BREAKING THE CYBERSECURITY DILEMMA: BALANCING NATIONAL SECURITY AND HUMAN SECURITY IN CYBERSPACE

BY

CHARLES KOBINA OTOO

(10242186)

THIS THESIS/DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MA INTERNATIONAL AFFAIRS DEGREE

LEGON **JULY 2016**

DECLARATION

I hereby declare that this dissertation is the result of an original research conducted by me under the supervision of Dr. Amanda Coffie, and that no part of it has been submitted elsewhere for any other purposes. References to other works have been duly acknowledged.

……	……
CHARLES KOBINA OTOO	**DR AMANDA COFFIE**
(STUDENT)	**(SUPERVISOR)**
Date: ……	**Date: ……**

DEDICATION

This thesis is dedicated to the memory of my grandfather, who taught me that the art of Kung Fu is achieving great skill through practice, to my mother for her words of encouragement, and to my father for giving me everything.

To the cyber warriors of this age and those to come, let us create a brave new world.

ACKNOWLEDGEMENT

I, first of all, wish to thank the Legon Centre for International Affairs and Diplomacy for the opportunity to carry out this study. I also wish to thank my supervisor, for guiding me through the first drafts that formed the basis of this research. Finally, I wish to thank Miss Nutakor for understanding the sacrifices and tolerating so much, and my friends and family for all their support.

LIST OF ABBREVIATIONS

ARPANET – Advanced Research Project Agency Network

AU – African Union

CDI – Critical Digital Infrastructure

CIA – Central Intelligence Agency

CII – Critical Information Infrastructure

CIIP – Critical Information Infrastructure Protection

CNI – Critical National Infrastructure

CSERT – Cyber Security Emergency Response Team

CSS – Cyber Security Strategy

DARPA – Department of Advanced Research Project Agency

EU – European Union

ISIS – Islamic State In Syria

ITU – International Telecommunications Union

LAN – Local Area Network

NCSS – National Cyber Security Strategy

NPSI – National Plan for Information Security Infrastructure

NSA – National Security Agency

RMA – Revolution in Military Affairs

USCYBERCOMM – United States Cyber Command

TABLE OF CONTENTS

ABSTRACT

In today's world, cyberspace and cyberpower have become crucial elements of international security. This brings cyber-threats and the measures to counter them to the apex of the modern security dialogue. In the post-Snowden era, national approaches to cybersecurity seem to be sparking a 'digital arms race' rather than fostering more security. Hence, cyberspace presents a dilemma of epic proportions, which challenges the traditional notions of state-centric security within the arena of international relations. The reason for this is the supranational architecture of cyberspace, which makes it difficult for states to unilaterally securitize existing and emergent cyber-threats. This study interrogates the cybersecurity dilemma and explores the utility of the application of the human security concept to cyberspace. The research shows that current national security approaches to the cybersecurity dilemma are inadequate in addressing the technical, political and social challenges predominant in cyberspace. The study concludes that a balance of the national security and human security approaches may provide states with a strong framework for addressing 21st century cyber challenges.

1.0 RESEARCH DESIGN

1.1 Background

The increase in interconnectivity among governments and non-governmental entities, groups and individuals across the globe has correspondingly given rise to intensified trade, rapidly evolving technology and an increase in mobility and communication. These significant developments have been made possible by the increasing presence and dependence on Cyberspace by state and non-state actors.

Barring the social, economic and political advantages that this digital community provides to actors such as states, private organizations and individuals, it has also connected criminals to the vulnerable. Cyberspace is thus akin to the image of the 'Wild West', and within the dark net[1] knowledge is power. The dark net, also called the dark web or deep web, is a term used to refer to the parts of the internet that are hidden and difficult to access. It hosts dark sites used for unauthorized mass surveillance, the internet's secret black market (Silk Road) used for trading de-classified information, and dark sites used by pedophiles to engage in child pornography. Clearly, this land of binary code, botnets and malware must be governed. However, the supranational architecture of cyberspace makes it difficult for states to unilaterally securitize emergent cyber-threats. Moreover, most of the global digital infrastructure is privately owned, therefore it makes it almost impossible for states to maintain and control the cyber world. Nazli surmises that the ubiquity, fluidity and anonymity of cyberspace has already challenged traditional notions of state-centric security in the arena of international relations[2].

According to Cavelty, this anarchy presents states with an almost intractable quandary termed the 'cybersecurity dilemma'. This is a modern variant of the security dilemma, where the actions of states in attempts to enhance their cybersecurity, regardless of their intention, creates a perception of vulnerability among other actors. They, in turn, prop their cyber capabilities in an attempt to level the playing field or best their perceived aggressors. These perceived threats over the years have played out in several cyber-attacks on governments and private organizations, and in some cases individuals. According to Hackmageddon[3], most cyber-attacks in May 2016 was to commit some form of cybercrime as indicated in Figure 1 below. However, most of the targets of these criminals are directed towards industries.

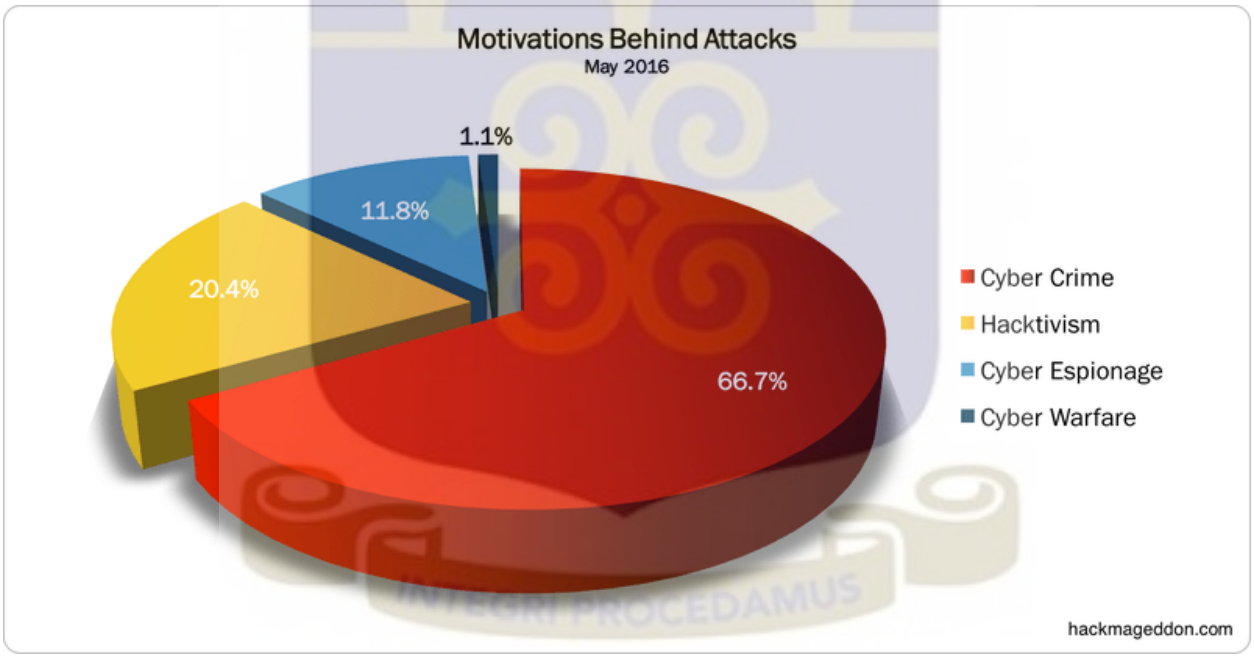

Figure 1

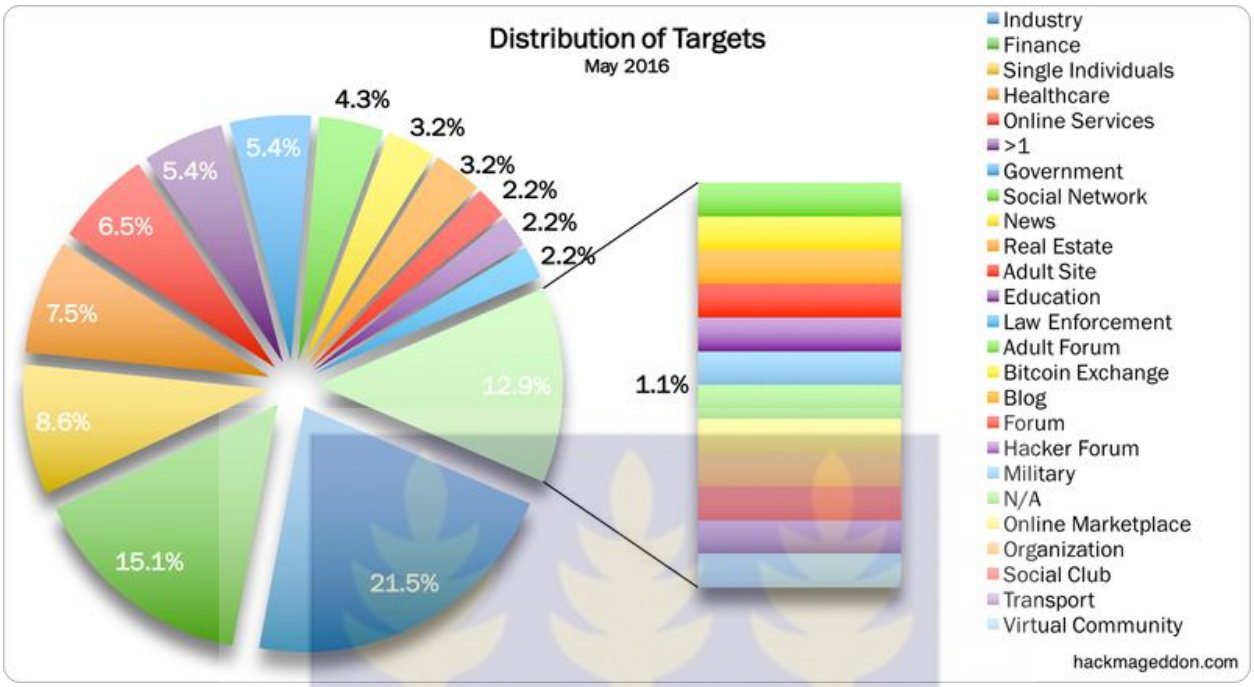

Figure 2

1.2 Problem Statement

The relationship between cyberspace and international security has been established by several scholars in international relations. Within this research area, the authors discuss a wide variety of phenomena – and use terms such as "cyber power," cyber conflict," or "cyber defense." The issues discussed in these articles include espionage, cyber terrorism, cyber military operations and cyber-attacks on critical infrastructure. Most of these articles often represent cybersecurity as an issue within the military domain.

The discussions in literature also takes place on two different levels. On one level, there is a discussion about the nature of the cyber threat and potential means to counter it. On another, there is a discussion about cyber power as a means bolstering national security by scholars such as Franklin Kramer, as against human security in cyberspace by others such as Derek Reveron, Kathleen Mahoney-Norris and Magdalena Defort.[4]

This study seeks to explore a new framework which balances national and human security needs in addressing the cybersecurity dilemma, as much has not been done in this regard.

The reconceptualization of cyberspace as a domain like air, land, and sea has influenced the relations between states within cyberspace. This designation of cyberspace as an operational environment is clearly seen in the United States Air Forces' Mission Statement[5] – "…to fly, fight and win in air, space and cyberspace[6] ..., and many others like it from states within the comity of nations.

As a global domain, attempts to securitize threats by state actors have failed because of the supranational architecture of cyberspace. While the global infrastructure of the internet has facilitated the connectivity of computer and telecommunications networks in an unprecedented way, it offers little of security of critical infrastructures in cyberspace.

This is where states have been concerned, and the belief that an increase in cyber capabilities is critical to national security has thrived. Cyberspace is comprised of both non-malevolent and malevolent actors. As the scale of attacks by the latter have increased, states have had no option than to formulate strategies to mitigate the threats they face in cyberspace.

The challenge is that the cybersecurity strategies setting the course for national efforts to strengthen security in cyberspace tend to be state-centric, with a focus on protecting digital borders in the form of critical national infrastructure. Thus, the state-centric (national security) approach to cybersecurity seems to ignore the security of individuals. Rather than producing more security, they seem to be having the opposite effect. Consequently, the use of cyberspace as a national security strategy, both in the dimensions of warfare and mass surveillance in the Post-Snowden era[7] has detrimental effects on the populace – who should be protected by the state as

dictated by the social contract. For instance, the Chinese government's monitoring of China's cyberspace, the United Kingdom's plan of tracking email, cellular and web activity, and the United States' programme named 'Perfect Citizen' whose mandate is to detect cybercriminals and terrorists, are seen by some academics as an infringement on the civil liberties of the very citizens these states have sworn to protect.[8]

Another challenge is that the actions of some states add an additional layer of 'cyber-insecurity' and are seen as a threat to the 'cyber-sovereignty' of other states.[9] Several states are now moving quickly to put in place Cyber Command Centres, usually under the military. As a result, an increasing number of governments have gone public with their plans of militarizing and balkanizing cyberspace through the use of cyber commands.[10] This trend is manifested in the United States Cyber Command (USCYBERCOM) and China's Cyber Blue Team[11] – a maneuver which has sparked a 'digital arms race'.

This represents a strategic shift from addressing the cybersecurity situation in the civilian domain to the military domain. Although a state's intent of securing cyberspace may be justified, the unintended effect is an increase in tensions within the comity of nations. The result is the growing threat of the cybersecurity dilemma to international security on the one hand, and the imminent threat of a 'digital arms race'.[12]

This study thus focuses on the peculiar problems that arise from some selected states' cybersecurity policy approach and actions, and how they affect the security of citizens within these jurisdictions and the international system.

1.3 Research questions

1. What is (are) the current state approaches to addressing the cybersecurity dilemma?
2. How do national security policies impact human security in cyberspace?
3. Does the current cybersecurity model adopted by states provide an adequate framework to guarantee both national and human security in cyberspace?
4. In what ways can a balance between the national security and the human security approaches to cybersecurity be achieved?

1.4 Research objectives

The main objective of this study is to explore the linkages between national security and human security in cyberspace. Specifically, the study will seek to:

1. Examine the current state approaches to addressing the cybersecurity dilemma.
2. Understand the phenomenon of the cybersecurity dilemma, and its implications for national security.
3. Evaluate the impact of national security policies on human security in cyberspace.
4. Determine if a balance between national security and human security approaches can provide the best framework for states to address national issues in cyberspace.

1.5 Scope of the study

This study fundamentally focuses on the cyberspace-security nexus. The national cybersecurity strategy documents of Canada and the United States within the temporal period of the Post-Snowden era would be used. According to Atanassova, the most active advocates of the Human Security concept are Japan, Canada and Norway.[13] Although Japan and Canada have turned their human security perspectives into concrete actions, they promote different approaches to the

concept. Thus the decision to use the Canadian and United States cybersecurity policies are based on the following considerations:

1. The choice of the United States and Canada would highlight the unique differences in the cyber strategies of a superpower and a middle power.
2. Moreover, the choice of United States and Canada would reveal the differences in the application of the concepts of national security and human security, and if the balance being proposed can or has been achieved.

1.6 Rationale of the study

The question of national security in the cyber domain presents the international community with new challenges, given the extent to which cyberspace has penetrated all spheres of life. While the information revolution has driven the discourse on cyber issues from a matter of low politics to high politics, there is still a knowledge gap in scholarly literature on how states can conduct their relations within the cyber realm.

This study will guide both state and non-state actors to adopt cybersecurity policies that balance the security needs of individuals and the state while removing vulnerabilities. It is also intended to provide additional insight into the cybersecurity dilemma and the linkages between national security and human security in cyberspace.

1.7 Research Hypothesis

The study is based on the following hypothesis:

Balancing national security and human security needs in cyberspace would markedly improve cybersecurity.

1.8 Conceptual Framework

This study explores the concept of human security as interpreted from the social constructivist perspective. Constructivism is an approach to international relations that highlights the social interaction of agents or actors in international politics.[14]

The coinage of the term 'constructivism' has been attributed to Nicholas Onuf. His argument that 'anarchy' as a concept used in international relations is socially constructed is shared by contemporary constructivists such as Richard Ashley, John Ruggie and Alexander Wendt.[15]

Wendt is the best-known advocate of social constructivism in the field of international relations. Wendt's 1992 article "Anarchy is What States Make of It: the Social Construction of Power Politics" laid the theoretical groundwork for challenging what he considered to be a flaws in the neorealist and neoliberal institutionalist approach to international politics.[16] Wendt posits that, the focus on interests rather than identities by mainstream international relations theories does not offer an adequate explanatory account of international relations. States have identities from which they derive fundamental goals such as physical security and recognition within the international system. However, how states fulfill their goals depends on their social identities – how states see themselves in relation to others within the comity of nations. On the basis of these identities, states construct their national interests.

According to Tannenwald the primary focus of constructivism is studying the construction of social reality by norms and the normative implications of such constructions.[17] In contrast to the aforementioned theoretical approaches, social constructivists explore the construction and influence of international norms. In other words, institutions are created and are constantly

changed by the activities of state and non-state actors. Institutions and actors are thus mutually conditioning entities.

Social constructivism is about human consciousness and its role in international life, and is based on the following key assumptions[18]. Social constructivists believe that reality is constructed through human activity. Members of a society together invent the properties of the world.[19] Thus, social facts are human creations, and that ideas are not only the building blocks of the material world, but can also change behavior in the international community. Constructivism believes that norms, customs, culture and learning can influence the behavior of state and non-state actors, and international system is characterized by the rule of norms. Constructivism asserts that the process of international politics influences shared interests and identity in the international system. It further posits that the actors in the international community and the structure of the international system exist in an interactive relationship of interdependence. Finally, constructivism emphasizes the role of ideas, norms, identity and culture in shaping individual and national behavior.

The concept of security is not static within the theory and practice of international relations. McDonald identifies from a constructivist perspective the implications of promoting the norm of human security at the international level.[20]

The constructivist interpretation of the human security norm is premised on the idea that all human lives are of equal value because we all belong to the human family.[21] Hence we share a collective identity namely humanity. In contrast to the paradigm of national security which places the security of the state above the individual, the human security paradigm as interpreted by constructivists suggests that human insecurity is linked to the construction of identity. In

consequence, the presentation of national identity over human identity in the political organization of the world represents a constitutive cause of human insecurity.

According to Schnurr and Larry[22], "Human security seeks to place the individual – or people collectively as the referent of security, rather than, although not necessarily in opposition to, institutions such as territory and state sovereignty."[23] Newman explores the concept of human security against the background of transnational norms. He argues that the emergence of the human security norm, as an expanded, inclusive, and evolving conception of security reflects the impact of norms and values in international relations. Thus, the paradigm shifts from state-centric to human security is best explained with reference to social constructivism rather than realism.

Realist, however, highlight the difficulty in studying norms. The norm of human security has been criticized by scholars such as Chandler as an ambiguous concept lacking a clear definition.[24] At present no general consensus has been reached on how the concept of human security should be understood, defined or operationalized. It is not a coherent school of thought or theory of international relations. There are different conceptions of human security that reflect different sociocultural and geostrategic orientations. Similarly, Martin and Owen (2010) posit that defining human security broadly creates a practical dilemma for policy-makers amidst competing policy needs and scarce resources.[25]

Although conceptual ambiguity is a key point of academic debate in the human security field, the constructivist interpretation of the human security norm is justified in that its inclusive, broad, and holistic nature represent its greatest strengths. Through the development of the interconnected principle of 'the responsibility to protect', the concept of human security not only emphasizes the individual as the referent of both national and international security.[26] According

to MacFarlane and Khong, it makes the security of "those over there" an international matter and inextricably linked to "us over here". "The link between human insecurity and international insecurity has been invigorated".[27]

In the context of cybersecurity, realist theories are mostly employed to explain how states use cyber capabilities advance their interests in security, and how they may respond to other states' cyber capabilities. According to Daniel Ventre, the usual approach to analyze cybersecurity is based on realist theories of international relations. For realism the international system is a given, is defined by anarchy, and state survival is imperative. The analysis is focused on the role of states and anarchy in the international system. The main ideas of such an approach are that states may acquire control of their national infrastructures, content and users of cyberspace, and the main struggles of cyberspaces are those between states. Consequently, several states have set up cyber commands. Cyber armies, cyber militias and cyber-defense agencies. This anarchy is based on the power of anonymity cyberspace provides, which makes the attribution of attacks very difficult.

In response to this assertion, Wendt posits that 'anarchy is what states make of it'; it is socially constructed and can be influenced by norms. Constructivists argue that many of the structures and practices of international politics are based on socially constructed worldviews, identities, and ideas. Because of this, these patterns of interaction and social structures can change according to changes in the actors' ideas and assumptions about the nature of the world.[28] Eriksson and Giocomello opine that from a constructivist point of view, "interactions between states, other states, and non-state actors must evolve to fit the Internet age".[29]

While the realist position does provide some insight into the nature of the cybersecurity dilemma, it only considers states in its analysis, never non-state actors. It is undeniable that states

have more financial and technological resources, but terrorist groups, corporations, terrorist organizations, and individuals are all equally capable of deploying attacks within cyberspace.[30] While there is certainly still a cybersecurity dilemma, realism does not offer ways to deal with non-state actors who use cyberspace to launch damaging attacks, nor does it offer ways to deal with ideas and hostile moods which may arise from their actions.

This conceptual framework is relevant to the study because the constructivist interpretation of human security proffers an insight into the nature of interactions in cyberspace. It embraces a range of actors, alliances and agendas. It recognizes the impact a multiplicity of actors has on the architecture of cyberspace – as both the state and the individual wield power in that space. For constructivists, state interaction "reflects a learning process in which action shapes, and is shaped by identities, interests, and values over time".[3132] Thus, both the state and the individual have an impact on security in cyberspace. The concept of human security when used in cyberspace may be viewed as an application of the tenets of constructivism. This changing context of security addresses transnational problems such as terrorism and cyber threats.[33] Constructivism reinterprets traditional ideas in a state-centric society. Human security as a norm promoted by constructivism seeks to reorient the asymmetry of priority: the statist promotion of cyber sovereignty which may threaten the security of its citizens.

The concept of human security in this study would be used to evaluate the referent object of security in national cybersecurity strategies, as well as its impact on citizens, their privacy and freedoms and on the overall stability of international security.

1.9 Clarification of concepts

This study adopts some key concepts and technical definitions.

Cyber Definitions

Cyber as a prefix refers to electronic and computer based technologies. ***Cyberspace*** is an operational domain. In addition to the traditional land, air and sea environments, new environments such as outer space and cyberspace have become operational domains for states in their conduct of international relations.[34] As the milieu in which state military actions are conducted, operational domains may be distinguished from each other based on the different technologies required to operate within them. For example, naval ships to operate within the maritime environment, and aircraft to operate within aerospace

Not to be confused with virtual reality or an entity that exists only in the infosphere, cyberspace is a confluence of the human and electromagnetic environments. This study adopts Reveron's description of the three components of cyberspace: the physical, the information and the cognitive dimension. It consists of the link between activities that take place in the real world (cognitive and psychological), which may be collectively termed 'the human dimension', the information being transferred, and the physical electromagnetic spectrum (television, radio, satellite and computer networks).

A crucial and useful perspective of the cyber domain was offered by the "2003 United States National Strategy to Secure Cyberspace", which defined cyberspace as the "*nervous system—the control system of the country . . . composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.*"[35] The National Military Strategy for Cyberspace Operations, approved in December 2006 by Chairman of the Joint Chiefs of Staff General Peter Pace, it included a definition that closely mirrored the one suggested by David Kuehl. "*Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and*

exchange information via networked information systems and physical infrastructures."[36] Two additional official definitions were issued in early 2008. One came out of the White House, with President George W. Bush's signature of National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," on January 8, 2008.[37] While NSPD 54 itself is classified, its definition of cyberspace is not: "*Cyberspace means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries*." Whatever the strengths and weaknesses of these definitions, it is important to consider that they were issued within the context of a specific issue, the safety and security of military and government information networks.

Cyberspace is therefore "a unique hybrid regime of physical and virtual properties, hardware and software, which is all computer networks in the world including the Internet as well as other networks separate from and not linked to the Internet".[38] In this study, cyberspace, the internet, the cyber domain, the cyber sphere and the cyber realm are all synonymous to cyberspace.

The Internet as the biggest network in cyberspace was designed to be open, minimalist, and neutral. Alternative manifestations can be found in China or Saudi-Arabia.[39] The bordered Internet that emerged through national changes of the Internet's architecture is the result of national laws, technological developments enabling the implementation of certain policies. Yet, the Internet remains, from a technological point of view, borderless. Transnational or global would be the corresponding adjectives in international relations theory. While it is true that national legislation does create borders legally and sometimes through specific technical features such as The Great Firewall of China, the original design of the Internet ignores national

borders.[40] It is designed such that, without governmental interference, it is borderless unless specific interventions are taken to alter this state of nature.

The overarching term 'cybersecurity' refers to security within the cyber domain. ***Cybersecurity*** has been defined by the International Telecommunications Union as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets".[41]

Cyber power is the "ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power." 'Cyber power can be used to produce preferred outcomes *within* cyberspace or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace.[42]

The ***Post Snowden Era*** refers to the period after the NSA analyst Edward Snowden released classified information about the United States government's spying on its own citizens as well as foreign nationals. It is characterized by a heightened awareness of the cyber surveillance and cyber espionage operations carried out by states in the name of national security.

The Security Dilemma and the Cybersecurity Dilemma

The concept of 'a security dilemma' in international relations is useful in explaining the dilemma states face in cyberspace. This study adopts the definition of Heidi and Guy Burgess who state that "a security dilemma refers to a situation wherein two or more states are drawn into conflict, possibly even war, over security concerns, even though none of the states actually desire conflict. Essentially, the security dilemma occurs when two or more states each feel insecure in relation to other states. None of the states involved want relations to deteriorate, let alone for war to be

declared, but as each state acts militarily or diplomatically to make itself more secure, the other states interpret its actions as threatening. An ironic cycle of unintended provocations emerges, resulting in an escalation of the conflict which may eventually lead to open warfare".[43]

For Myriam Cavelty,

> "*we seem to be facing is a 'security dilemma', where efforts by one actor (traditionally, states) to enhance its security decrease the security of others. Because cyber-capabilities cannot easily be divulged by normal intelligence gathering activities, uncertainty and mistrust are on the rise. Although most states still predominantly focus on cyber-defence issues, measures taken by some nations are seen by others as covert signs of aggression by others and will likely fuel more efforts to master ''cyber-weapons'' worldwide".*[44]

For the purpose of this research, the national security and human security approaches to cybersecurity are defined as follows:

The national security approach to cybersecurity may be defined as one which is rooted in the notion of cyber-sovereignty which requires states to prioritize national security, and by extension the protection of critical national infrastructure, from cyber-attacks. Critical national infrastructure, as used in the study refers to physical digital infrastructure of a state, such as its transportation, communication, information and utility systems and computer networks.

The human security approach to cybersecurity, on the other hand, may be defined as a comprehensive approach which recognizes the multiple sources of insecurity across several dimensions and addresses them accordingly. It works towards ensuring cybersecurity at the individual level by making the human being the referent object of security.

1.10 Literature Review

Introduction

The body of academic knowledge on cyber issues has been expanding over the past two decades. In a world of over seven billion people cyberspace has become a fact of life. As the world transitions from the internet to the internet of things, the realities in cyberspace do not correspond with the traditional view of the international system, and the hierarchy of power relations which exist within it. It is a Janus-faced phenomenon which simultaneously creates opportunities for both conflict and cooperation. Cyber-based conflict such as cybercrime, cyber espionage and cyber warfare have proven that states are not the only relevant actors in world politics. In the 21st Century, an understanding of how the cyber domain influences national and human security is crucial to harnessing the power of the internet and enhancing global security. This study seeks to contribute to the current discourse on how states engage in politics within this space.[45]

Defining cyberspace

In the late eighties and nineties of the 20th Century, cyberspace was a very technological term, defined by data on computer systems. Very few people dealt with the internet at this time. The concept of cyber space has evolved since then and today has a much broader meaning.[46]

The term cyberspace was first coined by William Gibson's his 1984 book *Neuromancer*[47] as " … a consensual hallucination of data … experienced by billions of legitimate operators, in every nation, by children being taught mathematical concepts … a complexity in the non-space of the mind, clusters and constellations of data."[48]

Michael Froomkin later expanded the concept of cyberspace beyond physical computer systems when he posited that "Cyberspace is part of a greater reality than the one we already know. It is beyond our physical borders and our physical living environment."[49] Froomkin extended the concept of cyberspace beyond private and national borders.

Gibson neglected the importance of using cyberspace for communication and social interaction. In his 1996 article 'The Zones of Cyberspace', Lawrence Lessig covers the social aspects of cyberspace.[50] According to Lessig:

> *"Cyberspace is a place. People live there. They experience all sorts of things that they experience in real space, there. For some, they experience more. They experience this not as isolated individuals … they experience it in groups, in communities, among strangers, among people that they come to know, and sometimes like. While they are in that place, cyberspace, they are also here … They live this life there, while here."*

Froomkin's definition is limited to a statement about the "size" of cyberspace. In the earlier definitions of the concept the potentials or uses of cyberspace were ignored – that is, what it is used for and what it can be used for. Cyberspace is a product of real conditions and circumstances expressed through sociocultural, political and economic interactions. Although it has no clearly defined borders, it has a very real physical impact on our world, and also has the power to change it.

Anja Mihr offers a more vivid description of the human dimension cyberspace. According to Mihr, "Cyberspace is a global and borderless space in which social interaction between people takes place via technologies. Cyberspace offers an environment that consists of many participants with the ability to affect and influence each other."[51] Cyberspace is transparent and open in its nature, but is defined, broadened, censored and often limited by its users – individuals, private companies, governments and organizations.

David T. Kuehl provides the most encompassing definition of cyberspace. He defines cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communication technologies".

Features of cyberspace

Still, offering an acceptable definition of cyberspace has been a mammoth task for scholars in the face of the rapid technological advancements in the field. The other challenge is that definitions are developed to fit the agendas of the actors using it. Betz and Stevens outline some laconic features which characterize cyberspace[52]. These features include: "the pervasive anonymity of cyberspace participants, the speed and spread of communication, the multiplicity of actors, as well as the low cost of the technology and tools employed in the cyber domain.

Created with the internet at its core, some critical features of cyberspace are not congruent with a state-centric system. The fluidity, ubiquity and anonymity cyberspace provides is already reshaping the theory, policy and practice of international relations.[53] Choucri describes seven key features of cyberspace: *temporality, physicality, permeation, fluidity, participation, attribution*

and accountability.[54] To begin with, cyberspace replaces conventional temporality with almost instantaneous human interaction. Its physicality transcends geophysical constraints as it is a borderless digital world. It permeates local and international boundaries and jurisdictions by having a global infrastructure. Its fluidity is able to sustain shifts and reconfigurations in the modalities of human interaction. With regard to participation, it reduces the barriers to activism and encourages political participation – as was seen during the Arab Spring. According to Froomkin, as an inclusive tool, the internet could increase communication among all citizens.[55] It could increase citizens' participation in decision-making processes thereby increasing the legitimacy of governments and governance structures. In addition, attribution in cyberspace is difficult to establish. The anonymity it provides obscures the true identities of actors who wish to remain invisible. Even with mass surveillance programs, an electronic-point-of-origin is difficult to trace. In consequence, accountability in cyberspace is an issue of contention in domestic and international law.

Over five decades ago, scholars had already started the discourse on the impact cyberspace would have on our social reality. After the turn of the millennium internet usage has increased exponentially. According to Mihr, the number of internet users increased from 360 million in 2000 to 2.5 billion in 2013.[56] The dramatic expansion of cyber access begs the question, who controls cyberspace?

Actors in cyberspace

Cyberspace is a global domain, available for almost anyone with access to a computer with an internet connection, a smartphone or any other type of uplinked multimedia device. Mihr describes cyber actors as 'many participants with the ability to affect and influence each other'. Within this domain many different actors exist in parallel, with varying needs, goals and

intentions. Some act alone, others in loosely connected networks or more formal structures. The roles they play may also vary depending on the situation, and may overlap.[57]

Actors in cyberspace may be categorized in several ways. Actors can move between categories over time and depending on their current aims and goals. Whereas the dichotomy of state and non-state actors may be applied in a broad sense, a more detailed categorization may be proffered premised on the utility of cyberspace –network actors, technical actors, corporate actors, individual actors and threat actors

Johan Sigholm offers a more detailed classification of threat actors in cyberspace below.[58]

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decisionmakers or innocent victims	Protests via web page defacements or DDoS attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Cyberspace as an operational domain

While there is a tendency to designate cyberspace as a virtual domain, with little or no consequence of action as in the physical domain, the cyber reality has proved otherwise. The physical infrastructures of cyberspace actually reside in local jurisdictions. The Chairman of the United States Joint Chiefs of Staff General Peter Pace, in December 2006 included a definition in

The National Military Strategy for Cyberspace Operations that closely mirrored the one defined by David Kuehl. "*Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures*."[59]Cyberspace is a confluence of the human and electromagnetic operating environments[60], colonized by a multiplicity of actors, the security actions by states directly come to bear on human lives in multiple ways.

The growing importance of cyberspace to modern society and its increasing use as an arena for dispute is becoming a national security concern for governments and armed forces globally.[6162] The special characteristics of cyberspace, such as its asymmetric nature, the lack of attribution, the low cost of entry, the legal ambiguity, and its role as an efficient medium for protest, crime, espionage and military aggression, makes it an attractive domain for states as well as non-state actors in cyber conflict. Betz and Stevens opine that within three decades, cyberspace "has been defined in military doctrine as a new domain of conflict". Military experts have characterized cyberspace as a viable operational environment for war fighting. The logical result of its designation as a military domain is the rapid development of cyber offensive technologies and the eventual weaponisation of cyberspace.[63]

Sigholm suggests that many nations are currently pursuing cyber warfare capabilities, oftentimes by leveraging criminal organizations and irregular forces.[64] Employment of such non-state actors as hacktivists, patriot hackers, and cyber militia in state-on-state cyberspace operations has also proved to be a usable model for conducting cyberattacks. Nikolas Gvosdev[65] posits that Russia is developing cyber offensive capability for the purpose of cyber warfare. This trend in cyber offensive technologies is evident in state-sponsored cyber commands. Gvosdev describes them as 'hactivists', who deploy cyber-attacks alongside conventional military operations on the

ground. China is also alleged to possess such cyber capabilities, perceived to offer its army an asymmetric advantage on the battlefield. In his article 'A Treaty for Cyberspace', Rex Hughes opines that by 2010, "China, India, and Russia alongside the United States, the United Kingdom and South Korea are among the first group of countries to establish formal command and control over military assets in the cyber domain".[66]

In recent years, the increased media attention cyber threats have received has resulted in several governments developing or updating their cybersecurity strategies. Furthermore, the actions of some states have escalated cyber-fears, and increased tensions in the comity of nations. Brito and Watkins suggest that although consolidated figures are hard to acquire, financial commitments to cyber defence campaigns by states are on the rise.[67] As a result of the current trend an increasing number of states have publicly announced the existence of cyber units (cyber commands) – a specialized military unit for the deployment of both offensive and defensive attacks in cyberspace.

The gradual shift in the utility of the cyber domain from a civilian to a military space by states is representative of the power structures within the international system. According to Schneider, "states are asserting their power positions rather forcefully in the name of national security". The assertion of state power in cyberspace is linked to the notion of a 'Cyber-Westphalia'- the creation of national borders in cyberspace. According to Deibert et al., creating borders in cyberspace would result in a change of its topology. The militarization and balkanization of the cyber domain is thus borne from concepts such as 'cyber sovereignty' and 'cyber territories' as states seek more influence within cyberspace. As Clemente posits, the tensions that result from the development of cyber capabilities into cyber power in the international system culminates into the cybersecurity dilemma.[68]

The cybersecurity dilemma percolates vertically to impact the security of the international system, and extends horizontally to the security between states. The cybersecurity dilemma is a social structure in which the maneuvers of a state to enhance its security in the cyber domain is regarded as an act of military aggression by others. Since cyber capabilities are not easily deducible through conventional intelligence gathering, perceived notions of cyber capabilities results in increased mistrust and tensions in the international system, and is likely to spark a 'digital arms race' – the proliferation of 'cyber-weapons' around the globe.

Rid opines that cyber war serves as a force multiplier in conventional war, and is unlikely to occur alone.[69] The argument that cyber war occurs in concert with conventional war is a valid one. The use of cyberspace in the 2008 Russia-Georgia war is a clear example of this argument. To further buttress this point, a lot of literature, national security documents and cybersecurity strategies have been developed over the past two decades. President George W. Bush issued the "National Strategy to Secure Cyberspace" in 2003. Subsequently in 2011, President Barack Obama also issue the "International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World" as well as the 2013 "President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity". Across Europe, the United Kingdom (UK) and France, along with several states have published their own cybersecurity strategies – The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (2011), and France's Cyber Security Strategy: Information Systems Defence and Security - France's Strategy (2011). Kuehl points out in the case of the United States that the cybersecurity strategy focuses on the protection of critical infrastructure such as the security of government systems and military assets. With states developing policies to regulate the use of cyberspace, the issue of cyber governance arises.

The governance of cyberspace is quite nebulous. In its very design, the internet, which forms the nucleus of cyberspace, was never engineered with security in mind; rather it was engineered for rapid data transfer. The notion of governance as applied in this study refers to states, and international governmental and non-governmental organizations. Puja Abbassi et al. opine that state interest in cyberspace governance is driven by the protection of their critical infrastructure from intrusions and cyber-attacks. Even so, the absence of a central arbiter in cyberspace, and the drive to consolidate cyber power has delayed international efforts in developing laws and treaties to govern cyberspace.

Governance of cyberspace

Harold Kwalwasser[70] posits that the current form of governance existing in cyberspace combines institutions with ever evolving best practices. The Internet Corporation for Assigned Names and Numbers (ICANN), The International Telecommunications Union, the World Wide Web Consortium and the International Organization for Standardisation are all technical entities. Although it is presumed that some states, particularly the United States, influence the operations of these technical bodies, most cyberspace interactions occur within the civilian space. As the world's hegemon, with a private sector that owns most of the global infrastructure of the internet, states such as Russia and China are not in support of the United State favoured governance model.

It is important to re-emphasize that discussions on cyber governance mostly focus on state-to-state relations in cyberspace. The critical issues for major players has been on the key issues for the negotiation of an international agreement. While attacks on critical infrastructure has been most important on the agenda for some actors, others are advocating for a free, open and very democratic internet for the unhindered flow of information. The only international agreements on

cyberspace is the draft agreement of the African Union, which mainly focuses on electronic transactions, and the European Convention on Cybercrime.

This study seeks a possible framework for breaking the cybersecurity dilemma. There is not much literature has discussed the application of human security to understanding the cybersecurity dilemma. The cybersecurity dilemma is a social construct especially since the basis of the situation is malleable by human action: Deibert et al. argue that, unlike aerospace, outer space, or the maritime environment, cyberspace is an artificial domain which shapes and is being shaped by the actors that operate in it.[71] In the way in which cybersecurity is understood and practiced, the cyber-security dilemma is a national security issue at the policy level. It is worthy to note that the social entities with power (mainly states) view this issue from different perspectives based on specific security-related practices. States actions within the international system is based on how a state views its position with relation to other states in the system. Thus, what is seen as a national security issue by the United States that requires military-operated cyber commands is regarded as a civilian issue by some European countries.

1.11 Research Methodology and Sources of Data

Sources of data

The study is mainly a qualitative research. Therefore, data used in the research relies heavily on secondary sources which focus on cybersecurity in international relations. These include journal articles, books and national cybersecurity strategy policy papers which are available in the public domain.

Methodology

This study utilizes a qualitative research methodology based on secondary sources of data to accomplish its objectives. An analysis of the cybersecurity policies of the United States and Canada, within the temporal period of the Post-Snowden era has been undertaken.

1.12 Arrangement of Chapters

The study is organized into four main chapters. Chapter one is the introductory chapter which outlines the research design. Chapter two is an Overview of Cybersecurity, and the National and Human Security Approaches to Cybersecurity. It describes the kind of security cybersecurity is, and elaborates on the linkages between cyberspace, national security and human security, as well as current national approaches to cybersecurity using the United States and Canadian cybersecurity strategy documents. Chapter three focuses on Balancing National and Human Security in Cyberspace. It describes the convergence of national security and human security in cyberspace and how such a balance can be achieved. Chapter four presents a summary of findings, recommendations and a conclusion.

ENDNOTES

[1] Saler, Michael. "THE DARK NET Inside the digital underworld." (2015): 3-5.

The Dark Net which represents the digital underworld is much different from the online world most people are familiar with – a world Google, Bing, Facebook and Twitter. Its content is beyond the reach of regular search engines, residing in a hidden network of sites, invisible digital communities and an online culture which gives ordinary people the freedom to be anyone, or do anything they want. Beginning with the evolution of the internet and the invisible wars that defined its early years, Bartlett investigates the digital underworld and presents an extraordinary view of an unknown internet: trolls, pornographers, drug dealers, hackers, political extremists, Bitcoin programmers, and vigilantes. The author puts a human face on such actors who cling to the anonymity this world provides.

[2] Choucri, Nazli. Cyberpolitics in International Relations. MIT Press, 2012.

Cyberspace is widely acknowledged as a fundamental fact of daily life in today's world. Until recently, its political impact was thought to be a matter of low politics--background conditions and routine processes and decisions. Now, however, experts have begun to recognize its effect on high politics--national security, core institutions, and critical decision processes. In this book, Choucri investigates the implications of this new cyber-political reality for international relations theory, policy, and practice. The unique nature of cyberspace have already challenged such concepts as leverage and influence, national security and diplomacy, and borders and boundaries in the traditionally state-centric arena of international relations.

[3] "Cyber Attacks Statistics – HACKMAGEDDON". *Hackmageddon.com*. N.p., 2016. Web. 13 July 2016.

[4] Reveron, Derek S., and Kathleen Mahoney-Norris. Human security in a borderless world. Westview Press, 2011.

[5] Kreuzer, Michael P. *Drones and the Future of Air Warfare: The Evolution of Remotely Piloted Aircraft*. Routledge, 2016.

[6] "U.S. Air Force - Mission". *Airforce.com*. N.p., 2016. Web. 12 July 2016. https://www.airforce.com/mission , "The mission of the United States Air Force is to fly, fight and win in air, space and cyberspace. Our rich history and our vision guide our Airmen as we pursue our mission with excellence and integrity to become leaders, innovators and warriors."

[7] Madden, M. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Internet Project* (2014). Edward Snowden's revelations of classified documents related to the National Security Agency's surveillance and spying operations has ignited a global debate over balancing personal privacy and national security since June 2013. The Post-Snowden Era denotes the period after this incident where the public is now more aware of government mass surveillance operations.

[8] Rohret, David, and Michael Kraft. "Catch me if you can: Cyber Anonymity." *The Proceedings of the 6th International Conference on Information Warfare and Security*. 2011.

[9] Ibid.

[10] Cavelty, Myriam Dunn. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and engineering ethics* 20.3 (2014): 701-715.

[11] InfoSec Institute,. 'China Vs. US, Cyber Superpowers Compared - Infosec Institute'. N.p., 2013. Web. 4 June 2015.

[12] Cavelty, Myriam Dunn. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities." *Science and engineering ethics*20.3 (2014): 701-715.

[13] Atanassova-Cornelis, Elena. "Japan and the 'Human Security' Debate: History, Norms and Pro-active Foreign Policy." *Graduate Journal of Asia-Pacific Studies* 3.2 (2005): 58-74.

[14] Griffiths, Martin, Steven C. Roach, and M. Scott Solomon. *Fifty key thinkers in international relations*. Routledge, 2008.

[15] Miller, Frederic P., Agnes F. Vandome, and McBrewster John. *Constructivism In International Relations*. VDM Publishing, 2010. Print.

[16] See Wendt, Alexander. "Anarchy is what states make of it: the social construction of power politics." *International organization* 46.02 (1992): 391-425.
[17] Carlsnaes, Walter, et al., eds. *Handbook of international relations*. Sage, 2002.
[18] Finnemore, Martha, and Kathryn Sikkink. "Taking stock: the constructivist research program in international relations and comparative politics." *Annual review of political science* 4.1 (2001): 391-416.
[19] Kukla, A. *Social Constructivism And The Philosophy Of Science*. New York: Routledge, 2000. Print.
[20] McDonald, Matt. "Human security and the construction of security." Global Society 16.3 (2002): 277-295
[21] Ibid.
[22] Schnurr, Matthew A and Larry A Swatuk. *Natural Resources And Social Conflict*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2012. Print.
[23] Newman, Edward. "Human security and constructivism." International studies perspectives 2.3 (2001): 239-251.
[24] Chandler, David (2008) 'Human Security: The Dog That Didn't Bark', *Security Dialogue*, 39(4), pp. 427-439.

[25] Martin, Mary and Taylor Owen (2010) 'The Second Generation of Human Security: Lessons from the UN and EU Experience', *International Affairs*,86(1), pp. 211–224.

[26] Madrueño-Aguilar, Rogelio. "Human Security and the New Global Threats: Discourse, Taxonomy and Implications." *Global Policy* (2016).
[27] MacFarlane, S. N. and Y. F. Khong (2006) *Human Security and the UN: A Critical History*, Indianapolis: Indiana University Press.

[28] Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *ISA Annual Convention, San Diego, CA April*. Vol. 1. 2012.
[29] Eriksson, Johan & Guacamole, Giampiero. "The Information Revolution, Security, and International Relations". International Political Science Review Vol. 27, No. 3 (Jul., 2006), pp. 221-244

[30] Petallides, Constantine J. "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Student Pulse*4.03 (2012).
[31] Griffiths, Martin, Steven C. Roach, and M. Scott Solomon. Fifty key thinkers in international relations. Routledge, 2008.
[32] Newall, Diana, ed. *Fifty Key Thinkers in International Relations*. Routledge, 2012.
[33] See Newman, Edward. "Human security and constructivism." International studies perspectives 2.3 (2001): 239-251. International security has been traditionally defined as military defence of territory from external attack in an anarchic state-centric system. According to Realist thinkers such as Waltz, national security is imperative for territorial defence, and deterrence of foreign military threats. However, the traditional approach to security does not address the state as an aggressor, as well as transnational threats which may contribute to human insecurity.
[34] Bashow, D. "Canadian Military Journal Vol. 12, No. 3". *Journal.forces.gc.ca*. N.p., 2011. Web. 12 July 2016.
[35] Sherwood-Randall, Elizabeth. Alliances and American National Security. Maroon Ebooks, 2015
[36] Kuehl, Daniel T. "From cyberspace to cyberpower: Defining the problem. "*Cyberpower and national security* (2009): 26-28. In Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. *Cyberpower And National Security*. Washington, D C: Center for Technology and National Security Policy, 2009. Print.
[37] Bush, George HW, and Brent Scowcroft. A world transformed. Vintage, 2011.
[38] Anderson, Charletta. "Cyber Security and the Need for International Governance." *Available at SSRN 2769579* (2016).
[39] "Four Quadrants - Identifying Difficult Problems In Cyber law". *Cyber.law.harvard.edu*. N.p., 2011. Web. 12 July 2016.
[40] Maurer, Tim. "Cyber norm emergence at the United Nations." *Science, Technology, and Public Policy Program* (2011).
[41] "Cybersecurity". *ITU*. N.p., 2016. Web. 12 July 2016.

[42] "Cyber Power In The Changing Middle East - Turkish Policy Quarterly". *Turkish Policy Quarterly*. N.p., 2016. Web. 12 July 2016.
[43] Kanji, O. 2003. 'Security' in Burgess, G. and H. Burgess (eds.). *Beyond Intractability*. Conflict Research Consortium, University of Colorado.
[44] Dunn Cavelty, Myriam. "Breaking The Cyber-Security Dilemma: Aligning Security Needs And Removing Vulnerabilities". *Sci Eng Ethics* 20.3 (2014): 701-715. Web.
[45] Choucri, Nazli, and Daniel Goldsmith. "Lost in cyberspace: Harnessing the Internet, international relations, and global security." *Bulletin of the Atomic Scientists* 68.2 (2012): 70-77.
[46] See https://iversity.org/en/my/courses/public-privacy-cyber-security-and-human-rights/lesson_units/4394
[47] Gibson, William. "Neuromancer New York." *Ace* 9 (1984).
[48] See McCaffery, Larry, and William Gibson. "An Interview with William Gibson."*Mississippi Review* (1988): 217-236.
[49] Froomkin, A. Michael. "Toward a critical theory of cyberspace." *Harvard Law Review* (2003): 749-873.
[50] Lessig, Lawrence. "The zones of cyberspace." *Stanford law review* (1996): 1403-1411.
[51] Mihr, Anja. "Public Privacy Human Rights In Cyberspace." (2013).

[52] Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. IISS-The International Institute for Strategic Studies, 2011.

[53] Choucri, Nazli. *Cyberpolitics in international relations*. MIT Press, 2012.
[54] Ibid.
[55] Froomkin, A. Michael. "Habermas@ discourse. net: Toward a critical theory of cyberspace." *Harvard Law Review* (2003): 749-873.
[56] Mihr, Anja. "Public Privacy Human Rights In Cyberspace." (2013).
[57] Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012).
[58] Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4.1 (2013).
[59] Kuehl, Daniel T. "From cyberspace to cyberpower: Defining the problem. *"Cyberpower and national security* (2009): 26-28.
[60] Gash Jim. Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits. Canadian Military Journal, Issue 12, No 3, 2012.
In addition to the traditional land, air, and maritime environments, many strategists are proposing the introduction of new environments for consideration by military force developers. The Canadian Forces (CF) Integrated Capstone Concept (ICC) published in 2011 by CF proposes three new environments, referred to as domains—space, cyber, and human—while declaring that even more operating domains will emerge in the future. Specifically, nano and quantum domains are mentioned as possibilities. Gash argues that the cyber environment is nothing new. Rather, it is simply a unique manifestation of the electromagnetic (EM) operating environment. The cyber environment is thus physical because it manifests only through the actual interaction between electrons and electromagnetic energy.
[61] See Kuehl, Daniel T. "From cyberspace to cyberpower: Defining the problem. *"Cyberpower and national security* (2009): 26-28.
[62] Sigholm, Johan. "Non-state actors in cyberspace operations." *Journal of Military Studies* 4.1 (2013).
[63] Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. IISS-The International Institute for Strategic Studies, 2011.

[64] Sigholm, Johan. "Non-state actors in cyberspace operations." *Journal of Military Studies* 4.1 (2013).
[65] Gvosdev, Nicholas K. "" The Bear Goes Digital: Russia and Its Cyber Capabilities." *Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. Washington DC: Georgetown University Press* (2012).

[66] Hughes, Rex. "A treaty for cyberspace." *International Affairs* 86.2 (2010): 523-541.
[67] Brito, Jerry, and Tate Watkins. "Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy." *Harv. Nat'l Sec. J.* 3 (2011): 39.

[68] Clemente, Dave. *Cyber Security and Global Interdependence: What Is Critical?*. Chatham House, Royal Institute of International Affairs, 2013.
[69] Rid, Thomas. "Cyber war will not take place." *Journal of strategic studies*35.1 (2012): 5-32.

[70] Kwalwasser, Harold. "Internet governance." *Cyberpower and national security* 510 (2009).

[71] Deibert, Ronald, et al. *Access denied: The practice and policy of global internet filtering*. MIT Press, 2008.

CHAPTER TWO

AN OVERVIEW OF CYBERSECURITY, NATIONAL SECURITY & HUMAN SECURITY IN CYBERSPACE

2.1 Introduction

In April 2014, the renowned security strategist, Myriam Dunn Cavelty, published an article on the uncertainty in security politics and changing conceptions of international security due to cyber issues (cyber-security, cyber-war, critical infrastructure protection). Earlier in 2012, Bruce Schneier also published an article about the imminent threat of cyberwar and the proliferation of cyber weapons when he stated that:

> We are in the early years of a cyberwar arms race. It's expensive, it's destabilizing, and it threatens the very fabric of the internet we use every day.[1]

Although from the above statement Schneier describes the Internet as the referent object of security, it is quite clear that digital arms race must be driven by states and their militaries. The increased media attention cyber threats have received has resulted in several governments developing or updating their cybersecurity strategies. Furthermore, the actions of some states have escalated cyber-fears, and increased tensions in the international system. Brito and Watkins posit that although consolidated figures are hard to acquire, financial commitments to cyber defence campaigns by states are on the rise.[2] As a result of the current trend an increasing number of states have publicly announced the existence of cyber units (cyber commands) – a specialized military unit for the deployment of both offensive and defensive attacks in cyberspace.

In many respects, the issue of cyberspace, particularly with regard to inter-state relations, has already assumed conflict dimensions. Dunn explains that states inability to gauge other states' intentions, through the conventional intelligence procurement methods when these perceived

belligerent states bolster their cyber-defense capabilities, creates an uneasiness in the international system.[3] Moreover, threatened states tend to react by also increasing their cyber-defenses infrastructure and capabilities which could lead to a race to master "cyber weapons."[4]

When one considers the underlying principle that states have an obligation to provide security for their citizenry and domestic corporations on the one hand, and the penchant of the private sector to commercialize security on the other hand, the situation becomes even more complex. It is therefore necessary to provide an overview of cybersecurity to delineate its overarching tenets.

This chapter deals with the emergence of cyberspace and the ongoing dialogue on cybersecurity. It would also provide some regional perspectives on cybersecurity and accompanying issues: its link to international security, the major actors, current cybersecurity concerns, and national approaches to cybersecurity. The chapter then discusses the national security and human security approaches to cybersecurity. The chapter ends with a conclusion on the prospects of the debate on cybersecurity.

2.2 The Emergence of cyberspace

While the term cyberspace entered literature when it was used by William Gibson in his 1984 book," Neuromancer", the term was widely used in the "early 1990s, when cyberspace was viewed as separate from the normal physical world".

The technical components of cyberspace were developed in the 1960s by the Defence Advanced Research Project Agency (DARPA). The brainchild of DARPA, which was then known as ARPANET (Advanced Research Project Agency Network) later grew to become the internet we know today.

The cyber domain is fast evolving, and this evolution is seen in the increasing numbers of users in cyberspace, and the quality of their participation. As an example, a 2015 International Telecommunications Union (ITU) report[5] stated that there were over 7 billion mobile cellular subscriptions worldwide, and globally 3.2 billion people were using the internet. In addition, if Facebook users comprised the citizenry of a state it would be the most populated country in the world.[6]

The emergence of innovative communication technologies and tools in cyberspace has increased the number of users and industry players from a few academics and engineers to a global membership. The increased dependence on cyberspace in human life today can be seen in its control of national and international transport systems, e-commerce, electric power grids and e-governance mechanisms. Almost all the physical components - the routers, switches, fibre optics, embedded processors, computer networks, electronic gadgetry – are networked. The internet-of-things interconnected in cyberspace continues to grow at exponential rates.

2.3 Cyberspace and security

In the face of their increasing complexity and rate of occurrence, some high-profile cyber-attacks have come to be recognized as an international threat. While some of these attacks are trivial and do not pose much of a threat to states or corporations, some pose a big threat as they are capable of taking out electricity grids, train networks or even nuclear plants(Stuxnet). As a result of some these attacks, cyber-space previously thought of as a haven of privacy is no longer a private realm. This is particularly evidenced by WikiLeaks, a whistleblower website, that has published several classified documents ranging from secret government documents to confidential corporate files

While the cyber domain presents exceptional opportunities to actors within cyberspace, trends in cyberspace also present major challenges to the security of states. These arise from the use of cyberspace by malevolent actors and its many security vulnerabilities that plague cyberspace – for example, challenges in attribution, denial-of-service attacks, exfiltration and corruption of sensitive data.[7]

Clarke and Lynn describe cyberspace as a new "domain" of conflict, an operational environment in which state and non-state actors can deploy strategic "cyber-attacks" against their adversaries.[8] The 2011 Pentagon strategic plan for cyberspace identified cyberspace as an "operational domain," akin to other domains such as air, sea, and space. The Defense Department stated its plan to "organize, train, and equip for cyberspace as we do in air, land and sea".[9] Such conflict may occur only within cyberspace, lead to escalation among the actors in the physical domain, or inflict economic or physical damage. In the literature, there is disagreement about the nature and scale of cybered -conflict Clarke refers to persistent and increasing attacks in cyberspace, but does not specify the target or scale of cyber-attacks. Most literature by experts in cyberspace describe the most dominant cyber threats as consisting of espionage and cyber-crime – activities which are not traditionally considered to be an attack at all, at least not in the context of internationally accepted laws of war.

Clarke, Clark and Levin, Lynn, and Christopher Hughes[10] all argue that large-scale strategic attacks through the cyber domain against "critical national infrastructure" pose a grave threat to national security. The advantage of offence goes to the adversary, they argue, because the low cost and anonymity the attacker enjoys. They all argue that cyber defense strategies do not provide sufficient protection against cyber-attacks, as they impose little or no cost on a failed

attacker, who is free to try again. As a result, Lynn raises the need for active defense – "the United States and its allies must develop offensive cyber capabilities as a deterrent.

2.3.1 The Major Players in cyberspace

As the technological advances increase, so does the number of threats in the cyber domain. From WhiteHat (ethical) hackers looking to highlight the vulnerabilities of a computer system, to BlackHat hackers trying to steal personal data for the purposes of blackmail, to experienced criminals devoted to stealing financial information, to hacktivists looking to protest, to states seeking to expand their influence in the cyber domain, malevolent hackers come in various forms.

The literature fails to fully address the roles of non-state and private actors in cyber defense. Several of the authors note that cybersecurity's heavy involvement of civilian actors in the private sector makes the employment of deterrence more difficult than in traditional domains. Clarke and Adams, for example, both describe corporations as the principal target for cyber-attacks. Both also suggest that the state play a larger role in defending civilian networks. Yet there has been little effort to explore the implications of this interdependence between the state and private sector beyond Rex Hughes's observation that cyberspace blurs the boundary between the two.

More is said about non-state actors in the academic literature. Der Derian describes how non-state actors are becoming "super-empowered players" in a "global heteropolar matrix" of networked relationships.[11] Dartnell similarly describes the empowerment of non-state actors and the formerly marginalized in cyberspace.[12] In this digital era, non-state actors infiltrate existing

legal networks through money laundering that links the criminal economy to the global market. In addition, they are able, independently, to build their own web nodes (e.g., terrorist or criminal organizations) and operate undetected. For example, terrorist groups, such as Al-Qaeda or most recently ISIS (Islamic State in Syria), are adept at using cyberspace for propaganda, recruitment and money laundering to forward their political agenda. They establish the covert networks to operate in every corner of the world. Consequently, their use of cyberspace has enabled these groups to intimidate global powers through cyberattacks, remote control bombs, and the radicalization of new followers from around the world.

However, these authors focus on non-state actors as the source of threats in cyberspace. They address neither the interdependence between the state and private sector in securing cyberspace, nor do they fully explore the ways in which different non-state actors might be empowered by cyber technology.

2.4 Current national approaches to cybersecurity

States depend on reliable communication networks and information services to ensure economic stability and the welfare of their citizenry. Attacks on critical national infrastructure, such as telecommunications networks cause disruptions in the provision of such essential services. Such disruptions reveal the increased dependency of our society on cyberspace and all the opportunities it provides. This is echoed in the German cyber security strategy which states that, "The availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international level."[13]

Cybersecurity is now regarded as a strategic national and international issue affecting all levels of society. States have therefore resorted to developing cybersecurity strategies to guide their actions in cyberspace. A national cyber security strategy (NCSS) is a "tool to improve the security and resilience of national infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such it provides a strategic framework for a nation's approach to cyber security".[14]

This study looks at the areas of focus of the current status of cyber security strategies within the European Union (EU) and elsewhere.

2.4.1 The cybersecurity strategies of some European Union member states

The first national cybersecurity strategies were developed within the first decade of the 21st Century. At the forefront of this movement was the United States who published the 'National Strategy to Secure Cyberspace[15] in 2003. It was a part of the overall National Strategy for Homeland Security, which was developed in response to the September 11th terrorist attacks in 2001.

Action plans and strategies with limited focus on state actions in cyberspace were developed for similar across Europe in the following years. In 2005, Germany published the "National Plan for Information Infrastructure Protection (NPSI)"[16]. The next year, Sweden adopted a 'Strategy to improve Internet security in Sweden'. Following the widely publicized cyber-attack on Estonia in 2007, the country was the first member of the European Union (EU) to publish a broad national cybersecurity strategy in 2008[9]. Since then a considerable number of states have published a national cyber security strategy.

While several member states in the EU have developed cybersecurity strategies, their areas of focus are not always the same. A summary of the key points of some selected cybersecurity strategies have been listed below.

Estonia (2008): Estonia emphasizes the necessity of a secure national cyberspace and focuses on the protection of information systems. Their recommended measures are all civil in nature and concentrate on education, regulation and cooperation.[17]

France (2011): France focuses on the creation of robust information systems to resist events in cyberspace which could compromise the integrity, availability or confidentiality of data. France emphasizes both technical means related to the security of digital infrastructure and the fight against cybercrime, and the establishment of cyber-defence capabilities.[18]

Germany (2011): Germany focuses on the prevention and prosecution of cyber-attacks, and on the prevention of disruptions in information services, especially where critical infrastructures are concerned. The strategy sets the ground for the protection of critical digital[19] infrastructures.

Netherlands (2011): The Netherlands cybersecurity strategy is aimed at the provision of a safe and reliable digital infrastructure while protecting the openness and freedom of the Internet. The Netherlands provides a definition of cybersecurity in their strategy: "Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."[20]

United Kingdom (2011): The UK approach is an amalgamation of national objectives and the evolving field of cybersecurity. It seeks to make the UK the largest economy of innovation, investment and quality in the field of information technology, and by this to be able to fully exploit the potential and benefits of cyberspace. This strategy also tackles the threats from cyberspace like cyber-attacks from criminals, terrorists and states in order to make it a safe haven for corporations and citizens.[21]

2.4.2 The Cybersecurity strategies of Africa

Below is a short description of cybersecurity strategies from Africa. Many other countries have also published NCSS, for example, Australia, India, Colombia and New Zealand.[22] The list is by no means exhaustive. However, it does illustrate that the importance of cybersecurity is recognized globally.

Although digital penetration on the African continent is on the ascendancy, African states have made little strides in cyberspace governance. There are very few states with cybersecurity strategies. Nine states have published official cybersecurity strategies. The first African state to release a cybersecurity strategy document was South Africa in 2010, followed by Uganda in 2011. Even though South Africa had already published a strategy in 2010 to regulate state actions in cyberspace, it released a strategy alongside Mauritania in 2012. The Mauritanian 'National Strategy for Modernization of Administration and ICT' developed specific action plans for the temporal period of 2012 to 2016. The following year Egypt and Morocco published their strategies, with Kenya and Mauritius following suit the year after. In the West African sub-region, Ghana announced the development of a cybersecurity strategy in 2014, while Nigeria published theirs in 2015.[23]

The most significant attempt on cyberspace governance has been advanced by the African Union (AU). The proposition of the Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa (Draft African Union Convention on the Confidence and Security in Cyberspace) in 2012 signifies an effort by the to influence the course of cybersecurity policy on the continent.[24]

The provisions of the Convention focuses primarily on e-commerce and financial transactions in cyberspace. The conceptual framework states that "the objective of this Convention is to propose the adoption at the level of the African Union, of a Convention establishing a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cybersecurity, e-governance and combatting cybercrime".[25] It urges individual states to establish legal frameworks in their jurisdictions such that domestic laws cover all the key areas in cyberspace highlighted by the conceptual framework.

All these actions towards the development of cybersecurity strategies to guide state actions in cyberspace underscores the importance of the issue on the African continent, as well as in the international system as a whole.

2.4.3 Common themes

According to Luiijf, Besseling, Spoelstra and De Graaf a harmonized definition of cybersecurity is clearly lacking.[26] The understanding of cyber security and other key terms[27] varies considerably from state to state. This influences the different approaches to cybersecurity strategy among states. While global powers describe cyberspace as a domain for future conflict, middle powers focus mainly on the protection of digital infrastructure and civil liberties. This lack of common understandings and incongruence in the approaches between states may hinder international cooperation, the need of which is acknowledged by all states.

The key areas covered by a typical NCSS include:

1. A governance framework for cybersecurity.
2. An appropriate mechanism that allows all relevant actors to discuss and agree on policies and regulations with regard to cybersecurity issues.
3. Policy and regulatory measures and clearly defined roles, responsibilities and rights of the state and private sector. For example, the Slovakian cybersecurity strategy identifies a need to define a legal framework for the protection of cyberspace.[28]
4. Goals and means to develop national capabilities and the necessary legal framework to engage in the international efforts of diminishing the effects of cybercrime. In several

strategies, there is a particular focus on cybercrime. For example in the Netherlands which aims to intensify investigation and prosecution of cybercrime.[29] France also stresses this point and wish to promote the strengthening of current legislation and international judicial cooperation.[30]

5. To identify critical information infrastructures including key national assets, services and interdependencies.
6. To develop or improve preparedness, response and recovery plans and measures for protecting such critical infrastructures. For example, national contingency plans, cyber exercises, and situation awareness. The Lithuanian strategy states that "to ensure cyberspace security it is necessary to establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation,"[31] to define a systematic and integrated approach to national risk management.
7. To define and set the goals for awareness raising campaigns that instill changes in the behaviour and working patterns of citizens.
8. To define the needs for new curricula with emphasis on cyber security for IT and security professionals and specialists; and also training programs that allow the improvement of skills of users. For example, the UK strategy aims to improve training and education for information security specialists to create a strong cyber security profession.[32]

2.5 The National Security Approach to Cybersecurity

Computers and national security have been linked since World War II. The first computers were created during World War II for military purposes. According to Daniel Ventre, national agencies in the United States such as the NSA and the CIA funded computer science research in

the 1950s. During the Cold War, computer industries were targeted by espionage. As a result, the protection of computers and computer systems from foreign espionage has formed the basis of cybersecurity as a national security issue.[33]

According to General Michael Hayden, former US National Security Director, and the Former Head of the CIA, "*the nature of today's internet constitutes a threat*"[34]. The internet was created by DARPA to link a very limited number of network nodes, all of which were known and trusted, for the free flow of information. That remains the engineering principle of the internet, in which there are an unlimited number of network nodes, most of which are unknown and do not deserve to be trusted. Thus, cyberspace is an indefensible domain because it was not engineered to be secure, but rather to facilitate rapid data transfer. As a result, in the absence of malevolent actors, cyberspace presents a threat to national security. Yet still, there are malevolent actors: cyber criminals, hactivists, terrorists, and states using cyberspace for espionage or to create physical destruction such as the Stuxnet attack on the Iranian nuclear plant.

Even in states with vibrant IT industries and cyber commands, governments are struggling to ensure that security in cyber domain is at par with security in the land, air and maritime domains. That reality drives the conclusion that no state, not even a global hegemon, can unilaterally securitize cyberspace without the help of the private sector and the citizenry. As most of the digital infrastructure is privately owned, the private sector the more dominant role of providing security in cyberspace, while the state protects its citizenry in the physical domains of land, air, and the sea.

2.5.1 Militarization of Cyberspace

Although the term "revolution in military affairs" or "RMA" dates back more than three decades, it became popular to speak of such a revolution after the first Gulf War.[3536] The term refers to qualitative changes in military capabilities brought on my technological innovation and/or novel forms of military organization.

As far back as the Gulf War, the United States military thinking designated cyberspace as an operational domain. Through the use of intelligence gathering in the cyber domain, mass bombings on targets had been transformed into precision strikes. Thus, battlefields effects were now achieved using precision weapons operated by weapons guidance systems. Consequently, the United States Air force invested vast resources into information dominance and information superiority in cyberspace, since precision relies heavily on intelligence. The most important military doctrine which was embraced by national security policy makers was the designation of cyberspace as an operational domain. Cyberspace thus became a place where a state's military could ensure freedom of action, while holding in reserve the ability to deny such freedom on action by other states.

Several of the authors treat information technology as a military technology that can enhance traditional forms of state military power. However, even within this group, there is some disagreement over the nature of the technology and how it can best enhance military capabilities. Newmyer and Goldman, for example, both discuss the contribution of information technology to the revolution in military affairs (RMA[37]). Goldman describes cyberspace as an efficiency-booster or multiplier that allows modern militaries to quickly distribute large volumes of information and filter them in order to identify what is strategically relevant. Newmyer, on the other hand, sees cyberspace primarily as a tool that can disrupt an enemy's information systems. For Goldman, cyberspace is most useful to states that already possess sophisticated military

capabilities, while for Newmyer, it is a tool of asymmetric warfare that provides advantages to weaker states through its low barriers of adoption and use.

Cyberspace is thus an operational domain with unique characteristics: it is inherently global, inherently strategic, and characterized by great maneuverability and speed. In this particular domain, practically all the advantage goes to offence. Every piece of information technology – hardware or software - can be compromised by exploiting the right vulnerabilities. Hence, a case can be made for cybersecurity.

In this context, policies addressing the cybersecurity issue developed by states naturally evolved from cyberspace as domain for intelligence gathering in 1997 to a Cyber Command at Forte Meade in 2009. As an operational domain, states military operations there could have decisive effects in future wars. This analogy is drawn from historical precedents. The Battle of Gettysburg was primarily a land battle, the battle of Trafalgar a sea battle, and the battle of Britain and air battle which decided if there would be an invasion of the British Isles. Consequently, the designation of cyberspace as an operational domain evokes the possibility of creating decisive effects in that domain.

This logic from the national security approach has driven the need for states to acquire cyber commands, cyber forces and cyber weapons to fight in this domain. According to the US Cyber Command Charter, the cyber command "is charged with the conduct of full spectrum of military cyber operations", thus the cybersecurity strategy of the United States is largely driven by national security needs.

Within a few months of the US Cyber Commands' establishment, cyber fears began escalating in the international system, sparking a digital arms race. In 2009, the United States was the most feared nation in cyberspace, buy by 2015 Russia, China, Israel and Iran had joined the fray.

Another complication is that the national security approach has institutionalized the its experience from other domains and conferred them on cybersecurity. While in traditional domains reconnaissance (surveillance) is employed prior to an attack, in the cyber domain it is very difficult to ascertain the intentions of a malevolent actor once they penetrate a network. This has informed the adoption of the preemptive strike doctrine with the establishment of cyber commands.

There is no global consensus on what constitutes cyber aggression by states. Does a computer file on a server in Ontario, Canada enjoy the same sovereignty as the building it resides in? Cybersecurity presents a challenge to states, laws, institutions and the way in which the concept of security has been constructed in other domains. Ensuring cybersecurity would require a more comprehensive framework which would align national security needs and reduce cyber tension within the comity of nations.

2.5.2 Sovereignty and Balkanization of Cyberspace

The cyber domain transcends national boundaries and diminishes state influence over their citizens and other actors. Sovereignty is a key feature of state authority and action. In the international system, sovereignty, the practice of exercising control over a territory, is one of the key elements of statehood.

The concept of sovereignty as defined by Krasner encompasses domestic sovereignty[38] (the arrangements within a state on the regulation of behaviour and public authority, interdependence

sovereignty (the control of ideas, people and materials), international legal sovereignty (the recognition of states as being equal to one another), and Westphalian sovereignty (states making decisions within their jurisdiction without external influence).

Developments within states such as China and Iran to create a national local area network (LAN) separate from the internet indicates that states wish to assert sovereignty over cyberspace (cyber sovereignty) and territorialize it. The 'Great Firewall of China'[39] is an experiment by a global cyber power to censor access to the Internet. In a similar direction, Iran has made attempts to build a national intranet deinked from the global internet to protect its citizens from the influence of western ideals and values, since a majority of online content is being generated by western nations. In both cases, the exertion of sovereignty in cyberspace is directed at controlling access to, as well as the free flow of information.

The issue of cyber sovereignty becomes more complex when dealing with cybercrime. The fundamental question of whether criminal actions considered illegal in one state can be prosecuted by another state when it occurred in cyberspace is still being debated. Cyberspace may then have a significant impact on what the state can or cannot do about acts that contravene its domestic regulations on cyberspace. As a result, state sovereignty and territorialisation in cyberspace coupled with the absence of an international agreement to guide state action has led to the creation of safe havens for cybercriminals to thrive.

2.6 The Human Security Approach to Cybersecurity

> *Faced with the potential good of globalization as well as its risks, faced with the persistence of deadly conflicts in which civilians are primary targets, and faced with the pervasiveness of poverty and injustice, we must identify areas where collective action is needed—and then take that action to safeguard the common global interest.*[4041]
>
> UN Secretary-General Kofi Annan, "Problems Without Passports," September, 16,2002

> *We stress the right of people to live in freedom and dignity, free from poverty and despair. We recognize that all individuals, in particular vulnerable people, are entitled to freedom from fear and freedom from want, with an equal opportunity to enjoy all their rights and fully develop their human potential. To this end, we commit ourselves to discussing and defining the notion of* ***human security****.*
>
> World Summit Outcome, UN General Assembly, 2005

During his tenure as United Nations Secretary-General, Kofi Annan coined the phrase "problems without passports" to capture the increasingly global reach of modern-day problems. The scope of interconnectivity of the world has made the old thinking of state centric approach to security and sovereignty irrelevant at best. This unwitting galvanization of the world has made citizens of the state inadvertently citizens of the world and as such, traditionally national problems global ones. Therefore, notions and views on security should go beyond the protection of state assets and interests to a focus on global security with citizens as objects of security.

2.6.1 Human security in a digital world

Would an alternative approach be required to safeguard human needs in cyberspace? Would such an approach adequately satisfy the needs of humans in the cyber realm? [42] Human security seems to be the answer. The term addresses the humanitarian, economic, and social issues that aim to alleviate human suffering thus ensuring security. In 1994, the United Nations Human Development Report argued that the concept of security has to protect the legitimate concerns of ordinary people.[43]

Human security advocates are criticizing traditional views of international security that are state-oriented and claim that the focus should be on humans. There are two points we need to consider here. First, the traditional and state-centric view of security already embraces the needs of humans. National security by definition includes the protection of a state's territory, sovereignty

and citizens. Therefore, it is not that states do not protect their populations, but rather that the state's security priorities might deemphasize certain human needs. Second, in the absence of global governance, the only actor that has the authority and capability to secure human needs is the state.[44]

Although definitions abound, human security can be approached in a positive and in a negative way. In the latter, human security is perceived as the absence of threats to core human values, whereas in the positive way, it is perceived as the policies and practices that safeguard and empower the people to exercise their human rights freely and secure. It is this positive conception of human security that seems to be undervalued in the current cybersecurity discourse. States seem to view security in negative terms and thus they also view cybersecurity as mainly the absence of cyber threats. According to Kovacs and Hawtin, 'Cyber security policies should not merely play a defensive role, but a facilitating role, by effectively putting the empowerment and well-being of people at their center. What we are aiming for is for people to be able to be *fearless*, as long as they are respecting other people's human rights'.[45] Echoing the above analysis, states must be convinced that citizen should enjoy the benefits of cyberspace and not be the target of cyber surveillance.

From a human-centric perspective, cyber-security should play a facilitating role in the empowerment of human needs in the cyber domain.[46] In such an approach, safeguarding privacy and freedom of expression as well as restricting unjustifiable public-private sharing of data are considered key issues.

The present state-centric approach on cyber-security rests on the notion that state provide its citizens with security. That notion expressed the reality of pre-Internet era. Cyberspace is different to the other physical domains (land, sea, air and space) that states have to safeguard.

Cyberspace is a transnational domain where states are trying to overcome the border paradox and exercise their sovereignty.[47] Currently, there is no human rights regime that can deal with the global flow of data, intellectual property and data protection. Securing the human needs in a domain that blurs the lines between national and international or public and private, are blurred is truly a challenging task.

2.7 The United States Cybersecurity Strategy

United States of America

The United States released the International Strategy for Cyberspace in May 2011, which describes[48] a set of activities across seven interdependent areas, based on a collaborative model involving government, international partners and the private sector. The areas of focus are as follows:

- Economy: Promoting International Standards and Innovative, Open Markets.
- Protecting Our Networks: Enhancing Security, Reliability, and Resiliency.
- Law Enforcement: Extending Collaboration and the Rule of Law.
- Military: Preparing for 21st Century Security Challenges.
- Internet Governance: Promoting Effective and Inclusive Structures.
- International Development: Building Capacity, Security, and Prosperity.
- Internet Freedom: Supporting Fundamental Freedoms and Privacy.

2.8 The Canadian Cybersecurity Strategy

Canada

Canada's cyber security strategy was published in 2010[49] and has three key areas of focus:

- Securing government systems.
- Partnering to secure vital cyber systems outside the federal Government.
- Helping Canadians to be secure online.

The first pillar aims to establish clear roles and responsibilities, to strengthen the security of federal information systems and to enhance cyber security awareness throughout the government. The second pillar covers a number of collaborating initiatives with the provinces and territories and involving the private sector and critical infrastructure sectors. Finally, the third pillar covers combatting cybercrime and protecting Canadian citizens in online environments. Privacy concerns are notably addressed in this third pillar.

2.9 Conclusion

The importance of the cybersecurity issue is due to the vital role cyberspace plays in the activities of states. In the absence on an international agreement to guide state actions within this domain, most states have developed, or are in the process of developing a cybersecurity strategy to engage other actors and mitigate threats in the cyber domain. The question of cyber governance and the approaches to achieving it has complicated the efforts by states to ensure cybersecurity.

ENDNOTES

[1] Schneier, Bruce. "An International Cyberwar Treaty Is The Only Way To Stem The Threat". N.p., 2012. Web. 13 July 2016.

[2] Brito, Jerry, and Tate Watkins. "Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy." *Harv. Nat'l Sec. J.* 3 (2011): 39.

[3] Cavelty, Myriam Dunn. "The militarisation of cyberspace: Why less may be better." *2012 4th International Conference on Cyber Conflict (CYCON 2012)*. IEEE, 2012.

[4] Dunn Cavelty, Myriam. "The militarisation of cyber security as a source of global tension." *STRATEGIC TRENDS ANALYSIS, Zurich, Möckli, Daniel, Wenger, Andreas, eds., Center for Security Studies* (2012).

[5] "ITU Releases 2015 ICT Figures". *Itu.int*. N.p., 2016. Web. 13 July 2016.

[6] "Facebook Users Worldwide 2016". *Statista*. N.p., 2016. Web. 13 July 2016.
[7] Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. *Cyberpower And National Security*. Washington, D C: Center for Technology and National Security Policy, 2009. Print.
[8] Clarke, Richard. "War from cyberspace." *The National Interest* 104 (2009): 31-36; Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy."*Foreign Affairs* 89.5 (2010): 97-108.

[9] Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *ISA Annual Convention, San Diego, CA April*. Vol. 1. 2012.
[10] Clarke, 2009; Lynn, 2010; Clark, Wesley K., and Peter L. Levin. "Securing the information highway: how to enhance the United States' electronic defenses." *Foreign affairs*(2009): 2-10. 9Hughes, Christopher R. "Google and

the great firewall." *Survival* 52.2 (2010): 19-26. It is Lynn (2010) who raises the need for "active" defenses. However, the term is not precisely defined, and its meaning is not entirely clear from the context of the article.

[11] Der Derian, James. "The question of information technology in international relations." *Millennium-Journal of International Studies* 32.3 (2003): 441-456.
[12] Dartnell (2003), In Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *ISA Annual Convention, San Diego, CA April*. Vol. 1. 2012.
[13] The German Cybersecurity Strategy. "Cyber Security Strategy Documents". *CCDCOE*. N.p., 2015. Web. 13 July 2016.

[14] "National Cyber Security Strategies (Ncsss) Map — ENISA". *Enisa.europa.eu*. N.p., 2016. Web. 13 July 2016.

15 http://www.dhs.gov/files/publications/editorial_0329.shtm
[16] http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf 9 Please see the annex for references to EU National Cyber Security Strategies
[17] "National Cyber Security Strategies (Ncsss) Map — ENISA". *Enisa.europa.eu*. N.p., 2016. Web. 13 July 2016.

[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] "National Cyber Security Strategies (Ncsss) Map — ENISA". *Enisa.europa.eu*. N.p., 2016. Web. 13 July 2016.
[23] Ibid.
[24] "DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBER SECURITY IN AFRICA | African Union". *Au.int*. N.p., 2016. Web. 13 July 2016.
[25] Ibid.
[26] H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.
[27] The definition of cyberspace, cyber-attacks and cyber security policies also varies from country to country.
[28] See page 10 of the Slovakian strategy. "Cyber Security Strategy Documents". *CCDCOE*. N.p., 2015. Web. 13 July 2016.

[29] See page 10 of the strategy from the Netherlands. "Cyber Security Strategy Documents". *CCDCOE*. N.p., 2015. Web. 13 July 2016.

[30] See page 8 of the French strategy. Ibid.
[31] See page 4 of the Lithuanian strategy. Ibid.
[32] See page 29 of the strategy from the UK. Ibid.
[33] Ventre, Daniel. "Discourse Regarding China: Cyberspace and Cybersecurity." *Chinese Cybersecurity and Cyberdefense Ventre/Chinese Cybersecurity and Cyberdefense* (2014): 199-282. Web.

[34] "Hayden: Hackers Force Internet Users To Learn Self-Defense". *PBS NewsHour*. N.p., 2011. Web. 13 July 2016.
[35] Goldman, Emily O. "Introduction: Information Resources and Military Performance." *Journal of Strategic Studies* 27.2 (2004): 195-219.
[36] Newmyer, Jacqueline. "The revolution in military affairs with Chinese characteristics." *The Journal of Strategic Studies* 33.4 (2010): 483-504. For a useful summary, see Theodor W. Galdi, *Revolution in Military Affairs?: Competing Concepts, Organizational Responses, Outstanding Issues*, Washington, DC: Congressional Research Service, 1995. Also see John Arquilla and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict" in *In Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds, Santa Monica, CA: RAND, 1995, pp.1-20.

[37] Goldman, Emily O. "Introduction: Information Resources and Military Performance." *Journal of Strategic Studies* 27.2 (2004): 195-219.; Newmyer, Jacqueline. "The revolution in military affairs with Chinese characteristics." *The Journal of Strategic Studies* 33.4 (2010): 483-504.
[38] Krasner 1999, In Bolt, Michael. "The Changing Nature of Sovereignty."

[39] "Great Firewall Of China". *Greatfirewallofchina.org*. N.p., 2016. Web. 13 July 2016.
[40] "Global Issues". *United Nations Foundation*. N.p., 2016. Web. 13 July 2016.
[41] "BBC - Radio 4 - News - United Nations Or Not". *Bbc.co.uk*. N.p., 2003. Web. 13 July 2016.
[42] Cavelty, Myriam Dunn. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Sci Eng Ethics Science and Engineering Ethics* 20.3 (2014): 701-15. Web.

[43] Mordini 2014, 622, In Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach."*ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. Academic Conferences Limited, 2015.
[44] Smith 2010, 42-3, In Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach."*ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. Academic Conferences Limited, 2015.
[45] Kovacs, Anja, and Dixie Hawtin. "Cyber security, cyber surveillance and online human rights." *Stockholm Internet Forum*. 2013.
[46] Cavelty, Myriam Dunn. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Sci Eng Ethics Science and Engineering Ethics* 20.3 (2014): 701-15. Web. ; Kovacs, Anja, and Dixie Hawtin. "Cyber security, cyber surveillance and online human rights." *Stockholm Internet Forum*. 2013.
[47] Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach."*ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*. Academic Conferences Limited, 2015.
[48] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
49http://publications.gc.ca/site/eng/379746/publication.html

CHAPTER THREE

BALANCING NATIONAL SECURITY AND HUMAN SECURITY IN CYBERSPACE

3.1 Introduction

In ensuring cybersecurity, states need to perform a balancing act between national security and our individual liberties. While critical infrastructures continue to be at risk from threats in cyberspace, the human dimension is often ignored, or presented as the source of cyber threats. The focus on state-centric cybersecurity strategies is also not doing much to reduce cyber tensions in the international system

This chapter examines the proposition of a framework which combines the strengths of the national and human security approaches to cybersecurity. It also examines the paradigm shift in strategic thinking about cybersecurity. The chapter finally examines the role of actors in the achievement of the proposed balanced framework.

3.2 National security versus Human security: differences in approach?

For the purpose of this study, I have operationalized the national and human security approaches to cybersecurity as follows:

The national security approach to cybersecurity may be defined as one which is rooted in the notion of cyber-sovereignty, and which requires states to prioritize national security, and the protection of its territory in the form of critical infrastructures, from cyber-attacks. **The human security approach to cybersecurity,** on the other hand, may be defined as a comprehensive approach which recognizes the multiple sources of insecurity to the individual across several dimensions and addresses them accordingly. It works towards protecting the human needs of privacy, human rights and the protection of personal data from cyber-attacks.

Many countries have developed national cybersecurity strategies to secure cyberspace. However, the complex threats that exist in cyberspace require an arsenal of solutions. Cybersecurity has to some extent been dealt with strategically.

In achieving certain national security objectives, individual users, corporations and governments are all opposed to cybercrime. Attribution may be difficult in this virtual environment, but great strides have been made by improving international legal assistance; harmonizing national laws, building up law enforcement capabilities; and working together in public-private partnerships to help address the issue of cybercrime.

Conversely, with issues such as free speech, states have philosophical disagreements about normative behavior. Normative behavior about cybercrime has been partially enforced by the International Convention on Cybercrime enacted in 2001. States have also agreed on normative behavior concerning weapons of mass destruction, nuclear weapons, money laundering, human and drug trafficking amongst other issues. With specific regard to the challenges posed by national operations such as cyber surveillance, espionage and warfare, human security provides a partial solution.

As governments embark on the militarization and balkanization of cyberspace, treating it as a domain for warfare, we have to start thinking about normative behavior. In times of war, we have the Geneva Convention, and it has a doctrine of proportionality. When military objectives are achieved with the action of kinetic attacks, the impact on the civilian population must be considered. The military objective must be so critical that the collateral damage to the civilian population would be deemed acceptable.

3.3 A proposed framework for balancing national security and human security in cyberspace

This study proposes a balanced framework of the national and human security approaches to cybersecurity for states to recognize the impact their actions have on all the actors within the matrix of cyberspace. Such a balance if achieved could have a positive impact on cybersecurity in the state and in the international system.

The basic principles of the balanced framework are listed below:

1. Protection of critical infrastructures to ensure national security
2. Ensuring the free flow of information and civil liberties such as freedom of speech and privacy protection to protect citizens.
3. Improving cyberspace resilience through dynamic response capabilities by employing multiple layers of security.
4. Acting in partnership based on shared responsibilities - where each actor serves its role for mutual cooperation and assistance.

The construction of a resilient cyberspace requires a multi-stakeholder approach usually achieved through public-private partnerships. This goal may be achieved through the development of a vibrant information technology industry, investments in research and development, human resource development, and IT literacy improvement.

The focus on human resource development and literacy improvement is a positive impact of the human security norm. Human resource development would ensure an adequate supply of cybersecurity professionals to advance the cause of cybersecurity.

Literacy improvement increases the literacy in ICTs of the public, so individual users can recognize the risks in cyberspace, and determine its use for their own safety. Additionally, it will promote practical initiatives in elementary and secondary schools such as teaching cybersecurity modules. Finally, it will launch a campaign to increase the cybersecurity awareness of the citizenry.

3.4 A Paradigm shift: From Problem to Solution

This study has identified and discussed implications of the national security approach for human security concerns, and the security of the international system. The focus on the representation of the cybersecurity dilemma as a political problem resulting from the practices of state actors is based on the tendency to resolve the issue in the military rather than the civilian domain.

The problem with the current approaches is that cybersecurity is underproduced, both from a traditional state-focused national security and from a human security perspective. The reason is that the contesting approaches are unable to fully address a multidimensional and multi-faceted security dilemma.

First, cybersecurity is increasingly presented in terms of power-struggles, warfighting, and military action. This is a matter of choice involving state-centric political processes that have produced this particular outcome. The result is not more security, however, but less: states spend more and more money on cyber-defense and likely cyber-offense, which is not leading to more, but less security, as evident by the flood of official documents lamenting the security-deficit. Second, the type of cybersecurity that is produced in the name of national security often ignores the security-needs of the population. Third, extending a notion of national security based on border control and sovereignty to cyberspace will almost inevitably have an impact on civil

liberties, especially on the right to privacy and the freedom of speech. Fourth, cyber exploitation by intelligence agencies linked to the manipulation of vulnerabilities in the Post-Snowden era is directly making cyberspace more insecure.

Kerr argues that, state practices pose the greatest threat to human security, constantly creating more insecurity and in fact hindering the removal of known insecurities.[1] At the same time, a secure, safe, and open cyberspace is not possible without involvement of the state. How, then, can this dilemma be overcome? Since the cybersecurity dilemma extends beyond the state, Booth and Wheeler suggest that solutions are not to be found solely in the cooperation between states.[2] Rather, a focus on areas of commonality for all the stakeholders that are interested in more security is needed.[3]

If we want a secure and resilient cyberspace, then a strategically exploitable cyberspace has to be eroded. This is a compromise that some state actors need to make if they want a type of national security that extends to cyberspace. If such a compromise is not made, then the quest for more national security will always mean less cybersecurity, which will always mean less national security because of vulnerabilities in critical infrastructures. Dynes et al. opine that the reason why vulnerabilities persist the current incentive structures in cyberspace are skewed towards cyber offence.[4] Kuehn emphasizes the need for states to help improve cybersecurity through additional regulation to water down the incentives for cyber offensive capabilities.[5]

3.5 The Roles of Actors

States have four distinct roles in cyberspace. First, states use cyberspace for socio-economic, political and diplomatic purposes. Second, states are mandated to protect the global infrastructure of the internet. From military installations to computer based healthcare, energy, transport and

financial network systems, governments are now concerned with what is called *Critical Infrastructure Protection*. Critical Infrastructure Protection refers to the protection of the physical components of cyberspace – the routers, switches, fibre optics, embedded processors, computer networks and information systems. Third, states are exploiters of cyberspace. They embark on mass surveillance actions in the name of national security and counterterrorism. Governments engage in economic espionage before trade negotiations to help domestic industries, before they commit to a trade pact. Finally, states need access to data to fulfil their public safety and national security mission. Their citizens expect them to investigate crimes, stop terrorist attacks and embark on activities that are consistent with that mission.

In the proposed framework, the state is responsible for diplomacy, defence and crime countermeasures in cyberspace, and must work toward increasing cyber confidence through the respect of civil liberties.

Critical infrastructure providers must ensure cybersecurity across various sectors. With collaboration through private-public partnerships, critical information infrastructures would be less vulnerable as Cyber Security Emergency Response Teams (CSERTs) would be better equipped to respond to threats.

Private corporations, educational and research institutions must encourage dialogue to promote information sharing and human resource development through industry-academia partnerships.

Individual users must adopt measures such as IT literacy improvement and information sharing to better recognize cyber risks when they encounter them.

3.6 A Comparative Analysis of the United States and Canadian Cybersecurity Strategies.

Cybersecurity policies are not only implemented by government agencies but by private enterprises, internet providers, and NGOs. This study will focus on state initiatives. It is a comparison between the United States and Canada's cybersecurity policies.

The methodology employed in the analysis identifies the areas of effort, and brings out the list of institutions concerned with the implementation of the cybersecurity policy, the legislative framework supporting this action and the impact such measures have on critical infrastructure protection and human security.

In the study both countries have one basic instrument called cybersecurity strategy, but it is worth noting that measures of cybersecurity go much beyond these plans.

3.6.1 Areas of effort

An analysis of the cybersecurity strategies (CSS) of the United States and Canada with the proposed framework yielded the following results.

Cybersecurity Strategies (CSS)

First, on the principle of *protecting critical infrastructures,* the United States CSS supports this principle with the second and fourth pillars of its strategy - *Protecting Our Networks: Enhancing Security, Reliability, and Resiliency*, and *Military: Preparing for 21st Century Security Challenges.* The Canadian CSS also upholds this principle with its first and second pillars - *Securing government systems,* and *Partnering to secure vital cyber systems outside the federal Government.*

Furthermore, on the principle of ensuring *the free flow of information* and the *protection of civil liberties* with the first, third and seventh pillars of its strategy. The first pillar which tackles the economy, promotes the development of a vibrant IT industry while the third pillar of *Law Enforcement: Extending Collaboration and the Rule of Law* facilitates the prosecution of malevolent actors. The seventh pillar, *Internet Freedom: Supporting Fundamental Freedoms and Privacy*, promotes the protection of civil liberties such as public privacy and freedom of expression. The Canadian CSS also upholds this principle with third pillar - *Helping Canadians to be secure online*.

Finally, the principles of *cyber resilience* and *acting in partnership based on shared responsibilities* are inextricably linked due to the collaborative actions of public-private partnerships between the state, critical infrastructure providers and the private sector.

Cybersecurity Institutions

Canada

In the federal level, the organ responsible to coordinate the implementation of the Strategy is *Public Safety Canada*, already responsible for the coordination of Canada's national security and public safety. Public Safety Canada has a specific department created to deal with cybersecurity - the Canadian Cyber Incident Response (CCIR). Two other agencies from Public Safety Canada that work in close relation to CCIR are the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).[6]

Public Safety Canada hosts the Government Operations Centre (GOC), which provides response by monitoring and reporting round-the-clock events of national interest. CCIR is actually a department within GOC. While GOC is focused on response to any critical infrastructure and

strategic-level hazardous event, CCIR is exclusively focused on response to cyber-related incidents.[7]

Independent ministries closely working with cybersecurity and vital to the implementation of Canada's Cybersecurity Strategy are the Treasury Board of Canada, the Department of Justice and the Foreign Affairs and International Trade.[8]

Canadian cybersecurity strategy is more concerned with the protection of the privacy of its citizens. This is evident in Canada reposing the responsibility of cybersecurity to state agencies that are taxed to protect Canadians online. On the other hand, agencies in the United States responsible for cybersecurity are traditionally entities taxed to protect critical national assets. Provincial and territorial agencies respond to the federal Office of the Privacy Commissioner of Canada (OPCC), which reports directly to the Parliament. The Commissioner supervises compliance and pursues court action under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the *Freedom of Information and Protection of Privacy Act* (Privacy Act).[9]

Two other guiding policies around which the Canadian CSS is built *is the protection of government systems* and *government's assistance to help Canadians to be secure online.* As part of this last goal, the government sponsors a website managed by Public Safety Canada to educate Canadians and to spur national public awareness on cyber threats.[10] It departs from the principle that when Canadians strengthen their own cybersecurity they contribute to strengthening Canada's cybersecurity as a whole.

An important institution that collects and disseminates information on mass-marketing fraud (telemarketing), advanced-fee fraud letters (Nigerian 419 letters), identity theft and internet fraud

in general is the Canadian Anti-Fraud Centre, which receives complaints of Canadians and American consumers and victims.

United States

In the United States, the main executive forum to consider matters of national security and foreign policy is the *National Security Council (NSC).* The forum helps the President on coordinating policies among various governmental agencies and is permanently attended by the vice-President, the Secretary of State, the Secretary of Treasury, the Chairman of the Joint Chief of Staffs (military representative), the Director of National Intelligence, the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Chief of Staff to the President and the Counsel to the President. When appropriate, the Director of the Office of Management and Budget, the Attorney General as well as senior officials and heads of other executive departments and agencies are invited to attend the meetings.[11]

Each institution, individually, has an important and well-defined role in matters of national security in general. Clearer responsibilities for the specific issue of cybersecurity was only attributed in the current Obama administration. During the two precedent administrations (G. W. Bush and Clinton), cybersecurity responsibilities were blurred, with limited leadership and dissolution between the White House, the Homeland Security, the Department of Defence and individual agencies. The issue of cybersecurity was treated as a sub-item inside policies for critical infrastructure protection.[12]

In 2009, a *Cybersecurity Office* was created inside the National Security Council and the President has appointed a US Cybersecurity Coordinator. The regular access to the President provided to the US Cybersecurity Coordinator shows that the protection of cyberspace

infrastructure became a main item and a national security priority. The Cybersecurity Office has the responsibility to orchestrate and to integrate all cybersecurity policies for the government, to work close to the Office of Management and Budget, to ensure that the Office's budget reflect its priorities and to coordinate the response in the event of cyber incident or attack.[13]

The United States *Computer Emergency Response Team* (US-CERT) is an arm of the Department of Homeland Cyber Security Division and a round-the-clock technical operator. It provides technical assistance to information systems operators and disseminates timely notifications regarding current and potential security threats and vulnerabilities. It partners with critical infrastructure operators and owners, academia, federal, state and local agencies, domestic and international organizations.[14]

Federal agencies work together in collaboration for research and development of areas of information technology like computing, networking and software. Their cooperation is called the *Networking and Information Technology Research and Development* (NITRD) programme. Inside NITRD, the *Cyber Security and Information Assurance* (CSIA) *Interagency Working Group* coordinates research and development "*to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems*".[15]

3.7 Conclusion

The cybersecurity dilemma is one of grave importance and deserves the full attention of the international community. Cyberspace is full of conundrums, and there is very difficult problem of balancing competing interests. States do want to secure cyberspace, however, they want to exploit it. They want to use it for military purposes as a force multiplier; they think about it as a

domain of warfare, and how to deal with the enemy in a cyber-enabled battlefield, but they are having conflicting priorities. However, it is not just governments that have conflicting interests, individual users do too. Citizens want their digital privacy protected, and yet want to be protected from terrorism simultaneously without giving up their data.

The challenge here is, amidst competing interests, how do we conceptualize cybersecurity for the benefit of all: for individual members of the society, for the cyber industry, and for states who are traditionally the sole purveyors of security? A framework that balances the strength of both approaches offers a practical solution in changing the focus of cyber command centres and reducing cyber tensions within the comity of nations.

ENDNOTES

[1] Pauline Kerr, In Collins, Alan. *Contemporary security studies*. Oxford university press, 2016.
[2] Booth, Ken, and Nicholas Wheeler. "The Security Dilemma." *Fear, Cooperation and Trust in World Politics, Basingstoke and New York: Palgrave Macmillan* (2008).
[3] Booth, Ken, and Nicholas J. Wheeler. "Rethinking the Security Dilemma."*unpublished paper, Aberystwyth University, Aberystwith, UK* (2008).
[4] Dynes et al. In Adams Jr, John A. *Cyber Blackout: When the Lights Go Out--Nation at Risk*. FriesenPress, 2015.
[5] Kuehn 2012, In Cruz-Cunha, Maria Manuela, ed. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. IGI Global, 2014.
[6] Belisario, Juliana. "U.S. and Canada: A Comparison on Cybersecurity Policies." (2012): n. pag. Web
[7] Ibid.
[8] Ibid.
[9] "The Commissioner works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector." Available at: http://www.priv.gc.ca/auans/mm_e.asp
[10] Available at: http://www.getcybersafe.gc.ca/index-eng.aspx In the website, the user can be informed of risks and have tips to protect various electronic devices. He can either share his story of identity theft, online scam, virus, computer invasion by hacking, as well as to read and to get aware of current threats with the stories of other users.
[11] Belisario, Juliana. "U.S. and Canada: A Comparison on Cybersecurity Policies." (2012): n. pag. Web
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Available at: http://www.nitrd.gov/subcommittee/csiaiwg.aspx

CHAPTER FOUR

SUMMARY OF FINDINGS, CONCLUSIONS & RECOMMENDATIONS

4.1 Introduction

This chapter presents the summary of findings in the study and conclusions. It also proffers some recommendations for policy makers.

4.2 Summary of findings

The study set out, among other things to examine the current state approaches to addressing the cybersecurity dilemma, evaluate the impact of national security policies on human security in cyberspace and to determine if a balance between national security and human security approaches can provide the best framework for states to address national issues in cyberspace.

A new framework balancing the national security and human security approaches is needed to guide state actions in cyberspace. The national security approach, which is the dominant state-centric model employed in national cybersecurity strategies is inadequate for addressing some unique challenges cyberspace presents. It is rather responsible for the escalation of cyber fears within the international system, and the establishment of cyber commands to consolidate power in cyberspace. It is worthy of note, however, that the focus on critical information infrastructure protection does engender some level of security for both the state and its citizenry. It reduces the vulnerability of vital networks and information services to large-scale disruptions. The human security approach is not wholly adequate either. In order to facilitate the detection and prosecution of malevolent actors, citizens must be prepared to sacrifice to some extent public privacy and some civil liberties. A new framework balancing the contesting approaches is therefore imperative in ensuring security in cyberspace.

In the absence of an international agreement governing cyberspace, states are divided in their understandings of what kind of security is needed in the cyber domain. While several regional agreements offer some guidelines on the conduct of states within this domain, pertinent issues such as differences in the definition of key concepts, and the operationalization of the cyber environment still exist. Consequently, the cybersecurity issue is addressed from a civilian or military perspective depending on its designation by state policy.

A critical analysis of the cybersecurity strategies of the United States and Canada revealed that both states support the principles of the new framework in their policy documents. These principles are concerned with the protection of critical infrastructures, ensuring the free flow of information, the protection of civil liberties, building a resilient cyberspace, and multi-stakeholder approach based on shared responsibilities.

However, the case studies revealed a difference in the understandings of what is meant by critical infrastructure protection. In the Canadian CSS, critical infrastructure protection refers to the protection of critical information infrastructure to safeguard sensitive and confidential government systems and personal information of citizens to ensure their safety online. In the United States CSS, however, critical infrastructure protection extends to networked infrastructure – critical life-sustaining infrastructures that provide utility services, control transport systems and support financial systems which are all networked in cyberspace. The difference in these understandings is clearly seen in the institutions mandated to provide this protection. Whereas the Canadian institutions charged with this task are civilian in nature, the United States has charged its military to 'defend against disruptions' against its digital infrastructures.

The emergence of cyber commands has added an additional layer of insecurity. The United States promotes the doctrine of 'active defense' to dissuade and deter malevolent actors. Under this doctrine, it clearly states that:

> "The United States will, along with other nations, … oppose those who would seek to disrupt networks and systems, thereby dissuading and deterring malicious actors, while reserving the right to defend these vital national assets as necessary and appropriate. …When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country".

The paradigm shift of the cybersecurity issue from a civilian to a military domain has created unease in the international system, escalated cyber fears and fueled the drive for cyber commands with cyber offensive capabilities to enforce deterrence in cyberspace.

4.3 Conclusions

Current national approaches to addressing the cybersecurity challenge are fraught with challenges. Hence, it is imperative to adopt a more balanced, comprehensive and inclusive framework that combines the strengths of the national security and human security approaches to securing cyberspace. Such an approach would align the needs of the actors involved in ensuring cybersecurity, while removing the vulnerabilities usually exploited by malevolent state or non-state actors.

The human dimension of cybersecurity is so crucial that it cannot be ignored. While the individual may be presented as a threat actor – the disgruntled government agent, the hacktivist, the cybercriminal or the terrorist – humans are also a state's greatest resource in ensuring cybersecurity. Through building human capacity, a state can nurture a populace who have high

levels of cyber awareness and can easily recognize cyber threats. It would also contribute to a thriving IT industry and a formidable cyber workforce.

States are covertly developing their cyber offensive capabilities. The development of these capabilities has taken institutional forms, usually as specialized cyber units within a state's armed forces. In some states, the function of these cyber commands has been specified, while in others they are almost indistinguishable from normal military operations. This trend has led to an attempt to militarize cyberspace by adopting the military doctrine of deterrence when such technologies have not yet been developed. Computer network breaches cannot be categorized as a denial-of-service attack or espionage until an intrusion has been detected. There should therefore be a push to transform cyber capabilities into more resilient networks and defensive shields to ease tensions and resolve the cybersecurity dilemma.

As Lewis posits, "because of the newness of technology, lack of agreement on norms, and the potential to mistake cyber espionage for military action, cyber competition can increase risks of miscalculation, conflict and escalation during wider interstate tension".[1] The study confirms the hypothesis that balancing national security and human security needs in cyberspace would markedly improve cybersecurity.

Finally, the difference in regional approaches to cybersecurity demonstrates the divergence in the understandings of the threats in cyberspace and the measures to counter them. What is a civilian issue in Europe falls within the military domain in the United States. The institutions responsible for implementing cybersecurity strategies, and the funding they have access to also reveals the areas of focus states prioritize when addressing the cybersecurity challenge. In Africa, threats to cybersecurity are presented primarily as cybercrime, just as in most European states. These differences should be resolved in an international agreement which promotes shared

understandings of key cybersecurity issues through cyber diplomacy, the institutionalization of normative behaviour and international partnerships to guarantee collective security.

4.4 Recommendations

The current cybersecurity dilemma represents one of the gravest threats cyberspace poses to the state and international security. In the light of current events, states may opt to build more cyber commands with a singular intent of purpose – deterrence.

A comprehensive cybersecurity framework that balances the national and human security approaches to cybersecurity offers a practical solution to addressing the cybersecurity dilemma. Such an approach would, among other things:

a. Change cyber metaphors to shape national cybersecurity policies. These metaphors guide how states approach cybersecurity. Metaphors such as deterrence should be changed in cyber policies because there is a tendency that states may focus on offence dominant technology to achieve such capabilities.
b. Promote shared understandings of key cybersecurity issues, and increase the prospects of an international agreement to govern cyberspace.
c. Promote the protection of public privacy and civil liberties such as freedom of expression within the cyber domain. This policy initiative is critical to improving cyber confidence in state actions in the Post-Snowden era.
d. Build human capacity to detect and mitigate cyber risks in a more digitally aware populace.

e. Ensure collaboration between state institutions, critical infrastructure providers, and the private sector through public-private partnerships to enhance cybersecurity at multiple levels of cyberspace operations.

ENDNOTES

[1] Lewis, James. *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*. Center for Strategic and International Studies, 2013.

BIBLIOGRAPHY

A. BOOKS

Alan. Contemporary security studies. Oxford university press, 2016.

Booth, Ken, and Nicholas Wheeler. "The Security Dilemma." Fear, Cooperation and Trust in World Politics, Basingstoke and New York: Palgrave Macmillan (2008).

Booth, Ken, and Nicholas J. Wheeler. "Rethinking the Security Dilemma."unpublished paper, Aberystwyth University, Aberystwith, UK (2008).

Bush, George HW, and Brent Scowcroft. A world transformed. Vintage, 2011.

Carlsnaes, Walter, et al., eds. Handbook of international relations. Sage, 2002.

Choucri, Nazli. Cyberpolitics in International Relations. MIT Press, 2012.

Dynes et al. In Adams Jr, John A. Cyber Blackout: When the Lights Go Out--Nation at Risk. FriesenPress, 2015.

Gibson, William. "Neuromancer New York." Ace 9 (1984).

Griffiths, Martin, Steven C. Roach, and M. Scott Solomon. Fifty key thinkers in international relations. Routledge, 2008.

Kanji, O. 2003. 'Security' in Burgess, G. and H. Burgess (eds.). Beyond Intractability. Conflict Research Consortium, University of Colorado.

Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. Cyberpower And National Security. Washington, D C: Center for Technology and National Security Policy, 2009. Print.

Krasner 1999, In Bolt, Michael. "The Changing Nature of Sovereignty."

Kreuzer, Michael P. Drones and the Future of Air Warfare: The Evolution of Remotely Piloted Aircraft. Routledge, 2016.

Kuehl, Daniel T. "From cyberspace to cyberpower: Defining the problem. "Cyberpower and national security (2009): 26-28. In Kramer, Franklin D, Stuart H Starr, and Larry K Wentz.

Cyberpower And National Security. Washington, D C: Center for Technology and National Security Policy, 2009. Print.

MacFarlane, S. N. and Y. F. Khong (2006) Human Security and the UN: A Critical History, Indianapolis: Indiana University Press.

Miller, Frederic P., Agnes F. Vandome, and McBrewster John. Constructivism In International Relations. VDM Publishing, 2010. Print.

Newall, Diana, ed. Fifty Key Thinkers in International Relations. Routledge, 2012.

Reveron, Derek S., and Kathleen Mahoney-Norris. Human security in a borderless world. Westview Press, 2011.

Saler, Michael. "THE DARK NET Inside the digital underworld." (2015): 3-5.

Schnurr, Matthew A and Larry A Swatuk. Natural Resources And Social Conflict. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2012. Print.

Sherwood-Randall, Elizabeth. Alliances and American National Security. Maroon Ebooks, 2015

Kuehn 2012, In Cruz-Cunha, Maria Manuela, ed. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. IGI Global, 2014.

B. JOURNAL ARTICLES

Anderson, Charletta. "Cyber Security and the Need for International Governance." Available at SSRN 2769579 (2016).

Atanassova-Cornelis, Elena. "Japan and the 'Human Security' Debate: History, Norms and Pro-active Foreign Policy." Graduate Journal of Asia-Pacific Studies 3.2 (2005): 58-74.

Bashow, D. "Canadian Military Journal Vol. 12, No. 3". Journal.forces.gc.ca. N.p., 2011. Web. 12 July 2016.

Belisario, Juliana. "U.S. and Canada: A Comparison on Cybersecurity Policies." (2012): n. pag. Web

Betz, David, and Tim Stevens. Cyberspace and the State: Toward a Strategy for Cyber-power. IISS-The International Institute for Strategic Studies, 2011.

Brito, Jerry, and Tate Watkins. "Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy." Harv. Nat'l Sec. J. 3 (2011): 39.

Cavelty, Myriam Dunn. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." Science and engineering ethics 20.3 (2014): 701-715.

Cavelty, Myriam Dunn. "The militarisation of cyberspace: Why less may be better." 2012 4th International Conference on Cyber Conflict (CYCON 2012). IEEE, 2012.

Chandler, David (2008) 'Human Security: The Dog That Didn't Bark', Security Dialogue, 39(4), pp. 427-439.

Choucri, Nazli, and Daniel Goldsmith. "Lost in cyberspace: Harnessing the Internet, international relations, and global security." Bulletin of the Atomic Scientists 68.2 (2012): 70-77.

Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012).

Clarke, Richard. "War from cyberspace." The National Interest 104 (2009): 31-36

Clark, Wesley K., and Peter L. Levin. "Securing the information highway: how to enhance the United States' electronic defenses." Foreign affairs (2009): 2-10.

Clemente, Dave. Cyber Security and Global Interdependence: What Is Critical?. Chatham House, Royal Institute of International Affairs, 2013.

"Cyber Power In The Changing Middle East - Turkish Policy Quarterly". Turkish Policy Quarterly. N.p., 2016. Web. 12 July 2016.

Dartnell (2003), In Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." ISA Annual Convention, San Diego, CA April. Vol. 1. 2012.

Deibert, Ronald, et al. Access denied: The practice and policy of global internet filtering. MIT Press, 2008.

Der Derian, James. "The question of information technology in international relations." Millennium-Journal of International Studies 32.3 (2003): 441-456.

Dunn Cavelty, Myriam. "The militarisation of cyber security as a source of global tension." STRATEGIC TRENDS ANALYSIS, Zurich, Möckli, Daniel, Wenger, Andreas, eds., Center for Security Studies (2012).

Eriksson, Johan & Guacamole, Giampiero. "The Information Revolution, Security, and International Relations". International Political Science Review Vol. 27, No. 3 (Jul., 2006), pp. 221-244

Finnemore, Martha, and Kathryn Sikkink. "Taking stock: the constructivist research program in international relations and comparative politics." Annual review of political science 4.1 (2001): 391-416.

"Four Quadrants - Identifying Difficult Problems In Cyber law". Cyber.law.harvard.edu. N.p., 2011. Web. 12 July 2016.

Froomkin, A. Michael. "Toward a critical theory of cyberspace." Harvard Law Review (2003): 749-873.

Gash Jim. Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits. Canadian Military Journal, Issue 12, No 3, 2012.

Goldman, Emily O. "Introduction: Information Resources and Military Performance." Journal of Strategic Studies 27.2 (2004): 195-219

Gvosdev, Nicholas K. "" The Bear Goes Digital: Russia and Its Cyber Capabilities." Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. Washington DC: Georgetown University Press (2012).

H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.

Hughes, Rex. "A treaty for cyberspace." International Affairs 86.2 (2010): 523-541.

Hughes, Christopher R. "Google and the great firewall." Survival 52.2 (2010): 19-26.

Kuehl, Daniel T. "From cyberspace to cyberpower: Defining the problem. "Cyberpower and national security (2009): 26-28.

Kukla, A. Social Constructivism And The Philosophy Of Science. New York: Routledge, 2000. Print.

Kwalwasser, Harold. "Internet governance." Cyberpower and national security 510 (2009).

Lessig, Lawrence. "The zones of cyberspace." Stanford law review (1996): 1403-1411.

Lewis, James. Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia. Center for Strategic and International Studies, 2013.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy."Foreign Affairs 89.5 (2010): 97-108.

Madden, M. "Public Perceptions of Privacy and Security in the Post-Snowden Era." Pew Research Internet Project (2014).

Madrueño-Aguilar, Rogelio. "Human Security and the New Global Threats: Discourse, Taxonomy and Implications." Global Policy (2016).

Martin, Mary and Taylor Owen (2010) 'The Second Generation of Human Security: Lessons from the UN and EU Experience', International Affairs,86(1), pp. 211–224.

Maurer, Tim. "Cyber norm emergence at the United Nations." Science, Technology, and Public Policy Program (2011).

McCaffery, Larry, and William Gibson. "An Interview with William Gibson. "Mississippi Review (1988): 217-236.

McDonald, Matt. "Human security and the construction of security." Global Society 16.3 (2002): 277-295

Mihr, Anja. "Public Privacy Human Rights In Cyberspace." (2013).

Newman, Edward. "Human security and constructivism." International studies perspectives 2.3 (2001): 239-251.

Newmyer, Jacqueline. "The revolution in military affairs with Chinese characteristics." The Journal of Strategic Studies 33.4 (2010): 483-504.

Petallides, Constantine J. "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." Student Pulse4.03 (2012).

Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." ISA Annual Convention, San Diego, CA April. Vol. 1. 2012.

Rid, Thomas. "Cyber war will not take place." Journal of strategic studies35.1 (2012): 5-32.

Rohret, David, and Michael Kraft. "Catch me if you can: Cyber Anonymity." The Proceedings of the 6th International Conference on Information Warfare and Security. 2011.

Schneier, Bruce. "An International Cyberwar Treaty Is The Only Way To Stem The Threat". N.p., 2012. Web. 13 July 2016.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." Journal of Military Studies 4.1 (2013).

Theodor W. Galdi, Revolution in Military Affairs?: Competing Concepts, Organizational Responses, Outstanding Issues, Washington, DC: Congressional Research Service, 1995.

Wendt, Alexander. "Anarchy is what states make of it: the social construction of power politics." International organization 46.02 (1992): 391-425.

Ventre, Daniel. "Discourse Regarding China: Cyberspace and Cybersecurity."Chinese Cybersecurity and Cyberdefense (2014): 199-282. Web.

C. REPORTS

"Cybersecurity". ITU. N.p., 2016. Web. 12 July 2016.

John Arquilla and David Ronfeldt, "A New Epoch – and Spectrum – of Conflict" in In Athena's Camp: Preparing for Conflict in the Information Age, John Arquilla and David Ronfeldt, eds, Santa Monica, CA: RAND, 1995, pp.1-20.

Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach."ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015. Academic Conferences Limited, 2015.

Kovacs, Anja, and Dixie Hawtin. "Cyber security, cyber surveillance and online human rights." Stockholm Internet Forum. 2013.

D. WEBSITES

"BBC - Radio 4 - News - United Nations Or Not". Bbc.co.uk. N.p., 2003. Web. 13 July 2016.

"Cyber Attacks Statistics – HACKMAGEDDON". Hackmageddon.com. N.p., 2016. Web. 13 July 2016.

"Cyber Security Strategy Documents". CCDCOE. N.p., 2015. Web. 13 July 2016.

"DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBER SECURITY IN AFRICA | African Union". Au.int. N.p., 2016. Web. 13 July 2016.

"Facebook Users Worldwide 2016". Statista. N.p., 2016. Web. 13 July 2016.

"Hayden: Hackers Force Internet Users To Learn Self-Defense". PBS NewsHour. N.p., 2011. Web. 13 July 2016."Great Firewall Of China". Greatfirewallofchina.org. N.p., 2016. Web. 13 July 2016.

"Global Issues". United Nations Foundation. N.p., 2016. Web. 13 July 2016.

http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf 9 Please see the annex for references to EU National Cyber Security Strategies

http://www.dhs.gov/files/publications/editorial_0329.shtm

http://www.getcybersafe.gc.ca/index-eng.aspx

https://iversity.org/en/my/courses/public-privacy-cyber-security-and-human-rights/lesson_units/4394

http://www.nitrd.gov/subcommittee/csiaiwg.aspx

http://www.priv.gc.ca/auans/mm_e.asp

http://publications.gc.ca/site/eng/379746/publication.html

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

InfoSec Institute,. 'China Vs. US, Cyber Superpowers Compared - Infosec Institute'. N.p., 2013. Web. 4 June 2015.

"ITU Releases 2015 ICT Figures". Itu.int. N.p., 2016. Web. 13 July 2016.

"National Cyber Security Strategies (Ncsss) Map — ENISA". Enisa.europa.eu. N.p., 2016. Web. 13 July 2016.

"U.S. Air Force - Mission". Airforce.com. N.p., 2016. Web. 12 July 2016. https://www.airforce.com/mission