument reflects a dangerous trend in international relations.”(Department of Defense, 2015)

“Military power and security form a significant role in the relations among states” (Nye, 1998), Cyberspace has provided a new domain where the ability to propagate power for achieving objectives is taking place. Conduct of the various states and Non-state actors in Cyberspace are analyzed below and how U.S Cybersecurity policy in response has taken shape. The source of the threats emanating in the transnational sphere includes both state and non-state actors. States such as China, Russia, North Korea and Iran were specifically identified for Cyberattacks on the U.S. Nature of the attacks vary, from waging information warfare i.e. creating disinformation distorting the truth leading to undermining of the democratic institutions. Other way includes the cyber-attack on the critical infrastructure, federal agencies, and military installations to disrupt the services and cause harm. Cyberespionage had also emerged as an important way to steal intellectual property containing plans of technology development. The non-state actors as

terrorist groups had utilized the internet for secure communication, online radicalization and funding terror operations.

The following sources of threat to U.S cybersecurity have been discussed to understand the source and nature of threats.

Implications of China Cyber Policy

The attacks such as the 2003 incident of Titan Rain involved the series of attack on the unclassified networks of Department of Defense, Department of Energy, Homeland Security computers with attacking the nodes as the email system of Secretary of Defense (CFR, 2005). The growing sophistication has been grown over years with the separate military unit for the Cyber operations PLA unit 61398. “China, meanwhile, views economic competition as a way to achieve peer status with the U.S. and sees cyberspace as an asymmetric instrument which it can successfully use to compete with the United States”. (Brown &Yung, 2017)

The major standoff with the attacks on U.S. MNC as Google and the operation Aurora in retaliation took place in 2010. The US accused China of economic espionage on US firms with the intellectual property rights issues. The commercial espionage of the intellectual property on major U.S forms including Google, Apple has been carried by China. However, the NSA reports revelation by NSA whistleblower Edward Snowden in 2013 was a watershed moment with the classified information leaks, it led China to counterattacks the US government claims with the Global Times proclaiming it removed the ‘sanctimonious mask’.

A recent paper by RAND Corporation titled, “System Confrontation and System Destruction warfare”, highlights the changing nature of warfare as perceived by the PLA (People’s Liberation Army). The Operational system is regarded as the field of ‘Comprehensive dominance’ along with other domains (Engstrom, 2018). Paralyzing the enemies operational System is considered as the important function of the war strategy. This would include:

- The degrading or disrupting the flow of information.
- Degrading or disputing the essential functions including intelligence

- Destroying the vital communication systems of the adversary

The changing notion of warfare as clearly conceived has pushed the Offensive in the cyberdomain with States developing a highly integrated system. China National Cyber strategy released in 2016 placed importance on two key i.e. sovereignty and open market. It outlines that the “Cyberspace sovereignty is an important part of the state sovereignty”, where the state will employ technological, scientific, legal, military and diplomatic tools to deter any efforts to undermine the sovereignty. Second, is the protection of the intellectual property and checking the organizations for unfair competition (Xinhua, 2016).

2015 agreement between U.S and China on the cybersecurity points to the halt of the commercial espionage and trade secret on each other network. However, the declaration was limited to the commercial aspect and intelligence activities as espionage were avoided.

“The United States and China agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors” (Whitehouse, 2015).

The interdependence of two economies (China is the largest trading partner of U.S) have been important and the agreement sort to layout the framework of the U.S engagement in cyberspace ton international platform. The U.S position on the Cyber espionage originating from China has been vocal with indictment case of 2014, where five Chinese military officers were indicted on a charge of hacking. These impacted several US business and commercial entities; Westing House Electric, Solar World, United States Steel Corporation, Allegheny Technologies Inc., Alcoa, Rubber Manufacturing, Energy, Allied Industrial and Workers Union (DOJ, 2014). This is the first instance of the state hacking, “State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country’s flag,” said John Carlin, Assistant Attorney General for National Security.

The recognition of the fact that the states are already waging information war is an important aspect of the understanding of the international Cybersecurity dimension. In this perspective, the National cyber strategy of the States including; China, Russia, Iran and North Korea recognizes the waging of the information warfare. The subsequent national strategy document exerts and legislation has focused on the war in the cyberspace. U.S National Military Operations for Cyberspace Operations in 2006 (now declassified) was the first strategy laying the military component, stating that the National Military strategy for Cyber operations is the comprehensive strategy of the US Armed Forces to maintain the US Military superiority in the cyberspace.

The United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack. Therefore, the Department of Defense (DOD) must be prepared to provide military options to the President and Secretary of Defense (NMS-Co, 2006). In testimony to the subcommittee, “The most advanced and persistent cyber threats to the US today remains nation-states and their proxies, and in particular China and Russia”. The increased threats from Iran and North Korea are also emphasized. The mention of the nation states publicly testifies of the growing threats and this led to cyberthreats finding a critical position in National security challenges in National Strategy document (NSS) 2015.

Information Warfare and Russia Cyber Policy

The espionage activities of the Soviet Union were a major concern during the Reagan administration from the telecommunications field as put in NSSPD -154. Russia position on the Cyber domain emerges from the aspect that it provides a new domain to continue its policies, what is termed as the ‘Hybrid Warfare’. Russia capability in the cyberspace has been well recognized by the US. The four major incidents are related to the Russia capabilities, the first is the Estonia attacks on the Cyber infrastructure and communications in 2007, the second was the Georgia attacks disrupting the Critical infrastructure just before the attacks in 2008, third is the Ukraine attacks in 2014 on the civil infrastructure electric grid and banking. The fourth is the on-going attacks against

the disruption in the Western democracies as evidenced in the U.S and several European state elections.

2010 Military strategy, the intensification of the Information Warfare in the modern conflict and lays the strategy,

“.....to develop forces and resources for information warfare. Also, implement methods for prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force, in the interest of shaping a favorable response from the world community to the utilization of military force.” (The Military Doctrine of Russian Federation, 2010)

Presidential Decree No.646, “Information War is the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force”. (Ministry of Defense, Russia, 2010).

Ronald Deibert, Canadian cyber expert describes it as the ‘Virtual Battle’. Syria led by the Syrian Electronic Army posting in favor of the Pro Assad Regime. From early 2011 for the calls against the regime’s atrocity against the civilian, a united opposition stands in the way. The usage of the social media, especially in the form of the grassroots communication, led to the strong united resistance against the regime. Anti-Assad forces supported by the Western powers and the technological sophistication of the SEA reached from the website defacement to the sophisticated Cyberattacks targeting each other. The case reveals the growing crayon of communication online which has blurred the gap between information and misinformation. This is important in case of war as waged in Syria and targeting the attacks. (Verton, 2013).

Iran Cyber policy and Threat to the U.S

Iran political situation combined with the economic sanction has pushed the action of the proxy interference in the Middle East region. The cyber capabilities are the outcome of the situation emerging. In 2009, the anti-government protest saw the vital usage of the social media and the subsequent crackdown of the government using the method of throttling internet speeds. The Stuxnet attack on the Iran Centrifuge in 2010 was an important movement allegedly by Israel and US development under the operation 'Olympic Games'. The counterattacks followed by the attacks on the Saudi Aramco in 2013, US banking. This is evident in the world of the Iranian leader Ayatollah Khomeini calling for 'Cyber Hezbollah'.

Iran Cyber-attacks on the western countries has grown in sophistication and intensity over the years. The attacks result from the fact of the 40 years discord between U.S and Iran and immediately the 2010 attacks on Iranian Nuclear centrifuge facility at Natanz famously called 'Stuxnet' and the assassination of the Iranian nuclear scientist. Iran offensive capability can ODA The attack on the Saudi Aramco and Qatar RaGaSin 2012 was a major attack leading to the disabling of the 30,000 computers infected with 'Shamoon'virus, (Connell, 2012). Operation Ababil targeted the U.S banking infrastructure, Navy Marines Corps Internet in 2013. Iran nuclear capabilities are not as sophisticated as the Israel, Russia, and China. However, the simple capabilities offered by the Cyber environment have provided impetus to launch credible attacks. State-sponsored attacks by the calls such as the 'Cyber Hezbollah', revolutionary forces are in retaliation to the Western powers led attacks and counter the powerful states.

North Korea Cyber Policy and Threats to the U.S

The activities of North Korea are not limited to the nuclear proliferation; rather the exploitation of the cyber has been a dominant strategy with a role in the ransomware as WannaCry, cybercrime, disruption as in the case of Sony pictures hacks. The attack on Bangladesh Central Bank, South Korean Banking system, financial and strategy security assets are evident of the massive potential for the cyber to play in the transnational field. The recognition of the North Korea as attacker behind the cybercrime did not cross the threshold of risking the national security. Also, the lack of international binding

agreement forbids any actions to be taken against the attacker. The state of international affairs as discussed above makes it a lacuna for the state to act.

Actions were taken by the state led to the security dilemma and the necessary response to it. The major part of which had transformed cybersecurity into the development of offensive. North Korea attacks the U.S was dubbed as the:

“The North Korean government’s cyber-attack on Sony is a serious national security issue. It goes beyond a movie and it demands an appropriate response. We don’t want to see copycat attacks like this in the future.” (Senator Jack Reed (D-RI) of the Senate armed intelligence committee).

Expanding the scope of the National emergency amending 2008, stating that ‘destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014. Constitute a continuing threat to the national security, foreign policy, and economy of the United States.’(White House 2015). Under the executive order 13694 released on April 1, 2015, the Secretary of Treasury was authorized to take necessary actions. Determining the course of the action which states could take in case of Cyber-attacks, the question of the threshold is answered in a limited manner. The relations would be impacted in the same manner which would be accompanied by the punitive actions such as the imposition of the sanctions on the aggressor. The attributions on which the state has been cautious are now becoming visibly audible in the alleged role with the start of the Estonia, Georgia attacks, and now the ‘WannaCry’ ransomware attack. In the Whitehouse briefing on WannaCry malware, “After careful investigation, the United States is publicly attributing the massive WannaCry Cyberattack to North Korea. We do not make this allegation lightly. We do so with evidence, and we do so with partners” (White House: 2017).

A new form of offensive with the private companies which were myriad in the espionage attacks from the foreign states as China reasoned, “Microsoft and Facebook and other major tech companies acted to disable a number of North Korean cyber exploits and disrupt their operations as the North Koreans were still infecting computers across the

globe. They shut down accounts the North Korean regime hackers used to launch attacks and patched systems” (White House, 2017).

Non-State Actors Position in Transnational Cyberattacks

Non-state actors have emerged as an important player in the Cyberdomain and the rapid expansion of technology; availability and low cost have allowed wider participation. Diffusion of technology into hands of deviant individual and groups has provided destructive powers that were once reserved primarily for governments with many experts proclaiming it as the “Privatization of War” (Nye, 2011). The creation of the virtual sanctuaries via chat rooms, blogs using encryption have led to the transcendent of the boundaries with the terrorist outfits such as Al-Qaeda, ISIS easily reaching the target. The recruitment, training is easily done, thus removing the barriers which were constraints before. Terrorist groups as ISIS use messaging apps as Telegram, TOR Browser which uses military grade encryption for messages sent. These are very difficult to decrypt, thus offering a safe passage for communication. Decentralized nature of technology has allowed exploiting which are reserved for security agencies of any state.

Patriot Hackers supported by the States are an important extension of the offensive strategy and regularly involved in destructive cyber-attacks. An example can be drawn of Estonia in 2007 where the Patriot hackers supported by Russian state have involvement in targeting financial and information infrastructure of it causing widespread disruptions. Similarly, the individual’s role has been reassigned with the capacity to play a key role in the cyberspace. Hacktivist groups such as Anonymous, which are politically motivated groups for social change, have released important files related to the national security. During Arab Spring in 2011 group supported anti-government supporters via social media support. Insider’s threat has serious implication on the nation’s security and international security environment. Chelsea Bradley Manning of U.S military leaked the Iraq war document in 2010 lead to the disclosure of several US operatives and the classified files of the U.S military. Edward Snowden NSA leaks in 2013 of classified intelligence material from the Department of Defense depict the human involvement, and the ripples it could have in the domestic and especially international cooperation. China responded strongly to the U.S surveillance over it and led to the Cyber agreement of

2015. There was a strong reaction from allies including Germany, France, and Ukraine over surveillance activities by NSA. It reflects the condition of cybersecurity internationally where trust deficit widens among states with such activities. Most important was the leak of the NSA tools named 'Eternal Blue' which was leaked by the Shadow Brokers group and caused the Denial of Service Attack (DDoS) WannaCry disrupting computers in over 150 countries.

The Dimensions of the U.S cooperation in International Cyber Domain

In the international arena, the control over the information technology and the competing vision of the state forms the major debate. International law is subject to willing and voluntary conduct of the states and any binding resolution requires deep trust among them. Cooperation in the cyberspace reflects this condition and lacks any binding agreement except the Budapest Convention on Cybercrime which is limited to 27 states. Control over ICT v. States.

UNGA (United Nations General Assembly) Res. 66/359 (2011) for the International cybersecurity was forwarded by the states including China, Russia Federation, Tajikistan, and Uzbekistan. 'Responsible State' behavior in the ICT was the major proposition of this resolution. The U.S objected to the clause in the resolution which states:

"To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage" (UN, 2011).

The definition encompasses the authority of State to control the information within its ambit. It would include the counterbalance to the perceived powers that are acquired by the international organization as ITU. The vision of the above states varies significantly from policies promoted by the U.S and its allies. U.S policy has been the open door interpretation where the security of the United States rests on the sustained economic and political expansion abroad (Kiggings, 2012). The open, interoperable internet forms the policy framework for the internet. The international institutions are, therefore, vital for the global expansion of the trade and commerce. The position maintains the vital role of the U.S in protecting the secure lanes of communication open.

Does Diffusion Of Technology Had Led Transnational Agreements Ineffective?

In the evolving Cybersecurity environment, the ability to strike first prevails offering credible defense with relatively lower cost and fulfilling the objectives. Maintenance of the defense structure in the cyber domain is a costly affair especially with the number of Cyberattacks with zero-day exploits¹¹. For an estimate, JP Morgan Chase spent \$250 million on its cybersecurity. The expansion of the technology to the other actors as an individual or terrorist outfits are in easy reach due to the presence of a large number of Dark markets providing sophisticated technology easily, where one even with limited or no technical knowledge can inflict harm.

The case of Iran elections in the wake of the 2009 results made the reformist youth challenged the results, and also demanding the access to social media websites as Twitter, Facebook. In response, the Iranian government launched ‘Green Movement’ leading to the throttling of internet speeds and disabling the protestors from reporting the conditions, only allowing news related to the regime. The U.S did support the social media websites including Twitter, but the action was rendered ineffective due to the state control of the physical electronic infrastructure, in this case, the Iranian government.

The Internet provides an effective medium for the state and non-state actors seeking to attack or exploit the U.S. cyber systems by concealing their identities by basing their efforts attacks from foreign locations and routing the attack to other locations through hacked computers¹². Often the State support or encourages the hackers (in form of Patriot hackers) involved in the transnational attacks from disruption to attacks on adversary state cyber capabilities, fulfilling interest with the advantage of attribution and low risk of retaliation. Cybersecurity assessment report for the Bush administration formed the comprehensive and influential “*Securing Cyberspace for the 44th Presidency*,” based on the findings of the CSIS (Commission on Cybersecurity). It recognized that “Foreign opponents, through a combination of skill, luck, and perseverance, have been able to penetrate poorly protected U.S. computer networks and collect immense quantities of

¹¹ Zero Day Exploits are vulnerabilities that have been first time found and there is no defense against them.

¹² Estonia attack remains wary of the incident in 2007, where the Estonian computers including personal forwarding the Cyberattacks sending large amount of data to servers.

valuable information”. The means for the high-end technology are available to non-state actors and there is an urgent necessity for the formation of a credible deterrence in the form of the offensive capabilities developed by the department of defense (Sofaer et al. 2009). The report recognized the highly volatile nature of the international cyber environment, supported for multilateral engagement, though recognizing it would be limited especially with opponent states.

Speaking for the Senate Resolution, Senator Diane Feinstein of California, “Supporting the Goals and Ideals of National Cybersecurity”¹³, called for international cooperation on regulating Cyberwarfare:

“The Government must consider that effectively Cybersecurity inside the United States will require stronger diplomatic efforts and on an international agreement on what will and will not be tolerated in cyberspace. An international agreement on cyber warfare, much like international conventions on traditional warfare is needed to govern this rapidly growing field.”

UN GGE Governmental experts under the aegis of United Nations first assembled in 2010 for discussion the state construct in cyberspace. The 2012 GGE summit was an important movement where the International law applies to the cyberspace applies which was reiterated in the words of participant states including Russia and China.

The Group of 7 (G7) declaration on “Responsible States Behavior in Cyberspace” recognized on April 11, 2017 recognized “the urgent necessity of increased international cooperation to promote security and stability in cyberspace consisting of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime” and reaffirmed “that the same rights that people have offline must also be protected online. The incoherency in debates emerges from the competing visions of security which are based on the political

¹³ The applicability of the laws of traditional warfare had been forwarded to the Cyberdomain with U.N (52) law considering a cyber-attack equivalent to an armed attack.

structure. Technology has brought new changes but the essential development of the Cyberspace is works within the political lines. Russia, China, Iran have very different sort of idea regarding information, security which was incompetent with the U.S led western allies. Multi-stakeholder agreement with the International Telecom Union, UN GGE have provided the platform for the states and Non-state actors to form the sharing the idea of the cyberspace development and security.

U.S. Administration Response to Cybersecurity: International Cooperation

The emerging cooperation on the Cybersecurity is evolving slowly, with the GGE releasing its second report, International on the cooperation. UN GGE (United Nations group of Governmental experts). The failure of the GGE in 2017 at its fifth session has been documented at the problem of the defining cyberspace and attacks originating from it. Homeland security adviser Thomas P. Bossert remarked, “We will also work with smaller groups of like-minded partners to call out bad behavior and impose costs on our adversaries. We will also pursue bilateral agreements when needed” (Bossert, 2017).

However, the most important stand comes from the bilateral agreements which have taken place over the years. United States EU dialog presents an important component of the cooperation in cyberspace which extends to the NATO cooperation also. Cyber exercised as the Cyber Atlantic and the NATO cyber simulation exercise are a major collaboration between the states over the threats emanating from Cyber domain. The U.S stand on the international cooperation is stated, “International Cyberspace developments are centered on our broader forum and security policy.” That is, the U.S Cyber policy is an extension of the National security policy and an essential means to the fulfillment of the strategic interest vital to it.

The 2010 Lisbon U.S –EU Summit paved the way for transatlantic cooperation, leading to the Transatlantic Cyber exercise in 2011. The situation is limited by the fact that the security dilemma of mistrust. This can be recognized by the fact that has led to a cyber arms race with 30 countries have formed the cyber offensive units and the non-state actors including terrorist outfits as ISIS using the technology for their motives.

The Obama administration led to the effective recognition of the International Cooperation, leading to the release of the International strategy on Cyberspace by Howard Schmidt in 2011. The first document laying out the full approach, the important points were

“When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.” (White House, 2011)

The U.S. stand on the International law has turned to the strong demand for the binding regulations in the Cyber domain. Amid the rising number of attacks a letter from ranking member of House Permanent committee Jim Himes, “Nonproliferation agreements were negotiated to curtail the exponential growth of nuclear weaponry during the second half of the 20th Century. Now is the time for the international community to seriously respond again with a binding set of international rules for Cyberwarfare: an E-Neva Convention” (Bennett, 2015).

Active Information Warfare and State of International Cybersecurity

Active Information warfare has integrated into the Cyberpolicy of various states including Russia, China, and Iran. It is defined as the use of the information and communication technologies to gain a competitive edge over the opponent (IWS, 1995). Debates on the protection of the Information systems and critical infrastructure system have been categorized as waging war. In 2014 at the Wales Summit, after years of debate, NATO finally agreed that a cyber-attack could rise to the level of a military assault and could trigger the Article 5 protection, which allows the alliance to go to the collective defense of another member that has been attacked.

NATO in 2016 included the Cyber to its operational capability in line with other domains; Secretary-General Jens Stoltenberg at the NATO defense, “we have taken a step further and that is to declare that cyber or recognize cyber as an operational domain, so we have air, land, sea and cyber as operational domains inside NATO and that will further strengthen our cyber capabilities and capacities” (NATO, 2016). The decision

came amidst the rising number of Cyberattacks targeting states including Ukraine which witnessed rising tension with Russia, where the sophistication of the attacks due to developed offensive capabilities inflict considerable damage (Baldor, 2016).

Stefan Lofen responding on the role of Russian interference in the Sweden elections, “We should not rule it out and be naïve and think that it does happen in Sweden. That’s why information and Cybersecurity is part of this strategy” (The Local, 2017). German Chancellor Angela Merkel party was targeted and similar strategy was conducted in French elections. The influence in the Europe states demonstrates the changing information war strategy. Cyberdomain is the way to strike influence, disruption with the advantage of anonymity and low possibility of retaliation. We already, even now, have to deal with information out of Russia or with internet attacks that are of Russian origin or with news which shows false information.”(DW, 2016). Similarly, France TV was targeted and posted with the extremist propaganda messages in 2015.

Attribution is difficult in case of the Cyberattacks, the Department of Homeland Security, “The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow-the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.”(DHS, 2017).

Information Protection: Issue of Securing EU-US Data in Transnational Cyber Environment

The data protection is the primary goal for the Cybersecurity. In International space, concern over the sovereignty, territory, international laws are the governing spaces. Increasing offensive cyber-attacks have led to the complex situation of the data sharing with other states. In 2013 Microsoft denied the data stored on Irish server to Federal agencies over a warrant issued. In hearing the case, the Supreme Court decided in favor of the Department of Justice that U.S companies in case of warrant provide the data

requested. Legislatively, Congress passed the *Cloud Act* in 2018, amending the 1986 *Stored Communications Act* updating the law and providing Executive power to enter into an agreement with the foreign government for the data sharing.

The current Stored Communications Act, part of the Electronic Communications Privacy Act, does not explicitly address if the law applies overseas, and Microsoft will argue before the Supreme Court that means it is assumed to apply only within U.S. borders. Government officials from the European Union (EU) and the United States (US) are currently engaged in a heated debate about the privacy of data that crosses national borders. There is hope that this debate can be resolved by something called the Privacy Shield, a new ‘Safe Harbor’ arrangement intended to maintain ‘transatlantic data flows’ by assuring Europeans that their privacy rights will not be negatively impacted if their data is transferred to the US (White paper privacy)

New security measures to protect EU data flows to the US

The question of privacy stated in terms of the fundamental rights has been driving Europe for securing the protection of the data. The strengthening of the privacy data resulted in stricter regulation for the companies on handling the data and setting the conditions under which the data could be used by intelligence agencies. A major debate on the privacy has resulted in Europe passing the “General Data Protection Regulation” (GDPR), considered landmark legislation allowing the citizens “the right to forget”, “the right to erase”. The provision of the legislation provides the highest level of data protection especially concerning the usage by the internet companies and the associated third parties. Based on it, the new “Safe Harbor agreement” provides the secure transfer of data between EU and US and also elaborating the terms under which the data can be transferred and the period for which it can be stored. European privacy groups had strongly advocated for the protection of information and the new agreement faces critique from the groups. (Cobb, 2016)

The revelations of the Edward Snowden played a prominent role in the European stand for privacy concerns in light of the National Security Agency surveillance programs, as a result of which the initial “Safe Harbor Agreement” was enunciated as “invalid” in 2015 (NY Times, 2015). The European Court of Justice (CJEU) ordered in favor of the plaintiff

Max Schrems that, “the NSA’s indiscriminate overseas surveillance interfered with the ‘fundamental rights’ of its citizens” (The Intercept, 2016). Giving up information stored in other countries would make those countries hesitant to trust U.S. data providers if their own privacy laws were not respected, the company has said. That could mean Microsoft loses the business of some foreign customers.

As demonstrated in the Titan Rain attacks, “Corporations often will not disclose cyber penetrations and intellectual property theft because they fear retaliation from the Chinese government, hope for future market access in China, fear the loss of consumer confidence, and fear the loss of stock value” (Testimony on July 9, 2013, Larry Wortzel). Integration of the spying hardware in the routers, phones, computer circuits by China has led to the question of the integrity of communication. The same rhetoric has been iterated by China on the Cisco routers, Microsoft Windows for espionage on the Chinese firms.

Economics of Intellectual Property and Cybersecurity for the U.S

The trade over the internet referred to as the digital economy is at the level of \$23.9 Trillion in 2016 forming 3percent of the Global GDP (IP Commission Report, 2017). Maintenance of the technological superiority is the key to attaining lead in the digital sector. Foreign states as China are involved in the intellectual property theft as a case of Google in 2010. State polices are on securing new technologies to compete with the developed economies. Micius Satellite launched in 2016 by China was the first quantum satellite based on highly advanced technology which nations are still working on. A major reason cited is China’s accumulation of the research reports which was a synthesis in making satellite (IP Commission Report, 2017). The cost of the intellectual property lost from the U.S exceeds \$225 Billion and estimated to as high as \$600 Billion forming 1.25 percent of U.S economy¹⁴, making it a priority area for security.

The policy response of the U.S have strengthened towards the intellectual property rights and the IP commission report released in 2013 made key changes related to the Cyber theft. A major outcome of the report was Section 1637 of the 2015 *National Defense*

¹⁴ Due to several difficulties, estimates are calculated by Intellectual Property Commission in Updated Report in 2017.

Authorization Act (NDAA). The provision of the law made it compulsory for the President to release the report on the Economic espionage activities. Also, it mandates the executive to relevant actions “prohibiting all transactions and property” of the person or entity involved in the Cyber-theft of intellectual property or trade secrets. On the similar line, *Defend Trade Secret Act* of 2016 was passed which established the private rights of action in federal court for the U.S entities. The response in view of the legislation saw the indictment of five Chinese officials of People’s Liberation Army for involvement in Cyberespionage against US companies. Similar, trade sanctions were involved in North Korea following the Sony Pictures Cyber-attack. Impact of the implication is a major challenge in these cases as the international law; jurisdiction and varying strategies of states limit the actions taken. A bilateral agreement with the U.S-China on Intellectual Property in 2015 paves the way forward, but the goals of achieving technological leadership and security scenario constrained the deal.

U.S Legislation on Emerging Cyber Security Environment

Incident’s such as the espionage activities conducted by foreign states has shaped the U.S policy and actions in the international arena. The amendment to the Executive Order 13694 was issued in form of “national emergency” considering a threat to “the national security” seizing the financial assets of the actors linked to the Cyberattack (Department of Treasury, 2015). The interference in the democratic process by the Russian state-supported groups led the actions as information sharing between private companies and government. President Trump reapproved the Executive Order 13964 to authorize sanctions on those who: ‘Tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions’ (White House, 2015). G20 leaders affirmed in their statement that “no country should conduct or support the ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.” (State Archives, 2009-17)

The vision of the states as China calls for ‘New Cyber governance’, the alternative structure is in contrast to the U.S. It states measures for Censorship, freedom of Speech,

espionage laws surrounded around the idea of National security law passed in 2015. The measures were strengthened with the Encryption Law amended in 2017 which was also stated in the International Cyber strategy 2017 released. “China has a structured system for standards-development. The national and industrial standards are developed under careful government supervision. The process is really government-driven and that contrasts with the system we’re familiar with in the United States, where standard-setting is largely industry-driven” (Wennblom, 2017). Though the measures are defended by China citing state control of information is vital to its sovereignty.

With the offensive on the rise and the number of Cyber-attacks, the Security dilemma is important in assessing the actions of the state. U.S international posture has focused on forming of the allies, partners and the arrangement of the bilateral agreements. 2012 House Permanent Select committee on Intelligence recommended telecommunications expert not to do business with Chinese equipment operators with the suspecting of the espionage hardware. The putting of the Back Door is a major Cybersecurity problem with information breach.

U.S policy of an open, interoperable continues to shape the international environment pushing for the economic expansion. Executive Order 13800 passed by the Trump administration designated secretary of state to designate strategic options to deter adversary and International Cooperation. Stating, “the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners” toward maintaining “the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft” (White House, 2017).

The Cybersecurity policy of the administration has been marked with the disinformation campaign by foreign actors as Russia. National Security Strategy 2018 mentions of the “The United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities” (NSS, 2018). The ability to form a credible deterrence is vital and therefore the administration has placed the nuclear option also on the table. In case of the scenarios discussed as the

critical infrastructure, severe physical harm including loss of life would lead to the options.

Maintain and build the allies and the partners capabilities are being initiated as demonstrated in the *Cybersecurity Enhancement Act of 2017*(H.R 1997) states the Department of State to: “providing Ukraine with the necessary support to secure government computer networks from cyber intrusions, particularly networks that defend critical infrastructure. Also, provide support to Ukraine to reduce reliance on Russian information and communications technology.”

U.S Engagement with International Organizations in Cyberspace

The Asia Pacific has emerged as the rapidly growing digital center with expanding technology. U.S investment in the Asia Pacific was expanded with the Rebalance policy towards the Asia Pacific also known as "Pivot". Cyberspace remains central to the U.S interest which includes both the defensive and offensive Cyber policies are promoted, especial in view of rising China. China has invested in the expansion of the ICT in the Asia Pacific countries and development of offensive Cyber capabilities. Regional Organization as with ASEAN, Sponsored and led the first-ever workshop on countering terrorist use of proxy actors in cyberspace in the ASEAN Regional Forum in 2012 (Department of State Strategy, 2016). Integrating cyber policy issues into numerous ongoing political-military, strategic security, and human rights dialogues, include in Presidential-level bilateral discussions with Brazil, India, Japan, and the Republic of Korea.

The International Cooperation in the cyberspace remains contested and limited due to the evolving nature of technology and the diffusion of power providing actors capability to disrupt and destroy. The attacks inflicted such as the Estonia attacks, Saudi Aramco targeted by Iran or the numerous hacking by the groups highlights the role played by the actors including non-state actors. Yet, the highly sophisticated technological precision remains limited to larger states which in recent years have used the offensive cyber weapons. Along with it the control of the information such as the varying definition of the information security or Cybersecurity and the state sovereignty to control are leading debates from international cooperation. The next chapter through the case studies

analyzes the major cyber-attacks and the U.S government response to understanding the position on issues basis.

Chapter 4

U.S Response to Cyber-attacks – Select Case Studies

The ability to maintain open, interoperable internet with economic benefits on hand, and the growing array of security threats on the other hand in cyberspace are shaping the U.S cybersecurity policy. Diffusion of cyber technology has enabled wider participation of actors other than nation-states. Policymaking, law enforcement, and the technical experts differ on the view of Cyber as a domain and its security. The massive data breach of the Office of Personnel Management (OPM) in 2015 resulted in the loss of sensitive data belonging to federal government employees, contractor and their relatives affecting approximate 21.5 million people (OPM, 2015). The case was attributed to China for the data breach and the response of the U.S government was limited to employees being receiving little information about the data breach. The stand of the U.S government differs widely, depending on the nature of threats and its impact on the national security.

The Chapter focuses on the case studies of prominent cyber-attacks on the U.S and its response. Case studies are in thematic order including, economic espionage (trade secret being stolen for the benefit of a foreign government, foreign instrumentality or foreign agent)¹⁵. The second case examines the state attributed attacks focusing on the attack on Sony Pictures attack which was followed by strong reactions from the U.S towards North Korea. Third, includes the growth of ransomware industry for financial gains rendering user system ineffective covering WannaCry and Petya malware attack DDoS (Denial of service attack). Fourth case study covers the insiders' threats to Cybersecurity analyzing the case of NSA files by Edward Snowden. The fifth case examines the Russia sponsored disinformation campaign attacks the creation of information and misinformation shaping the public opinion and the effect on the working of democracy. The testimony of General Keith Alexander states that the cyber-attack has passed the law with more unpredictable actors today (Congressional Hearings, 2016). Several authors point to the question of the 'arbitrary threshold' i.e. the level at which the attack is considered to have reached the level of war. Cyber-attacks had blurred the line between the war and peace with network penetration occurring on daily basis. The case study provides the account of the major cyberattacks on the U.S. analyzing the effects and the response in light of these cyber-attacks.

¹⁵ Defined in Economic Espionage Act of 1996 it includes all kinds of trade secret including financial, technical, and scientific.

Economic Espionage and Cyberthreats

The Economic Espionage is foreign power sponsored intelligence activity at the U.S government, U.S Corporations, establishment to influence economic decisions and unlawfully obtain sensitive financial, trade or propriety information causing significant economic losses. (FBI, Losses due to economic espionage have been growing in number and sophistication. Primarily the attacks are directed towards the private companies for the breach of the Intellectual property and financial assets for commercial benefit. Cyber-attack on Google was a major turning point with the firm openly revealing the cyber-attacks blaming the Chinese government and politicizing of the matter.

Cyber Attack on Google

Highly sophisticated Cyberattack targeted the Google in December 2009. The attack led to the stealing of the intellectual property as the source codes (the base of the software program). Also, the records of the human rights activist of the US, China, and Europe working in China were compromised. Attack was not just limited to Google rather several other major U.S firms in the field of the chemical, mining, construction was targeted. The way it was conducted was a method called ‘phishing attack’ i.e. malware hidden in the attachments or document. It would compromise the system as soon as the link is opened, and created a backdoor for access by the hackers.

Google publicly disclosed in January 2010¹⁶ that its subsidiary in China was targeted with Cyberattacks. Further investigations by Congress and Private sector companies led to the establishment that it more than 30 technology companies mostly located in Silicon Valley, California witnessed series of intrusions. The cyber attackers infected computers with hidden programs allowing unauthorized access to files that may have included the companies’ computer security systems, crucial corporate data, and software source code.

In the case of Google, its employee was under constant surveillance. Many of them joined the social media groups and revealed personal information. The attachment was sent in the form of the email which contained the computer virus. When the attachment

¹⁶ The revelation was done on official Google blog post by Vice President David Drummond titled, “A New Approach to China”.

was opened it led to the malicious malware enter the user system and from there gained access to Google servers located in the U.S. The attack targeted the source code (main program) of the email password management system under which email services of Google runs.

Operation Aurora

Google incident in 2010 was a major incident which changed the threat perception regarding the espionage attacks. Critical infrastructure protection was considered vital to the national security. The attack changed the perception much focused on critical infrastructure to the economic espionage and the protection of intellectual property. The U.S leadership is highly dependent on the intellectual property, “very lifeblood of America’s innovation industry (IP Commission Report, 2013). The threat frame is built around the image that the U.S leadership in the development of intellectual property. The initial threat framing came in the form of the Google public announcement of the attacks. The security firms as the Secure Works recognized the malware written in Chinese characters and discuss on Chinese websites. Similarly, idefense traced the IP address to the single foreign entity supported by China (Report to Congress on U.S-China Economic and Security Review Commission).

Entry into the High Politics

The incidents have strengthened the government response related to the issues related to National security. Comprehensive Policy Review 2009 by the Obama administration was taking place at the time of the Google attacks with the focus on the espionage-related activities also.

Was the action taken by the US government incident specific or it is reflected in other similar Cyber-attacks? As demonstrated in the Titan Rain attacks China over the course of several years, “Corporations often will not disclose cyber penetrations and intellectual property theft because they fear retaliation from the Chinese government, hope for future market access in China, fear the loss of consumer confidence, and fear the loss of stock value”. (Testimony on July 9, 2013, Larry Wortzel)

The Framing of The Threat

The opening window for the Google threat can be found in the ensuing document and the policy decision by the U.S government. The formation of the 1996 Economic Espionage Act by the Congress was a major reform defining policies and practices for dealing with issues of economic espionage. The subsequent legislation focused on the protection of the critical infrastructure, with limited attention to the issue of economic espionage. The 2003 legislation Homeland security “Securing Our Homeland” designated protection for the critical infrastructure. CSIS Commission formed in 2008 made references to the protection of the intellectual property. 2009 Comprehensive Review emphasized the protection of the technology from espionage.

“The Google incident can be considered as the watershed movement where the China threat, Human Rights, and the economic vulnerability were all coupled together. While the economic Cyber espionage threat frame was out there, it lacked a precise prescription and failed to impress key policy actors” (Read, 2014). Google introduced its search engine in 2006 as part of the increased access to the information for the people of China outweighing the condition to censor some results (Drummond, 2010).

Talk of the Internet freedom by Hillary Clinton in 2010 references to China censorship stated of the “information curtain descending across much of the world”¹⁷ Mike Rogers (2011), “Cyberthreats and the ongoing efforts to protect the nation”, House Select Committee on Intelligence highlighted the devastating effects of espionage activities on the U.S economy which is directly related to its national security, stated that:

“Death by thousand Cuts....from Cyberespionage being conducted every day against nearly every sector of the economy. You don’t have to look far these days to find a press report about another firm, like Google, whose networks have been penetrated by Chinese cyber espionage and have lost the valuable corporate intellectual property. The massive campaign being conducted by the Chinese government.” (Congressional Hearings, 2011).

Former President Barack Obama released Joint Strategic Plan on Intellectual property Enforcement, June 2010 states that “We are going to aggressively protect our intellectual

¹⁷ Speech delivered at U.S-China Institute at University of Southern California on Jan 21 , 2010.

property”. Citing the vital importance of the innovation to the U.S economy, 2011 White Paper on Intellectual Property Enforcement legislative Recommends putting more stringent punishment for economic espionage increasing the sentence from the 15 to 20 years which was later legislated in *Economic Espionage Enhancement Act of 2012*.

The attack on Google on other U.S multinational and the related security reflects a dichotomy and highlighted the vulnerability of the large corporations due to the large fixed investments, working in a complex environment, intellectual property, and reputation (Nye, 2010). The Obama administration passed legislation for Cybersecurity, Innovation, and regulation called for the voluntary code of conduct. The private industry sees any form of regulation as a hinder the innovation and the growth of the industry.

2018 National Security Strategy (NSS) considers the “Economic security as the National security”. Importance of the ransomware attacks and the Economic attacks are more vocally pushing demand for Cybersecurity with strong countermeasures. China denied any involvement in the attacks and the put the blame on the U.S for several Cyberattacks on it. The Home Depot retailer witnessed a breach of its payment systems from April to September 2014 including users of both the U.S and Canada. Data breach resulted in the loss of information of “roughly 56 million unique payment cards and 53 million email addresses” (Home Depot, 2014). Attackers used the vendor credentials to login and steal the information from the point of sales terminals resulted in \$19.5 Million as settlement and business loss (Stempel, 2016). The attack on the intellectual property reflects the part of the strategy to gain technological superiority in the Cyber-age.

NSA leaked documents highlighted the surveillance program by U.S government on foreign states and companies where the U.S-China Cyber-agreement was eventually passed in 2015 with the declaration not to conduct economic Cyberespionage against each other. Cost of the cyber espionage attacks had increased. The problem of attribution regarding the attacker is still misleading, leading to the compromise on the action. The U.S has in the case directly alleged China and taken action for the stealing of the trade secrets. Yet, the calculation of the retaliatory measures is difficult and the issue of calculating the estimated advantage in the espionage.

State Attributed Cyber Attack: Case of Sony Pictures

Background

The massive Cyberattacks on the Sony Pictures entertainment was a major breach for the US private companies and the course of the action and responses is vital to understand the US response to Cyberattacks. A series of attacks mounted on Sony Pictures Entertainment (SPE) division of the Sony Corporation on November 24, 2014, led to the breach of the massive amount of data. Computers displayed the neon skeleton with the message that all the internal data have been obtained and shared (USA Today, 2015). The attack took place during the course of the satirical comedy movie “The Interview” portraying the assassination of North Korea leader Kim Jong -Un.

Series of disruption took place on the Sony pictures computers on where a large amount of data was stolen. It includes the information, personal information of the celebrities, and company employees, financial data of the company and the print of unreleased films. In the wake of attacks, 75 percent of the servers were damaged. Guardian of Peace (GOP) was the group that took the responsibility for the attacks. A week later, data which was breached from SPE, some part of it was released by the hackers including the private emails, unreleased films, financial records, film contracts. On December 5, the hackers warned employees of warning of a physical attack, the hackers released a memo. December 8 message contains explicit demanding for not releasing the film. The matter took an unprecedented turn when hackers on 16th December warned of dire consequences, “Soon all the world will see what awful movie Sony Pictures has made. The world will be full of fear. Remember the 11th of September 2011”.source The message made explicit reference to the dire consequence in wake of the scheduled Christmas release of the movie.

Framing of Threat

Two set of issues arises from the attack, the identification of the attacker i.e. the question of attribution and the ability to deter the attack. The attack on Sony Pictures highlighted

the vulnerability of the security systems of the private sector, second the reporting. Despite, the US government warning the system architecture was weak and the attack confirmed it.

The attack on the Sony pictures initially was considered as the corporate nuisance. Disruption was limited with the Hackers posted online the some of the data including the private emails, databases, an episode of unreleased program confirming the data stolen. December 16 was the major turning of the conversion of the private sector company annoyance to a national security threat. Guardians of Peace (GOP) warned that the attack would be conducted in the manner of the 9/11 attacks. Major attacks on the U.S are embedded in the political scene such as the Pearl Harbor which highlights the U.S vulnerability from the threats. Political language constituted reference to the nuclear threat imaginary. The attack on the Sony Pictures was considered as the most devastating attack on the U.S Company. The situation was changed into a global issue with the direct involvement of the U.S government.

The reaction of the U.S government was unfrequented, resulting in the first ever attribution of cyberattacks by the nation-state and the modest retaliatory measures (Haggard; Lindsay, 2015). The response included the involvement of the highest U.S office including the President, Congress, the State Department, Department of Homeland Security, the FBI and CIA. The notion also contained the attack on the freedom of Speech where the controversial movie Interview was deferred for release. FBI press release, North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express them. Such acts of intimidation fall outside the bounds of acceptable state behavior (FBI, 2014).

Public opinion helped shaped the threat perception, where the freedom of speech and expression vital to American values were threatened by North Korea.

North Korea actions constitute the provocations against the U.S and South Korea (ROK). War on a large scale is highly unlikely, likely due to the severe consequences on both sides. Effective deterrence leads to the low risk of conflict escalation but also incentivizes the participation in proxy low-end conflicts. Similar to the Cold war era with the Superpower supporting the proxy war in other nations, North Korea also provokes low-

end conflict and provocations have been the part major policy towards South Korea and the U.S. The Sunshine policy of South Korea under Kim Dae-Jung presidency in 1998 soften the approach of South Korea towards North Korea working for effective cooperation and was effective deterrence leading to Stability. (Min, 2017) As a result, North Korea launched the low-level aggression in wake of the low probability of major conflict. The policy effectively continued till 2008 when the Six-party talks over nuclear issues failed and the same period also witnessed the conflict in the cyberspace by North Korea.

Since 2009, South Korea has been witnessing cyber-attacks from North Korea regularly on military establishment and institutions. (Avery et al., 2017) The conflict in other domains has been associated with the provocation in the cyberspace, where the attribution, low cost of entry has enabled participation of several actors. After the 2011 U.S–South Korea military exercise the South Korean and the American computer systems suffered an attack on media, critical infrastructure, financial services in a series of Denial of service attacks attributed to the North Korean cyber units (Haggard; Lindsay, 2015).

U.S Government Response to Sony Pictures Attack

The turning of matter to the level of the National security issue saw the involvement of the highest U.S leaders, policymakers, and enforcement officials. December 16 warning lead to the announcement by the Sony Pictures of not releasing the film on the eve of Christmas as planned earlier. It provoked strong sentiments with the citing of the Article 1 of the U.S constitution in favor of freedom of Speech. U.S former President Obama citing the pulling of the movie regarded it a mistake, “We cannot have a society in which some dictator someplace can start imposing censorship here in the United States.”(White House, 2014). The sanction was imposed on North Korea on January 2, 2015, which was almost symbolic in nature citing the stringent sanction imposed before. During the same period Chinese military officials were convicted for the series of espionage cyber-attacks on the U.S. State Department stated that it, “Utilized diplomatic channels, in conjunction with technical, law enforcement, and military engagements, when responding to serious cyber threats and incidents, such as the Sony Pictures incident in 2014 and the financial

sector denial-of-service attacks in 2012-2013”. (Department of State International Cyberspace Strategy, 2016). North Korea witnessed the internet service blackout for the period of 24hours, many of the reports pointed to the involvement of the United States in the act.

The Cyberattack on the Sony Pictures saw strong reactions from the U.S government, media and film industry. The major problem is the threshold i.e. the level of attack does not create a major damage. Instead, the provocations lead to disruption and do not affect the critical systems. Provocation on low intensity has been part of the states and non-state actors to involve in conflict with major powers. The cyber-attack was remainder of the hostile cyber capabilities being developed by North Korea and strong resentment against the U.S policy in the Korean peninsula.

Problem of Attribution

North Korea was directly attributed for the Cyberattacks The targeting of the Sony Pictures saw responses from the U.S government with the former U.S president directly stating the role of North Korea, ‘They caused a lot of damage, and we will respond. We will respond proportionally, and we’ll respond in a place and time and manner that we choose.’’(White House, 2014). North Korea was acquitted in a direct state responsible for the Cyber-attacks. North Korea has made attacks on the South Korean bank in 2011 and attack on U.S. Cyber vandalism or act of war. North Korea witnessed a series of disruption including the internet disruption for 10 hours; in addition, the U.S imposed sanctions on North Korea. However, the low-level intensity Cyberattacks is continually waged by North Korea. Cybercrime including Ransomware has targeted systems globally of which WannaCry in 2017 leads to widespread damage.

Privacy, Surveillance and National Security – Case of NSA Leaks

NSA (National Security Agency) leaks forms a significant debate in the issues related to the privacy, surveillance activities, international relations, ethics, and technology. Insider threat forms one of the most eminent dangers as was evidenced in the case of Iraq war cables leaked by Bradley Manning in 2010. Chelsea Manning served as in Army Intelligence Unit during her serving period in Iraq; she downloaded the classified files

from Defense Department servers related to Iraq and Afghanistan war, and Guantanamo Bay prisoner record in form of moral duty “towards her country and a sense of duty to others”. (Peralta, 2014) Later, the revelation was shared with Wikileaks and distributed publicly revealing from the location of the army personnel to the conduct of US defense forces. Many documents revealed the wrongdoings of defense towards in form of war crimes and caused an uproar in the US and abroad. Several insiders threats have revealed over years including the CIA, FBI operatives revealing the classified information. The Internet has made it possible to collect, disseminate the information at an unprecedented scale. Former President Obama highlights the insider threat as a grave danger, “Our nation’s defense depends in part on the fidelity of those entrusted with our nation’s secrets. If any individual who objects to government policy can take it in their own hands to publicly disclose classified information, then we will not be able to keep our people safe or conduct foreign policy” (White House, 2013).

Edward Snowden a former NSA contractor case reveals the risks of maintaining classified systems, national security, and privacy which are linked to each other in the cyberspace. NSA (National Security Agency) was founded in 1952 and its primary function of the data collection, were primarily restricted by the Privacy Act of 1978 which states, “Prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual”¹⁸ and public notice for the group record maintained. 9/11 attacks prompted immediate urgency for the threat and provide extensive power to the agency for the collection of data. Surveillance programmes PRISM were enacted in 2002 for countering the threat of terrorism.

Setting the Precedent

National Security agency witnessed the major beach of the classified documents in 2013 by Edward Snowden, a contractor under Booz Allen Hamilton affiliated to NSA. Snowden earlier worked in CIA, Dell and later hired by National Security Agency as a contractor. Snowden during his part of the work was exposed to the surveillance program by the security agencies. Reportedly, Snowden behavior began to cast suspicion in 2009

¹⁸ Privacy Act of 1978 was reviewed and republished by Department of Justice in 2015. [Accessed Online] Url: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>

while working as CIA operative. 9/11 attacks are a powerful image of the vulnerability of the American security system. In the aftermath of it, several provisions were passed as the Patriot Act 2002. It enabled the surveillance, tapping of the necessary for the security. Various programs as the PRISM, Boundless Informant collected information on the U.S citizens including the foreign government. These programs under the Obama administration hardly changed and it led to Snowden released the classified material. Clandestinely, in 2013 after downloading the classified materials in flash drive, and handed the information to new agencies Guardian and Washington Post. Leaked part revealed the calling details, surveillance of the head of foreign states, foreign embassies, UN, and intelligence agencies. Cyberattack on foreign governments downloading the His work profile allowed him the access to the highest level of the classified information. After collecting data, Snowden went to Hongkong where he exposed the leaks to news agency Guardian and Wikileaks. Later, he sought asylum in Russia which led to the suspected role of the foreign state in undermining U.S National security.

Threat Framework

Edward Snowden formed part of the Whistleblower activist, whose actions were derived from moral and legal actions rather than economic benefits. Leaking of the classified files leads to the revealing of the massive surveillance program on foreign states, US nationals by NSA. Insider's threat forms one of the crucial cybersecurity threat, where the contractors have leaked the sensitive information files. Classified material is directly related to the Nationals security, Mitch McConnell house leader responded, "What's difficult to understand is the motivation of someone who would intentionally seek to warn our nation's enemies of the lawful programs created to protect the American people". Intelligence programs fall within the purview of the state conduct in international relations. Revelations resulted in strong reactions from the privacy advocates, citizens, and the foreign government on part of the U.S surveillance program. Intelligence programs have been under the purview of the Congressional oversight. Other senators also raised the harm leak has done.

U.S Response to the NSA Leaks

The leaks drew a sharp response from the U.S government over the release of the classified information which contained the U.S surveillance programme on U.S citizens and foreign states and classified U.S policy. Senator Dianne Feinstein (D-Calif.) called it as ‘act of treason’, while Senator McCain(R-AZ) stated the memoirs of the 9/11 events and the necessity for the surveillance to stop the threats. The federal appellate court ruled that the NSA has exceeded the powers Congress has authorized. Many libertarians and civil activist groups hailed Snowden as Whistleblower and demanded legal support for him. Major changes were adapted to the legislation including the Patriot Act 2002, Privacy Act 1978 concerning data collection for the U.S citizens.

As part of the security assessment, the NSA was ordered with greater surveillance power by the Court, oversight by the Congress and Presidential approval. Patriot Act which was to be reauthorized before expiry was debated and many Congressmen supported its expiry. They eventually reached consensus and the USA Freedom Act 2015 (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring) law was passed in 2015. It ended the mass bulk collection of the phone records under Section 215 of the Patriot Act allowed for the collection of the bulk data collection both of the phone and the internet data. Section 501 for the prohibition of the bulk collection and specifically specifying the person, entity, phone number, or account for the request”. Section 601 for business under the Patriot Act, Created a panel of the experts of the FISA court for overseeing the activities. However, the counterterrorism measures remain under the act including the foreign intelligence.

Under the section 702 enhanced National security provisions for the Non-U.S persons are enabled. The debate on the privacy and the civil liberties is deemed futile, even after the measures as the Private sector companies have to provide backdoor access to the U.S government for providing information in case of emergency or warrant issued by the court. The vulnerabilities are there in place which has been used by the hackers.

International Response to the NSA Leaked Files

In the International arena, the EU –U.S Trade, Privacy discussion were impacted with the EU members as Estonian President Toomas Hendrik contended for the creation of cloud servers in EU and operating under EU law for the protection of its citizens. NSA Leak shrouded EU-U.S. Trade, Privacy Discussions. The revelations of the Edwards Snowden played a prominent role in the European stand for privacy concerns in light of the National Security Agency surveillance programs, as a result of which the original Safe Harbor Agreement was declared “invalid” in 2015 (NY Times, 2015). The European Court of Justice (CJEU) ordered in favor of the plaintiff Max Schrems that, “the NSA’s indiscriminate overseas surveillance interfered with the ‘fundamental rights’ of its citizens” (The Intercept, 2017). Globally, the leaks drew sharp criticism from the foreign governments. German leader Angela Merkel office demanded a full inquiry into the matter.

Reform of the NSA surveillance reform program passed by Congress over the issue of privacy in the domestic surveillance, Senator Patrick Leahy regard, “the first major overhaul of government surveillance laws in decades” (DW, 2015). China which was accused of the espionage cyberattacks also criticized, “Ironically enough, the bugging undermines the very thing it is supposed to protect - national security. As America pins its security on alliances, the tapping tale would sour its relationship with allies - and thus erode its security bedrock - more than any terrorist would be capable of.”(Xinhua, 2015)

Post Snowden Period

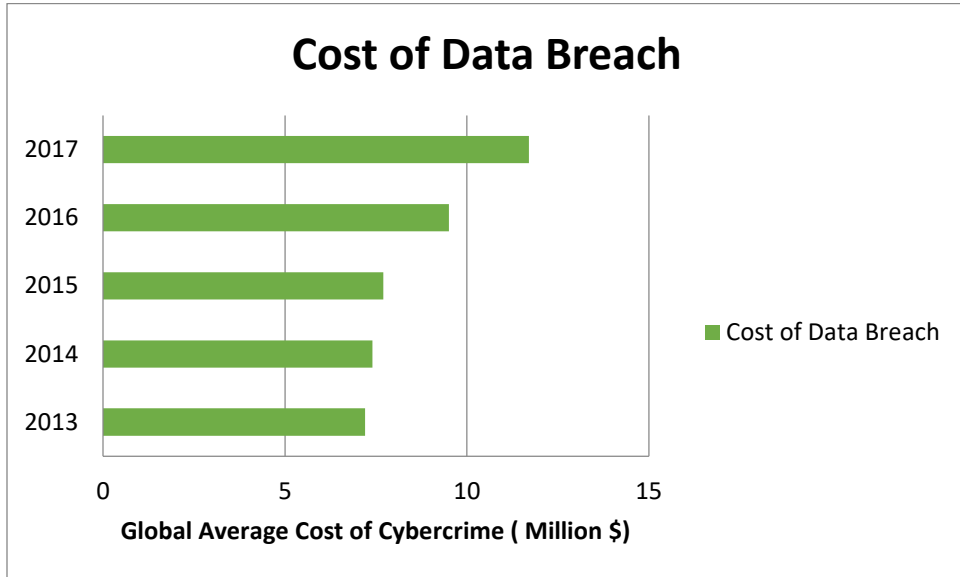
U.S policy changes its policy for the insider’s threat of placing emphasis on “trust but verify”. Actions by the “Decades ago all the bad actors were motivated by greed and money. Now, people are motivated by social issues than by financial issues.”(Christy, J., 2016). Major states including some EU members, Russia, China, Turkey, and Indonesia have pushed for the data localization processing and stored in the country. Efforts to control the information had been pushed by states linking the threat to their own sovereignty.

Distributed Denial of Service Attacks (DDoS) - Case of WannaCry and Petya

In a distributed denial-of-service (DDoS) attack, an attacker may use the hacked computer as an agent to attack another computer. Finding the security vulnerabilities of the agent's computers the hacker can gain access to the system. The hacked system can be used to send huge traffic over the network in form of spam to different email addresses. (US CERT, 2013). The growth of the ransomware industry has resulted in the largest losses, especially in the private sector. Microsoft report (2016) estimated that 71 percent of all business was a victim of Cyberattacks in 2014 leading to financial losses. Equifax Attacks on the similar line led to the massive breach of the consumer data including the Personal data affected the 143 million consumers exposed. An important trend in the ransomware is the scale of these attacks which is global in nature affecting users worldwide.

Dependency on data has led to the high value of it, DDoS attacks target the data asset. WannaCry and Petya were two major ransomware which affects the public utility systems, erased user data and insert malicious content in system networks. Ransomware has transformed into an industry which is being pushed by the easy availability of cyber tools to inflict harm and the decentralization of the financial market structure. Development of the cryptocurrency as Bitcoin works on the peer to peer i.e. direct transfer from the sender to the beneficiary without any central author as bank and regulation authorities. It has led to the mushrooming of various illicit activities as Cybercrime where a transaction can be paid in complete anonymity. Effect of the Cybercrime has devastating effects on the financial, technology growth and maintaining security. Stealing of the trade secrets lead to the loss of jobs and undermine the technological innovation which is vital for the leadership in the internet age.

Figure 4: Cost of Data Breach



Source: The figure represents the Global Average Cost of the Data breaches which exceeds \$11.7 Million (Accenture Report, 2017).¹⁹

For the U.S, the average cost of the Cybercrime was \$21 Million in 2017 which exceeded 22percent the 2016 cost of \$17 Million, ranking highest in the world. Companies in the U.S have regularly faced data breach including major tech firms like Microsoft, Google, Apple, and Yahoo.

Background for Ransomware Attacks

A series of the Cyber-attacks mounted took place affecting over 200,000 computers in 150 countries including Ukraine, U.K, Netherlands and the United States. The attack formed part of the Denial of Service attacks (DDoS) where the computer is held at ransom for \$300 to be paid in Bitcoin. The system is crippled by the malicious content taking over the storage unit of the computer. The National Health Service (NHS) was seriously disrupted leading to the shifting of the emergency patients. It provides an

¹⁹ The figures represent average cost . The U.S government estimates for the Cybercrime including intellectual property loss at \$59 Billion to \$167 Billion in 2016. Figure includes the estimation of jobs lost, insurance payment, data cost, (The cost of the malicious Cyber Activity to the U.S Economy Report , February 2018)

interesting case as the situation directly affects the patients several of them in an emergency. Exploiting the security flaw of the Windows version XP, the malicious software targeted the system Ukraine witnessed the waves of attacks in 2015 on the critical infrastructure leading to the electricity outage. Then, the banking services were disrupted. WannaCry virus continued disrupting the services for 4 days. An anonymous hacking group named Shadow Brokers released the details of the vulnerability in the Microsoft systems where the user can run the program on other Windows machine. The vulnerability was part of the NSA Eternal Blue program and was hacked into the group (Hern, 2017). Hacker group is affiliated to the North Korean state and made its first appearance in 2016. Microsoft's President and chief legal officer describing the attack as a wake-up call for the threats. "An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen." The vulnerabilities were stolen from the NSA (Guardian, 2017).

Opening Window for DDoS attacks

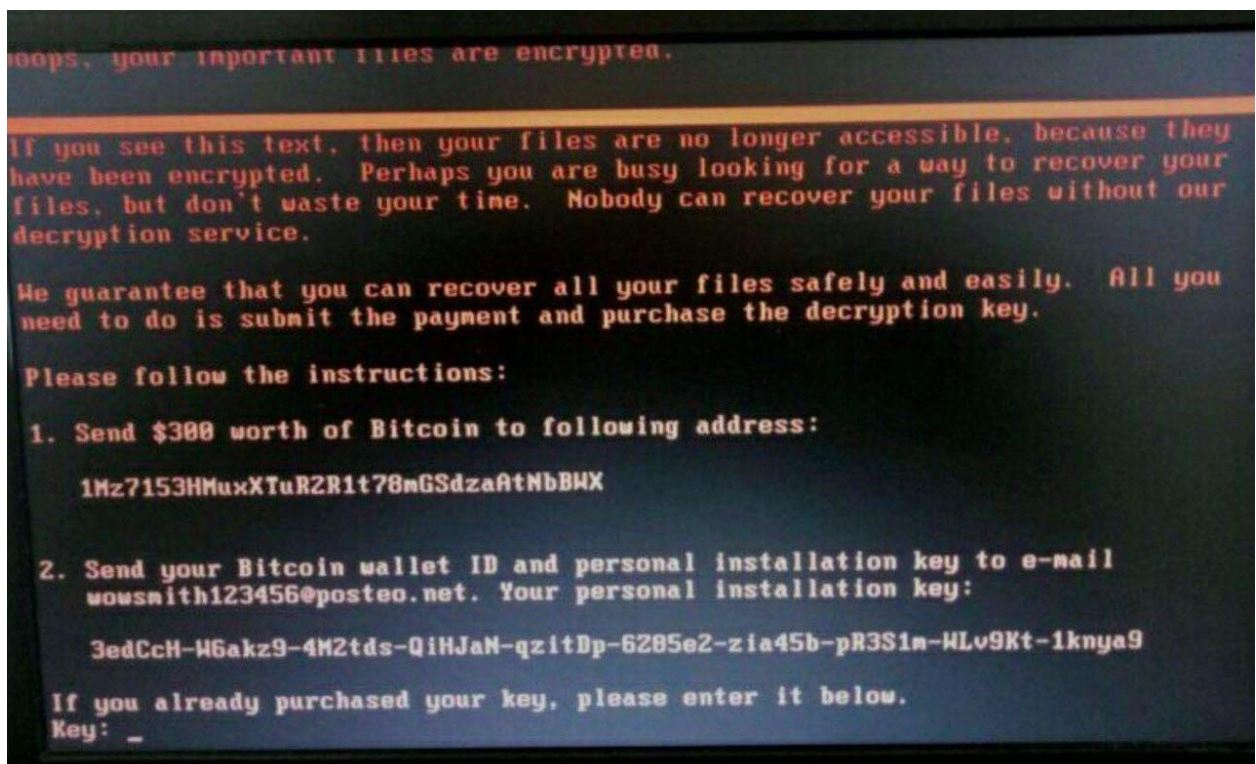
Commercialization of the internet in 90's saw the rapid expansion of the networked connection and the development of the private industry. Home connection reached a level of .and the internet reached 88percent of the population in the U.S²⁰ in 2016. The computer system was attacked for the information in form of the breaches. Titan Rain attacks which originated from China in 2003 led to a series of disruption and information breach from the White House, Department of Defense. At the same time, the digital economy based on the internet reached the level of \$29 Billion. Major works at commercial places as well as at home were digitized and the dependency on it increased over years. Denial of Service attacks was considered in Cybercrime where the breaches were limited to the certain systems. The sophistication of technology has led to the series of attacks which have a huge effect on security, economy, and privacy aspects. WannaCry malware is the sophisticated form of the ransomware developed over the years. It exploited the vulnerabilities in the Microsoft software and rendered the user system ineffective until the ransom is paid. The malware affected 200,000 computers worldwide. Major threat issues come from the fact that the NHS (National Health

²⁰ Figures from Pew Research Center for survey conducted for 17 years from 2000-2016. Available at : Url <http://www.pewinternet.org/fact-sheet/internet-broadband/>

Service) of the United Kingdom suffered the damage and the critical services were delayed from functioning

Petya virus or termed as Not Petya²¹ affected user over 64 countries attributed the attack by the Russian military. The scale of the Petya was limited to the WannaCry; however, the impact was severe. Petya Virus uses the same exploit as the WannaCry of the Eternal Blue which attacks the Windows XP, 7 systems and demanded ransomware of \$300 in Bitcoin.

Figure 5: Petya Virus Screenshot for Ransomware from a User



Source: Twitter

Petya was much more refined than WannaCry and attacked the companies closed networked system wiping their system data entirely. Ukraine was the starting point with the MS accounting software targeted and the virus spread to the other companies system using the same software. Major firms including U.S pharmaceutical firm Merck, FedEx Dutch shipping company Maersk were among companies hit. Ukraine was the most

²¹ To differentiate from the earlier version of the malware which occurred in 2016

affected by the major banks, government services were rendered ineffective. Hospital in Pennsylvania was affected due to the virus for a week and patient's appointment was affected. The financial consequence of the NotPetya virus amounts to \$850 Million in economic cost (Independent, 2017). In the U.S hospital which was not able to process, medical records for over one week. The cost of the attacks cost over \$200 million to Maersk shipment alone when it shipment was delayed.

Threat Framework

The scale of the influence of the computer malware led to the alarm among the U.S. Attributing the attack to North Korea, the malware attack combined with the nuclear proliferation threat by the state. The financial cost of the breach is huge and the data breach in the U.S cost \$7.35 million (IBM Security report, 2017). Private sector companies Microsoft and Facebook responded to the Cyberattacks with the offensive on the hackers attributed to the attacks. The offensive by the private companies is “without any direction by the U.S government”. The loss to the private companies has been huge on the financial scale and the response of the U.S government has been limited. In the case of the WannaCry, the vulnerabilities were due to the Microsoft system operating system. Microsoft president Brad Smith responded strongly against the hoarding of the vulnerabilities by the intelligence agencies. Appealing for the applying the same laws as applied to the weapons in the physical world (Microsoft, 2017). Data breaches are occurring on a large scale resulting from the hacking and the data breach published by an organization like Wikileaks. “Unfortunately through the shadow brokers dims, the average bad guy now has access to exploits, hack tools and information that was open only available to organizations conducting the state-sponsored operation. “The vulnerabilities stored by the intelligence agencies are not being shared by the companies. The case of the WannaCry and Not Petya reveals that the consumer protection becomes riskier in the event of a data breach where chances of vulnerabilities being exposed are possible. A recent report of the Boeing computers being affected by the virus points out that the WannaCry is still active (Forbes, 2018).

U.S Government Response On Not Petya Virus

Public attribution in the case of the Not Petya virus demonstrated the state abilities to detect the Cyberattacks and the international efforts to form a major front to confront the issues. Information sharing between security agencies played an active role leading the White house to attribute the Not Petya virus to Russia. Thomas Bossert chief adviser to President Trump stated that “It was part of the Kremlin’s ongoing effort to destabilize Ukraine”. In response, the U.S issued a sanction against five companies and 19 including for the combined Russian effects in the US election and Not Petya virus. Though the ransomware attack Petya attack the major Russian companies as Rosneft major energy company, Home center one of the Russia loan lender were affected. Statesman words are more driven by the National security concerns and the attribution points to the states from which the gravest concerns are there. NATO organization stated it as the “internationally wrongful act” and the imposition of the article 5 i.e. as an act of war. The attack led to the widespread loss which an only a nation-state can lead.

The gap between the Private sector companies which create, organize, and disseminates large portion of digital data and the government exists. Microsoft President Brad Smith outlined that the data breaches are far more common and the stockpiling of vulnerabilities by NSA have pushed for increasing threat. The gaps in the system should be shared by the vendors. Vulnerabilities stored for the national security has pushed the demand for the global cyber arms race. The ransomware industry continues to thrive as the offensive in the cyberspace yield financial, political benefits with a low probability of retaliation.

Social Media Information Warfare: - Case of Russia Involvement in the U.S Elections

Background

Nation-states have interfered in the elections of foreign states in the past. Use of the cyberspace has added to the new tool deployed by the states to disrupt while maintaining anonymity via crowdsourced groups i.e. people working independently employed for achieving the goal. Efforts by the nation-states to undermine the democratic process

represent the changing tactics to fulfill the state objectives using cyberspace. In the cyberspace creating and distributing, information/misinformation is relatively easy due to the low cost of entry, anonymity and widespread effect. The past cyber-attacks were directed for the purpose of espionage and gathering intelligence or disruption of the interconnected automated systems. A major difference from the past attacks is the objective of the attacker by acquiring data from users, exposing them in public at the time of maximum gain from it. It represents a “very tight connection between cyber warfare and psychological warfare” (Siboni and Siman –Tav: 2016).

The integration of the digital in the political process of U.S remained high, with the start of the 2008 elections campaign where the Barack Obama campaign harnessed the social media. The fact arises from the fact that the Russian involvement dates back to the early years of espionage and is a continued extension. In 2008, Barack Obama and John McCain election campaign were disrupted by the Russian state. Blake Darche, the former NSA analyst, revealed that the hackers supported by the Russian government have been attacking the U.S politicians primarily through the phishing attacks (Chaitin, 2015). U.S presidential election 2016 was reported to have been disrupted using the digital tools. Reports of fake news were reported in large number after the 2016 U.S presidential elections. Investigations suggested the interference of Russia in collusion for the political gains. Attacks in the contemporary time are directed for influence opinions, behavior and the lack of trust in the public and the private institutions. The campaign was part of the disinformation campaign where the use of inaccurate information is spread considerably as opposed to misinformation where the user intent is unintentional in spreading the information (Krag and Asberg, 2017).

The data from the Democratic National Center was penetrated by hackers exposing sensitive data including personal emails of the party leaders including Hillary Clinton.

Later, the information was leaked by Wikileaks revealing the sensitive data related to US political parties and associated organizations. Later, the investigation revealed that the ‘Auto Bots’ i.e. automatic social media accounts of the Facebook, Twitter, Instagram were being used to direct the users to the news, blog. After the promotion of the story by bots, real users commented, retweeted the news to other users. Large web of the

propaganda information was being circulated in the U.S. Facebook and Twitter revealed that 1.7 million U.S accounts at one point of the duration remained in contact with these accounts. The Internet Research Agency “posted thousands of ads that reached millions of people online. The IRA also organized and coordinated political rallies during the run-up to the 2016 election, all while hiding its Russian identity”. (Department of the Treasury, 2017). There were attempts by the Hackers most notably by Guccifer 2.0 for attempting to hack into the elections machine and disrupting the vote counts. These efforts by the hackers supported by the Russian state have resulted in series of investigations and political debate over the democratic elections which form the bedrock of the institutions and the national security.

Threat Framework

The U.S elections of 2016 saw the rapid deployment of the social media in the elections campaign with reliance on content generated online²². Leading to the changing notion of politics where “the conventional rules have changed and digital is king” (Politico, 2016). The vast amount of information generated online is being targeted by the malicious actors. Russia meddling in the western democracies included the U.S and European states have been widely criticized with the inquiry tracing the alleged state role involvement in disruption.

Russia developed the information warfare during the cold war period and restructured in the post-cold war period as part of the psychological warfare accompanied by the attack in other domains. In protest within Russia over blogger Alexei Navalny in 2011, the government used the social media to punish the demonstrators. In 2014, the U.S was planning to sanction Russia in response to the invasion in Ukraine blocking the export of drilling and fracking technologies, which cost over \$82 Trillion in oil reserves. The same period saw the broadcast material containing disinformation being put on social media (Calabresi, 2017). Massive Cyberattacks on Ukraine in 2015 affected the critical infrastructure including electrical grid, banking system which continued for several days. 2016 U.S elections were a continued expansion of the attacks which were waged by the

²² Presidential media coverage spending in 2016 campaign of Trump campaign was \$2.5 billion and Hillary campaign \$1.5 Billion on Online news. Media Quant report cited in The Economist edition, Nov 20th, 2016.Dim

Russian state. Treasury Secretary Steven Mnuchin said, “The Administration is confronting and countering malign Russian cyber activity, including their attempted interference in U.S. elections, destructive cyber-attacks, and intrusions targeting critical infrastructure. These targeted sanctions are a part of a broader effort to address the ongoing nefarious attacks emanating from Russia”(White House, 2017). Several investigation committees were formed to reveal the extent of involvement of Russian in meddling elections. However, attributing the attacks to Russia directly remained a key challenge, as the Cyber domain provides anonymity where the attackers can conceal their identity and route the attack to other destinations.

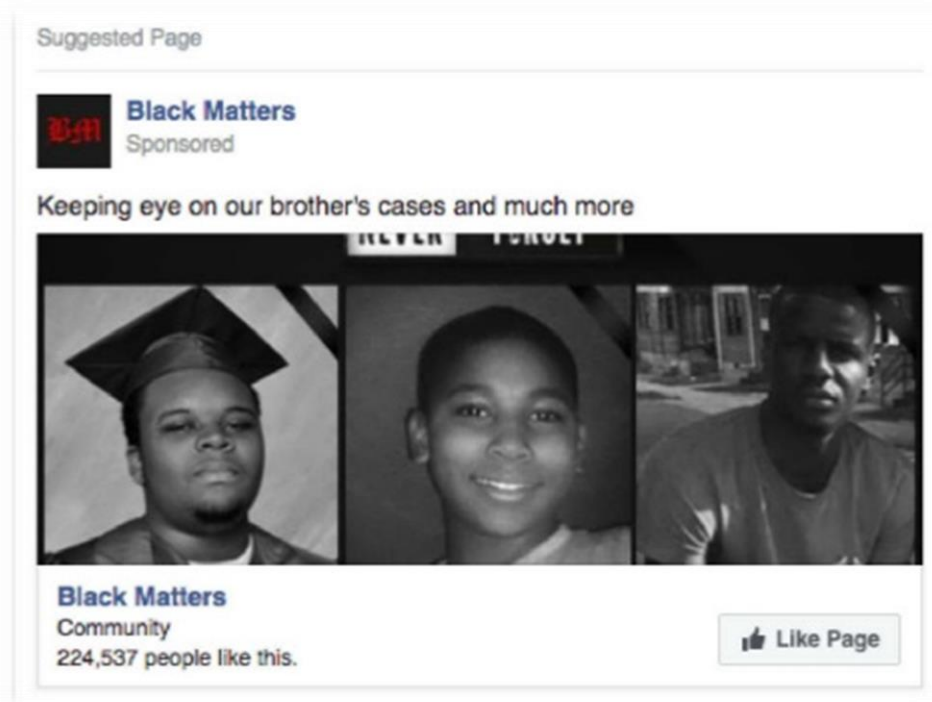
Interference of the foreign states has reached far beyond the espionage and the intelligence activities of the early days. The misinformation campaign launched by Russia affirms the role of the Hybrid Warfare, where the information is a crucial factor for warfare.

Threat Analysis

The involvement of the Russian interference was categorized under the information warfare. In June 2017, Department of Homeland Security (DHS) linked individuals to Russia who infiltrated in the election-related computer system in more than 21 states. Several Russian entities were also found involved in the interference in February 2018. Tactics used by Russia included the overt operations, State-backed media and internet “Troll” supported by the state. Means to undermine the election process involved the usage of the identities of the U.S citizens, leasing the servers and the usage of the virtual users. Under the false accounts, the groups posted on various decisive political and social issues representing the grass root U.S activist. AI (Artificial intelligence) was used for the bots (machine) to post the various issues and make them trending on the social media. Numerous fake advertisement with false identity was posted on the social media; an example is the *#PrayforMizzou* hashtag under the profile name of Jermaine posing as a black man. Post reported of the beating of his brother and coming of KKK to the campus of the University of Missouri. The profile was fake and linked to the Russian Operatives. Similarly, same profile name Jermaine under the username *@FanFan1911* appeared in Germany, it posted anti-Islamic, an anti-immigration post which trended and retweeted

hundreds of times (Jared Prier, 2017). Active information measures have been part of the Russian information warfare strategy and practiced widely during the Soviet era. Disinformation is an important component where the propaganda was spread through the familiar media, and which is now widely being spread through social media.

Figure 6: Example of Russia Disinformation Campaign



Source: Facebook Ad as part of Russia Active Misinformation Campaign (Source : (House Intelligence Committee Report)

Algorithms were employed to segment large population in various group and subgroups based on the political, religious beliefs and likes. The propaganda message was specifically designed for the target group. Moscow developed the sophisticated technology and employing via the social media in various forms. Various investigations were conducted with Mueller leading the Department of Justice (DOJ) criminal inquiry case, House of Representative Intelligence Committee Report and U.S Senate Judiciary Committee on Science and Terrorism. Investigations began on 31st July based on the intelligence report. Emails leaked were circulated in the public domain by Wikileaks and a hacker under alias name 'Guccifer 2.0'. During the course of 2016, Internet Research Agency (IRA) started buying ads from the social media sites. Ads were especially

promoted for specific issues such as immigration, gun rights, civil rights, LGBT rights. Similar, kind of cyber-attacks have been reported in the European states including France, Sweden, Germany, and Ukraine. Ukraine witnessed widespread critical infrastructure attacks which included attacks on electric grid failures in 2015 followed by the disruption of the banking systems. It was a response to the ongoing conflict in Eastern Ukraine supported by the Russian state. German parties database were hacked in part by the same hackers with intention of disrupting the election process and dividing voters over critical issues.

Problem of Attribution

Several investigations by the US Federal agencies by CIA, FBI and Department of Justice pointed to the involvement of Russia in the interference of the 2016 U.S elections. First, the nature of the Cyber domain in the form of concealing identity using hacked systems worldwide. Second, are the sponsored hackers also known as “Patriot Hackers” working under the direction of the foreign states. It has maintained total deniability in case of the interference. The attacks on the U.S systems formed part of the larger strategic environment, where the major conflict was followed by attacks in cyberspace especially the stained environment due to the deployment of NATO troops in East Europe.

Response to the Russian involvement was responded with mild response mostly limiting to the investigation. Obama administration removed 35 Russian diplomats in response to the role of Russia after the release of the investigation report by CIA and FBI in November 2016. Robert Muller Court sentenced 13 Russians in involvement in the interference in U.S elections. U.S Treasury Secretary Steve Mnuchin had put sanctions on Russian as a response to their role in the meddling of elections. The nature of the issue being highly politicalized and the issue of attribution had limited the actions being taken. Homeland Secretary Jeh Johnson outlined the efforts on the need to designate election as the critical infrastructure. In legislation bills such as the *Countering Information Warfare Act of 2016* (Senator Portman Rob-OH) recommend strong measures on foreign intelligence information and center for Information analysis and research for integration of data. Other is the *Honest Ads Act (S.1989)* proposed in Congress for the transparency,

accountability in the advertising in the response to Russia linked organizations buying ads during US presidential elections

Private Sector and the U.S Elections

The vast amounts of user data including sensitive personal information are stored by the social media companies. Most of the social media companies offer the services for free in return for the advertisement. They are customized according to the user preferences, search history, posts resulting in a revenue model for the companies. On data storage of users, Facebook acknowledged that the data of American voters have been targeted during the 2016 campaign, and 3000 ads supported by the Russia based were placed. (House Intelligence Committee, 2018). Effectively, the advertisement major content was related to issues as the immigration, gun rights and instead of candidates. Similarly, Twitter saw the automatic Bots trolling issues using a specific hashtag²³ to circulate the issue. APT 28 (a Russia affiliated group) created the fake accounts and shares the information with Wikileaks. The actions of the social media companies related to the sharing of information have remained confidential until the expose of the leaks. Facebook itself in 2011 ignored the FEC (Federal Election Commission) guidelines for labeling the ads as a political advertisement. The gap between the private industry and government is visible in the Cybersphere where the revenue generation by private industry and security standards by the government is often a mismatch.

The criminal case was prosecuted by the United States Justice Department and sentenced 13 Russian officials involved in the case and the Internet Research Agency. The U.S announces sanctions on Russia for its role in the interference in the elections. Effects on the U.S elections are highly debated; Russian efforts have been continued in the form of the movement as the ‘Black Life Matters’. Russian media agencies as the Sputnik and RT have been actively engaged in the creation of the news, opinions voicing the Russian state views. Widespread misinformation in form of the Fake news erodes trust which forms the bedrock. Propaganda operation has been conducted to manipulate the views

²³ Hastag are part of algorithm which categorized the topic in the order of their popularity referred as ‘Trending topics’.

and perception. Private firms emphasize the innovation and research along with the economic conditions for the growth.

The final report of the House Intelligence Committee concluded that the Russian state was actively involved in the disruption of the 2016 elections using the information warfare method of social media, including the use of sponsored groups and organizations like Internet Research Agency. Russia involvement in the U.S case reflects the development of the psychological warfare where the internet has been used to disrupt the social cohesion and affect the political process on a large scale. Disruptions in the cyberspace are a continued extension of the conflict occurring in other domains. The architecture of the cyberspace provides the adversaries advantage to wage cyber-attack without getting identified and poses challenges for the security agencies to identify the source and the attacker. Also, the limited consensus on cybersecurity measures internationally, almost makes it impossible to punish the perpetrator. The case of Russia disinformation campaign in U.S elections 2016 was a larger part of the active information warfare towards the west. Creating distrust towards democracy and disrupting election infrastructure using information as a weapon, inflicting psychological harm.

Chapter 5
Conclusion

Cyberspace underpins all domains of life; social, economic, and political. Properties of the cyber domain such as interconnectedness, low cost of entry and anonymity have created new opportunities for individuals and non-state actors to a challenging position which were earlier limited to the state. Technological diffusion has reduced the sophistication required for actors to wage cyberattacks and increased the tools available for offensive operations. Internet characterized an open global network that has blurred the distinction between the civilian and military sectors. The impacts of these attacks are severe as the interconnected network allows the spread of malware from system to system.

Development of the internet was under the aegis of the US Department of Defense Agency DARPA for establishing a secure communication. This project was not restricted to the Soviet nuclear threat over the years but internally it facilitated and expanded communication network in the U.S. This feature is embedded in the structure of the internet which was designed for communication rather than security. Harnessing of the internet as the information superhighway by the Clinton Administration also accompanied commercialization of the sector with the rapid growth of internet companies, users, and digital economy. It connected the erstwhile inaccessible markets and created new investment opportunities. The total global trade volume of the digital economy recently crossed \$16.3 trillion. The U.S pioneered the task of expanding the electronic market with emphasis on zero duty over transactions occurring online. These steps were later adapted by WTO and laid the foundation for the digital-based global economy.

The same interconnection also created new threats in the cyberdomain. The number of threats has grown in sophistication and intensity over the years. From the initial attempts of the Morris Worm in 1988 with simple execution to crack passwords, it has resulted in state-led offensive cyber-attacks on of various countries. The involvement of states and non-state actors has led to the militarization of the cyberdomain. The political language regarding the cybersecurity represents the vulnerabilities arising from the technical structure of the cyberspace. Usage of words such as Electronic Cyber Pearl Harbor and cyber Armageddon refers to the deep psychological impact of emerging information

cyberwarfare. Scenarios of the vast devastation have been built surmounting critical infrastructure protection to prevent electric grid failures, nuclear weapons malfunction and many others. These scenarios have shaped the cybersecurity policy of the U.S. though no major attack on the critical infrastructure has yet happened. Policies on the Cyberspace are also driven by the future scenarios due to the fast-evolving nature of technology and increasing number of threats.

Terrorist attacks on the US in September 2001 created the need for the protection of the critical infrastructure. The events showcased emerging new realities of abilities of non-state actors to cause enormous damages. Security of the information in the digital age has greatly transformed with the individuals, non-state actors who are able to exert greater influence. Bush administration's Cyber policy was mainly driven by the fear of terror attacks which led to America's response in the form of strong legislation like Patriot Act and FISMA Act which pushed for extended surveillance measures and policies to strengthen cybersecurity. Cybersecurity remains the top national priority for every U.S government since the Clinton administration. The Cyberattacks in large number are directed at the public systems, private sector entities which are visible and widely propagated in the media and government circles. They represent what is labeled as "Soft underbelly" of the U.S national security and moving of the cybersecurity issues to the national security arena is attributed to such kind of attacks. The case of Sony Pictures demonstrated the capabilities of small nation-states to inflict harm and cause damage. Cyber-attacks on Sony Pictures drew strong reactions from the U.S government connected to the ongoing conflict with North Korea. The politicization of the issue emphasized the assault on the American ideals of freedom of speech and expression.

Cybersecurity policy has been event-driven and the attacks on the nation-state such as Russia in the case of Estonia and Georgia demonstrated the state-sponsored attacks as a reality. Offensive capability development started with the states setting up separate Cyber Military Command. Obama administration in 2009 conducted the Cyber Policy Review for strengthening cybersecurity in wake of increased cyber-attacks targeting both civilian and federal digital systems. This review was transformed into Cybersecurity Act 2009 which contained measures for development of counterstrategy to develop attacks

capabilities in cyberspace leading to the establishment of Cyber Military Command, under the Department of Defense. In the cyber domain, the defense cost is much higher with less reliability on protection, therefore the weapons to attack in cyberspace has been developed for strategic gains. Stuxnet Virus developed jointly by the U.S and Israel targeted the Iranian nuclear site in 2010 and destroyed several nuclear centrifuges. It represents the development of new warfare with low risk of retaliation due to the attribution provided by the cyberspace. Current cyberspace environment without any legal international instrument is defined by the lack of trust among states. Development of the offensive i.e. harming capabilities in cyberspace is expanding. On one hand the U.S led coalition under NATO has developed CCDOE Cyber Command center and on the other hand states like Russia and China have their own dedicated cyber military units.

State-led cyber-attacks reflects the competing vision in international relations that have shaped the cyber domain. Cyberspace is not a technical zone of the network only; it is based on the political structure in which it is embedded. Actions in the cyberspace by the states have been driven by the historical, cultural and economic factors. The cyberspace is viewed differently by states as Russia and China in the form of information control connected to their sovereignty and stability as opposed to the U.S. Maximum numbers of cyber-attacks are transnational in origin, where the actor's motivation varies such as Russia's attempt to undermine the U.S led liberal order disrupting democratic states across Europe and the U.S itself in 2016 Presidential Elections. The U.S faced major criticism globally with revelations of Edward Snowden of NSA classified files disclosing massive surveillance practice and leading to resented international response. It has pushed various States to follow the practice of data localization and more control of the data originating in their country. International cooperation in cyberspace has been hampered by the growth of such events.

The absence of any binding legal treaty on cybersecurity in the international relations has resulted in a situation where the states respond in the way they seem fit. Limited cooperation has emerged in form of the various international organizations working towards defining the cyber domain and the framework of its operation. UNGGE Tallinn Manual based on the voluntary framework is a step ahead in the development of norms in

the cyberspace. Yet, the failure of the Tallinn Manual 2.0 reveals the difficulty in reaching the consensus in cyberspace. The international agreements are rendered ineffective due to the actors varying motives such as cyber espionage for gaining technology. China continued industrial espionage of intellectual property of the U.S for several years to gain the lead in the technological superiority. The growth of the U.S leadership in the cyberspace is directly linked to the research and development in cyberspace and actions of China poses as a threat to U.S leadership in the matter of information technology development. Escalation of the cyber espionage matters has resulted in an increased number of cyber-attacks from both the U.S and China. Data is the “new oil” driving the global economy and the intellectual property debates revealed that protection of data remains vital to the U.S cybersecurity policy.

Cyberspace creation and the internet development have led to the creation and storage of the vast amount of data, a substantial portion of which is available in the public domain. Diffusion of technology has expanded globally in the form of low cost of products, technology innovation, raising awareness of the technical products. The extent to which the population connected using the internet, cellular technologies is staggering. Reliance on data has not been only for connection, but it has also shaped our lifestyle, ideas, and beliefs. Technology interdependence for information has been used by states, non-state actors in the form of the disinformation. Terrorist groups such as ISIS spread the propaganda mission to a greater portion of the world, and are able to recruit by infiltrating the minds of individuals through radicalized content online. Arab spring revolution fuelled by the social media and was also referred by names such as Twitter revolution or Facebook revolution, signifying the role of social media.

Disinformation campaign has emerged as a major way of disrupting and affecting the democracy and the trust in its institutions. Actions by states like Russia are aimed at the information warfare which was demonstrated during the U.S elections of 2016. It was a large part of the active information warfare, where the information is used as a weapon to affect beliefs and change perception. Use of social media to generate content for wedging divide over key issues in the U.S pointed to the larger effort to disrupt the U.S society. As the process is ongoing, the effects of the use of social media in disruption would be

demonstrated in future. The ongoing rift between the U.S and Russia had been witnessed in the case of Ukraine in 2015 which saw widespread cyber-attack that affected the electric grid and banking system. The study highlights that the rivalry in other domains is continued through cyberspace. The widespread cyber threats are continued with the extension of the tension between the U.S and its adversaries.

The increased monitoring by the state which is driven by concern for national security has also raised a question about privacy and surveillance of the citizens. Insider's threat has emerged as a form of the moral vigilantism exposing the sensitive material. The human factor in the cyberspace is crucial for the data protection and classified information can be leaked easily. The Iraq war cable leaks by Bradley Mannings exposed the classified war logs of Afghanistan, Iraq, and Guantanamo Bay prison. The case of the NSA leaks revealed the massive surveillance program by the U.S conducted globally. Classified information leak brought to the question of compromise of national security and the concerns for privacy and surveillance. It brought major changes to the international relations with the states pushing for the control of information and data localization. The NSA file leaks by Edward Snowden in 2013 exposed large-scale surveillance including not only foreign governments but also the US citizens. The U.S politicians, academicians and private industry debated the balance between the national security measures in cyberspace and the concerns for the privacy of the individuals. The social activist groups such as the Electronic Foundation and public opinion has forced the government to bring transparency in surveillance practices. Some measures such as the US Freedom Act in 2015 have strengthened the privacy by curbing bulk collection of phone and internet data. Enactment of the stronger European privacy laws in form of General Data Protection Regulation has also pushed for demand for strong legislation in the U.S over the privacy issues.

Disruption in the cyberspace on a daily basis has narrowed the boundary between the peace and war. Computer systems are penetrated regularly to find the vulnerabilities. The majority of cyber-attacks target the public sector and private sector as they are easily penetrable as compared to military targets. Cybercrime is the commonly inflicted cyber threat, targeting the civilian sector. Two factors promoted it, one the development of the

computer technology with relatively lower cost and other is the financial gains from it. Ransomware attacks have quadrupled in five years. The effect of the ransomware is far beyond the user data being rendered ineffective. The case of WannaCry and Petya malware demonstrated the impact of ransomware beyond financial gains, disrupting the National Health Service of the UK and affecting emergency medical equipment and patient's appointments. Integration of the critical services is based on the networked systems which are monitored on a real-time basis. Denial of Service attacks not only disables computer but the equipment's attached to it, posing a larger threat.

Cyberspace is led by the private sector accounting for the majority of data created, organized and distributed by it. There is a substantial gap between the private sector, government capabilities and objectives. Private industry aims for the economic gains while the government prioritizes the security policies. The case of Microsoft revealed the problem of information sharing where the company denied the information from its server located in Ireland. In case of major attacks, the companies have refrained from reporting the attack due to the reputation and lack of business. Equifax attacks in 2016 were reported after 3 months when the data breach took place. The U.S government has efforts in form of providing incentives through legislation as Information Sharing Act to the private industry has proven to be ineffective. The vulnerabilities stored by the security agencies pose danger for the global cybersecurity. Various hacker groups targeted the critical information and electronic systems of States and major corporations; releasing the exploits from the data breach is easily available in the dark market. The case of Petya virus highlighted the risk of storing the vulnerabilities by intelligence agencies. U.S cybersecurity policy has been shaped by the triad i.e. the maintenance for the open, interoperable internet, concerns for the national security and the protection of data in form of the privacy.

The technological diffusion in the cyber domain has resulted in increased threats to the U.S national security. Increased penetration of technology in the modern has corresponded with an increased use of cyberspace for malign activities by the state and non-state actors. Non-state actors have conducted low-intensity cybercrime including financial fraud, data breach, and website defacement. However, the diffusion in the

cyberspace has not provided an equal platform; rather the state has maintained leverage with the control of physical infrastructure and flow of information. Cyber offensive weapons are complicated, expensive, difficult to construct and deploy; as in highlighted in the case of the Stuxnet virus to destroy Iranian centrifuge. The state is a dominant player that acquires capability especially in transnational affairs and disruptive capacities as seen in the case of U.S, China, Iran, North Korea and Russia. Disinformation campaign attributed to Russia demonstrated the expansion of cyberattack to include psychological harm on a large scale. Exploiting the information from the data breach also required the tool to decipher information, limited to the major states, highlighted in the issue of WannaCry and Petya virus.

In the first chapter of the dissertation, two important assumptions were made, namely;

- The technological diffusion in cyberspace has led to the increased threat for the U.S
- The transnational nature of Cyberspace makes it hard to arrive at international agreements and renders the U.S. response ineffective in the wake of Cyber attacks

Based on the detailed analysis and the accumulated research findings of the dissertation, the above-mentioned assumptions stand validated. Thus, the U.S search for cybersecurity represents the combination of the vulnerabilities from the evolving technology and the political considerations of it. Private control of the large data has brought challenges to the protection of it and enacting measures for strengthening the privacy of citizens. The traditional challenges of the international order are being continued in the cyber domain.

Even though the contours of cybersecurity are constantly constructed and deconstructed on a daily basis, it will take consistent political will, administrative actions, even international cooperation and guidance of the technological community for protecting U.S interests and maintaining global order.

References

(* indicates primary sources)

Abelson, Han and Lawrence, Lessig (1998), “Digital Identity in Cyberspace”, *White Paper for 6.805 for the Law of Cyberspace*, MIT Press, 10 December 1998.

Accenture (2017), “Cost of Cybercrime Study: Insights on the Security Investments that make a difference,” *Accenture Annual Report*, [Online: web] Accessed on 4 May 2017, URL: https://www.accenture.com/t20170926T072837Z__w__us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

*Awareness Month and Raising Awareness and Enhancing the State of Cybersecurity in the United States, September 24, 2009, Senate, S. Res. 285, 111th Cong., 1st sess., *Congressional Record* 155 (September 24, 2009): S 9852-3.

Baldor, L.C. (2016), “Air, land, Sea, Cyber: NATO adds Cyber to operations areas”, Brussels: June 14, 2016, [Online: web] Accessed on 15 April 2017, URL: <https://phys.org/news/2016-06-air-sea-cyber-nato-areas.html>.

Baldwin, D.A. (1997), “The Concept of Security”, *Review of International Studies*, Vol. 23(1):5-26.

Bandreth, R. (2001), “The Cyber debate: Perception and Politics in US Critical Infrastructure Protection”, *Information and Security*, (7): 80-103

Brown and Yung (2017), “Evaluating the U.S –China Cybersecurity agreement”, *The Diplomat*. [Online:web] Accessed 4 March 2017, URL: <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>

Buzan, B. et al. (1998), *Security: A New Framework for Analysis*, Boulder: Lynne Rienner Publications.

Carr, M. (2016), *US Power and the Internet in the International Relations: The Irony of the Information Age*, London: Palgrave Macmillan Publishing.

Chaitin, D. (2017), "Obama's 2008 Campaign was Hacked by Russians", *Washington Examiner*, May 12, 2017. Url:// <https://www.washingtonexaminer.com/obamas-2008-campaign-was-hacked-by-russians-report/article/2622994>

Choucri, N. (2012), *Cyberpolitics in International Relations*, Cambridge: MIT Press.

Chourci, N. et al. (2016), *Institutions for Cybersecurity: International Responses and Data Sharing Initiatives*, Massachusetts Institute of technology: Cambridge.

Cavelty, M. D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge Press: New York.

Clarke R. and Knake, R. (2010), *Cyber War: The Next Threat to the Cyber Security and What to Do about it*, New York: Harper Collins.

Clinton, Hillary, "Cyber Cold war is Just Getting Started", *Guardian News*, October 16, 2017.

*Congressional Hearings, I, (2002), US 107th Congress, Session 1st, Senate, Committee on Commerce, Science, Transportation, Hearings, Cyberterrorism Preparedness Act, January 28, 2002.

*Congressional Hearings, I, (2012), US 102th Congress, Session 2nd, Subcommittee on Oversight, Investigations, and Management of the Committee on Homeland Security, House of Representatives, America is under cyber-attack: why urgent action is needed, April 24, 2012.

*Congressional Hearing (2013), 113th Congress, Senate, Testimony of General Keith Alexander United States Cyber Command, House Committee on Armed Services Intelligence, Emerging Threats and Capabilities Subcommittee, 13 March 2013.

*Congressional Hearings (2013), 113th Congress, Testimony Larry Wortzel (2013), Cyberespionage and the theft of U.S Intelligence Property and Technology: House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, July 9, 2013.

*Congressional Hearings, I, (2015), US 114th Congress, Session 1st, Permanent Select Committee on Intelligence, House of Representatives, Protecting Cyber Networks Act, April 13, 2015 URL:// <https://www.congress.gov/congressional-report/114th-congress/house-report/63/1>

*Congressional Hearings (2016), 115th Congress, Testimony of General Keith Alexander on Digital Act of War: evolving the Cybersecurity Conversation, Subcommittee on Information Technology and National Security, Committee on Oversight and Government Reform, July 13, 2016.

*Department of Defense (1958), Department of Defense Advanced Research Project Agency Directive 5105.5, DARPA Publications, February 7, 1958. URL: http://semanticvoid.com/docs/darpa_directive.pdf

*Defense Advanced Research Agency, *About DARPA*, URL: <https://www.darpa.mil/about-us/about-darpa>

*Department of Defense (2005), “National Military Strategy for Cyberspace Operations (NMS-CO)”, Office of the Chairman of the Joint Chiefs of Staff: Washington D.C., Dec 11, 2006

*Department of Defense Archives (2012), Remarks by Defense Secretary Leon Panetta to the Business Executives for National Security, October 11, 2012. New York.

*Department of Defense (2018), Nuclear Posture Review (NPR), Office of the Secretary of Defense: Washington D.C. URL: <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>

*Department of Justice (2014), “Conspiracy to Commit Computer Fraud and Abuse”, Case No. 14-118, *U.S District Court Western District of Pennsylvania*.

Drummond, D. (2010), “A New Approach to China”, Google Blog, January 12, 2010 [Online: web] URL: <https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>

*European Commission, “Guide to the EU-US Privacy Shield”, European Union Publications Office: Brussels.

*Executive Office of the President of the United States (2010), *2010 Joint Strategic Plan on Intellectual Property Enforcement*, U.S Government Printing Office: Washington D.C. June 2010. URL: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf

Facebook (2018), “Letter to the ranking member Diane Feinstein and Adam Schiff”, Washington D.C.

Forsyth, J. (2013), What Great powers make it: International Order and the logic of Cooperation in Cyberspace, *Strategic Studies Quarterly*, 93-113.

Gellman, B. (2013), “Here’s How The Post covered the ‘grand social experiment’ of the Internet in 1988”, *Washington Post*, November 4, 2013.

*Gore, Al. (1994), ‘Speech Information Superhighways Speech’ delivered on March 21st, 1994, International Telecommunications Union, The White House Archives.

*Government Accountability Office (2010), *United States Faces Challenges in Addressing Global Cybersecurity and Governance*, “Publication No GAO-10-606”. Washington D.C.: U.S Government Printing Office.

*Government Accountability Office (2017), *Cybersecurity: Actions Needed to Strengthen U.S Capabilities*, [Online: web] Accessed on 13th May 2017. URL: <https://www.gao.gov/assets/690/682756.pdf>

*Government of United States (1988), 100th Congress, *Computer Security Act of 1987*, Public Law n. 100-235, United States Government Printing Office URL: <https://www.csp.noaa.gov/policies/csa-1987.htm>

*Government of the United States (2003), *National Strategy to Secure Cyberspace*, The White House, Washington D.C.

*Government of United States (1998), Protecting America's Critical Infrastructure, The White House, Washington D.C.

*Government of United States (1997), Critical Foundations – Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Plan, The White House, Washington D.C.

*Government of United States (2009), Cyber Policy Review, The White House, Washington D.C.

*Government of United States (2011), Department of Defense Strategy for Operating in the Cyberspace, The Department of Defense, Washington DC.

Greenberg, P. (2017), Privacy Legislation related to Internet Service Providers 2017", National Conference of State Legislatures, Washington D.C. Dec 29, 2017. URL: <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx>

Greenwald, G. (2014), No place to Hide: Edward Snowden, the NSA and the U.S Surveillance State, New York: Metropolitan Books.

Haggard, S. and J. Lindsay (2015), "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", East-West Center.

Hare, F. (2010), "The Cyber Threat To National Security: Why can't we agree?" *CCD COE Publications*.

Hellman, G. (2009), "Beliefs as rule of Action: Pragmatism as a Theory of Thought and Action", *International Studies Review*, 11: 638-662.

Hoffman, W. and Levite, A. (2017), *Private Cyber Defense: Can Active Measures help stabilize Cyberspace?*, Washington: Carnegie Endowment for International Peace.

*House Permanent Committee on Intelligence, "Report on Russian Active Measures", House of Representatives, Washington D.C., March 22, 2018 [Declassified] URL: https://intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf

Inkster, N. (2016), "Information Warfare and the U.S Presidential Election", *Global Politics and Strategy*, Routledge Press, 58:5, 23-32.

IP Commission Report (2017), "The Theft of American Intellectual Property: Reassessments of the Challenges and the United States Policy", *The National Bureau of Asian Research*, Washington D.C.

International Telecommunication Union (2008), Cybersecurity Policy, Document no ITU-T X.1205, 04/2008. URL: <https://ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf>

Jensen, E. (2012), "International Law and the Internet: Adapting Legal Frameworks In response to online warfare and revolutions Fueled by Social Media: Cyber Deterrence", *Emory International law review*.

Jervis, R. (1978), "Cooperation under the Security Dilemma", *World Politics*, 30(2):167-214.

Kremer, Jan. and F. Muller (2014), *Cyberspace and International Relations: Theory, Prospects, and Challenges*, New York: Springer Press.

Libicki, M. (2017), "The convergence of Information Warfare", *Strategic Studies Quarterly*, spring 2017: 49-65.

Liebethel K. and Singer P. (2012), "Cyber Security and U.S China Relations", Brookings Report.

Loughary, Kelly (2013), "Averting a 'Cyber Pearl Harbor' 'without sinking corporate America: the ramifications of cyber security regulations on the private sector", *Contract Management*, (53): 34-39.

Lynn, W. (2010), *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs Magazine: October 2010 Issue.

Magnus H. (2011), "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", *Journal of Strategic Security*, 4(2): 1-24.

McLaughlin, J. (2016), “New Safe Harbor Data ‘Deal’ Maybe More Politicking Than Surveillance Reform”, *The Intercept*, [Online: web] Accessed on 21 April 2017, URL: <https://theintercept.com/2016/02/03/new-safe-harbor-data-deal-may-be-more-politicking-than-surveillance-reform/>.

Medvedev, S.A. (2015), Offensive-Defensive Theory analysis of Russian Cyber Capability, National Institution Archive (NPS), March 2015.

Melnitzky, Alexander (2012), “Defending America against Chinese Cyber Espionage Through the use of Active Defenses ‘’. *Cardozo Journal of International & Comparative Law*, 20(2): 537-570.

*Ministry of Defense (Russia), “The Military Doctrine of the Russia Federation”, February 5, 2010. [Online: web] Accessed 21 April 2017, URL: https://carnegieendowment.org/files/2010russia_military_doctrine.pdf

*National Research Council (2002), *Making the Nation Safer; the role of Science and Technology in Countering Terrorism*, The National Academic Press: Washington D.C.

*North Atlantic Treaty Organization (2015), “Press Conference by General Jen Stoltenberg Nato Defense Minister “Projecting Stability”, Brussels, Jun 15, 2015 [Online: web] URL: https://www.nato.int/cps/ua/natohq/opinions_132492.htm?selectedLocale=en

Obama, B. (2012), Taking the Cyberattack Threat Seriously, *Wall Street Journal*, July 19, 2012. [Online: web] Accessed 4 April 2017 URL: <https://www.wsj.com/articles/SB10000872396390444330904577535492693044650>

*Office of the Director of National Intelligence (2017), Background to “Assessing Russian activities and Intentions in recent US elections: “The Analytic Process and Cyber Incident Attribution”, U.S Government Printing Office: Washington D.C.

*Office of the Executive (2016), *Department of state International Cyberspace Policy Strategy*, Public Law 114-113, Department of State, Washington D.C.,

Peralta, E. (2014), “Chelsea Manning Says She Leaked Classified Info Out of Love for Country”, National Public Radio, June 15, 2014, Washington D.C. [Online: web] Accessed on 1 June 2017, URL: <https://www.npr.org/sections/thetwo-way/2014/06/15/322252062/chelsea-manning-says-she-leaked-classified-info-out-love-for-country>

Pew Research Statistics (2017), *Census on Internet Users in the U.S 2001-2017*. URL <http://www.pewinternet.org/fact-sheet/internet-broadband/>

Pomerantsev, P. and M. Weiss (2014), “The menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money”, *Institute of Modern Russia*, New York.

Powner, D.A. (2010), *Cyberspace: United States Faces Challenge in Addressing Global Cybersecurity and Governance*, United States Government Accountability Office: Washington D.C.

*President’s Council on Integrity & Efficiency (2001), *Review of Federal Agencies Implementation of PDD-63*, March 21, 2001. URL: <https://www.hsdl.org/?view&did=437334>

Scott, M. (2015), “Data Transfer Pact between the U.S and Europe is Ruled Invalid,” *The New York Times*, New York, October 6, 2015, [Online: web] Accessed on 22 April 2017, URL:<https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html>

Sanger, D. (2012), “Obama Orders Sped Up Wave of Cyberattacks Against Iran”, *The New York Times*, New York, June 1, 2012. Accessed on 22nd May 2012. URL: <https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-Libya-was-debated-by-us.html>

Schmitt E. and T. Shanker (2011), U.S Debated Cyberwarfare in Attack Plan on Libya, *The New York Times*, New York, Oct. 17, 2011. Accessed on 21st May 2017, URL: <https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html>

*Space Policy Institute (2008), Remarks by Ambassador Donald A. Mahley, “The State of space security”, George Washington University, January 24 , 2008. Department of State Archives

Shmuel, E. et al. (2016), “Structuring Israel’s Cyber Defense”, Institute for National Security Studies, INSS Insight No. 856, [Online: web] Accessed 4 May 2017, URL: <http://www.inss.org.il/publication/structuring-israels-cyber-defense/>

Smith, Brad (2017), “The Need for a Digital Geneva Convention”, *Microsoft Blog* February 14, 2017 [Online: web] Accessed on 2nd June 2018. Url: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>

Smith, C. (2001), “The First World Hacker War”, *The New York Times*, May 13, 2001. URL:<http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html?mcubz=0>

Stannic, Z. (2013), “What is an international Cybersecurity Regime and How we can achieve it?” *Journal of Law and Technology*, 11:(1)

Stephenson, R. (2018), “Consumer need an Internet Bill of Rights”, Open Letter from AT&T Chairman, January 24, 2018. [Online: web] URL: <https://www.attpublicpolicy.com/consumer-broadband/consumers-need-an-internet-bill-of-rights/>

*The White House (1984), *National Policy on Telecommunications and Automated Information Systems Security NSDD- 145*, Government Printing Office: Washington D.C. URL: <https://fas.org/irp/offdocs/nsdd145.htm>

*The White House (1998), “Protecting Cyber Security”, *Clinton White House Archives*, May 22, 1998. URL: <https://clintonwhitehouse5.archives.gov/WH/EOP/NSC/html/nsc-22.html>

*The White House (1998), White Paper on Framework for the Global Electronic Commerce, Clinton White House Archives, July 1, 1997. URL: <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/index.html>

*The White House (1998), *Critical Infrastructure Protection PDD-63*, Clinton Presidential Library archives, URL: <https://clinton.presidentiallibraries.us/items/show/12762>

*The White House (2008), National Security Presidential Directive-54, *Cybersecurity Policy*, U.S Government Printing Office: Washington D.C.

*The White House (2009), President Obama Speech, Remarks by the President on Securing Our Nation's Cyber Infrastructure, May 29, 2009. [Accessed Online] <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>

*The White House (2012), Presidential Policy Directive 20, U.S Cyber Operations Policy, U.S Government Printing Office: Washington D.C.

Thomas, T.L. (2014), National State Cyber Strategies: Examples from China and Russia, Department of Defense Publication [Online: web] Accessed on 1 June 2017, URL: <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-20.pdf>

*U.S-China Economic and Security Review Commission (2010), 111th Congress, 2nd Session, *Report to Congress of U.S –China Economic and Security Review Commission*, November 2010, U.S Government Printing Office: Washington D.C. [Online: web] URL: <http://www.uscc.gov>

*U.S Congress (2011), Recommendation of the House Republican Cybersecurity Task Force, House of Representatives, Accessed on 2 March 2017, URL: https://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf

*US Congress (2013), Foreign and Economic Espionage Penalty Enhancement Act, Public Law 112-269- Jan. 14, 2013, Government Printing Office: Washington D.C

*U.S Congress (2017), S.1989 Honest Ads Act. 115th Congress, House of Senate, Committee of the Judiciary Subcommittee on Crime and Terrorism, October 19th, 2017.

Verton, D. (2003), *Black Ice: The Invisible Threat of Cyber-Terrorism*, New York: Osborne Books.

Waldrop, M. (2015), "DARPA and the Internet Revolution", Defense Advanced Research Projects Agency Publication, URL: [https://www.darpa.mil/attachments/\(2015\)%20Global%20Nav%20%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20\(Approved\).pdf](https://www.darpa.mil/attachments/(2015)%20Global%20Nav%20%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf)

Warner, M. (2012), Cybersecurity: A Pre-History, *Journal of Intelligence and National Security*, Taylor & Francis, 27: 781-799.

Washington Post (2013), "Here's How The Post covered the 'grand social experiment' of the Internet in 1988", Washington D.C. November 4, 2013. URL: https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/heres-how-the-post-covered-the-grand-social-experiment-of-the-internet-in-1988/?noredirect=on&utm_term=.2f4b750f1e98

Winterfield, S. (2013), *The Basics of Cyber Warfare: Understanding the fundamentals of Cyber Warfare in theory and Practice*, Boston: Syngress Publisher.