People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mostéfa Benboulaïd, Batna-2 University
Faculty of Letters and Foreign Languages
Department of English Language and Literature

Rethinking US National Security Policy in the 21ST Century and its Impact on International Educational Policy Decision

Thesis Submitted for the Degree of "Doctorat Es-Science" in American Civilization

Presented by
GOUDJIL Kahina

Supervised by
Prof. ABOUBOU Hachemi
Co-supervised by
Prof. Alison J. BRUEY

Board of Examiners:

President:	Prof. Amor GHOUAR	Mostéfa Benboulaïd, Batna-2 University
Supervisor	Prof. Hachemi ABOUBOU	Mostéfa Benboulaïd, Batna-2 University
Co-Supervisor:	Prof. Alison J. BRUEY	University of North Florida UNF
Examiner:	Prof. Abdelhak ELAGGOUNE	University of 8 May 1945 / Guelma
Examiner:	Dr. Houda BOUHIDEL	Mostéfa Benboulaïd, Batna-2 University
Examiner:	Dr. Samih AZOUI	Teaching Training School/ Constantine

April 2023

Dedication

To the memory of my Father, May Allah rest his soul.

Acknowledgments

First and foremost, alhamdulillah for blessing me with his guidance and mercy to finish this research.

Second and most importantly, I acknowledge my thanks to many people in my life who Cheered and inspired me to finalize this work. To my family members who have always supported me throughout my whole career, to my husband Mohamed Bouchikhi who stood by my side to finish my thesis. To all my friends who were a source of energy to me.

Next, It is more than being grateful and eternally indebted to some people; to whom I could not have completed this thesis without their guidance, help, and inspiration, to my supervisor ***Pr. Hachemi Aboubou*** and my Co-supervisor ***Pr.Alison J.Bruey;*** their constructive critique and unconditional support made me rise with my thoughts to meet their expectations. No less recognition and gratitude to the honorable examiners who read and corrected my work.

Lastly, and to whom I could not have completed this thesis without their help and guidance, especially during my stay in the USA. To Lila Tahar a friend and a sister. To ***Dr. Abdel-kader Haiereche,*** Chief Political Affairs at the United Nations. To ***Dr. Lakhder Boukerrou Lakhder,*** Director of International Programs and Global Initiative. To ***Pr. Azzeddine Layachi,*** Associate Professor in Political Science at St. John's University. To the staff of the Department of History in the University of Florida UNF, to the Housing Services Staff, at UNF, who welcomed me, hosted me, and kept me safe and healthy during the pandemic, grateful to all of you at UNF and grateful to Alison Bruey and ***Ruth Lopez*** who was always there for me. With no less recognition, I would love to thank all the English Department staff at Batna University 2 for their help, assistance, and support. Thank you all.

Abstract

This thesis aims to study the progressive development of U.S. National security since 1940, and the prominent threat that comprises its national security policy in the twenty-first century. This work is devoted to diagnosing the U.S. national security development, new tactics and policies, the primary initiatives employed to handle the problem of a new emerging threat of cybersecurity, and its consequences on American national policy. The type of this research is an Exploratory Descriptive Qualitative research EDQ, it examines the advent of a new field of Cyber security as the rising danger to national and international security. It investigates the relationship between agencies and the educational system to mitigate the threat. To analyze and evaluate education's role in creating a cybersecurity workforce to overcome U.S. national security threats, a comprehensive statistical analysis was conducted to determine the effectiveness of higher education in addressing the shortage of skilled workers in cybersecurity, and the extent to which it has reduced U.S. vulnerabilities to cybercrimes. The work will demonstrate if expanding cybersecurity in higher education has contributed to developing a pipeline of human cybersecurity capital. Despite the efforts that programs in higher education have made, the study's findings show that the United States is still susceptible and vulnerable to cybercrime. Higher education has helped offset the problem of labor shortage, but it has not been enough to eradicate or diminish the country's cyber risks. As the results illustrate, higher education played and still plays a crucial role in bridging the skills gap in the cybersecurity sector, but it could not address the country's cyber risks and diminish the country's vulnerability to cyberattacks.

Keywords: National Security, Cyber Security, Threat-Higher Education, Cybercrimes, Policy.

Résumé

Cette thèse vise à étudier le développement progressif de la sécurité nationale américaine depuis 1940, ainsi que du majeur danger qui menace sa politique de sécurité nationale au XXIe siècle. Ce travail est, en premier lieu, un diagnostic du développement de la sécurité nationale des États-Unis, de ses nouvelles tactiques et politiques ainsi que des initiatives recourues pour traiter le problème d'une imminente menace émergente qu'est la cybersécurité et ses conséquences sur la politique nationale américaine. Cette recherche est une analyse Qualitative Descriptive Exploratrice : EDQ. Cette dernière examine l'avènement du domaine de la cybersécurité comme étant un danger croissant pour la sécurité nationale et internationale américaine. Elle étudie la relation entre les agences et le système éducatif pour atténuer cette menace. Pour cela, elle analyse et évalue le rôle de l'éducation dans l'apprentissage d'une main-d'œuvre spécialisée en cybersécurité afin de surmonter les menaces contre la sécurité nationale des États-Unis, une analyse statistique complète a été menée pour déterminer l'efficacité de l'enseignement supérieur à minimiser la pénurie de travailleurs qualifiés en cybersécurité. Ce travail démontre que l'expansion de la cybersécurité dans l'enseignement supérieur a contribué au développement d'un capital humain important dans le domaine de la cybersécurité. Toutefois et nonobstant les efforts déployés par les programmes d'enseignement supérieur, les résultats de l'étude montrent que les États-Unis est toujours vulnérable face à la cybercriminalité. L'enseignement supérieur a contribué à atténuer la pénurie de main-d'œuvre spécialisée, mais il n'a pas été suffisant pour éradiquer les cyber-risques contre le pays. Les résultats, l'enseignement supérieur a joué et joue toujours un rôle crucial pour combler le déficit de compétences de la cybersécurité, cependant il n'a pas pu réduire la vulnérabilité des Etats-Unis contre les cyberattaques.

Mots clés : Sécurité nationale- Cybersécurité-Menace-Enseignement supérieur-Cybercriminalité.

ملخص

تعالج هذه الأطروحة قضية أساسية وراهنة، تتمثل في التغيرات التي تمس سياسة الأمن القومي للولايات المتحدة الأمريكية وتأثيراتها منذ عام 1940، والتهديدات التي يتعرض لها الأمن القومي للولايات المتحدة في القرن الحادي والعشرين. تم تخصيص هذا العمل لتشخيص تطور الأمن القومي للولايات المتحدة، الاستراتيجيات السياسات الجديدة، والمبادرات الأولية للتصدي لتهديدات الأمن السيبراني الناشئة وانعكاساتها على السياسة الوطنية للولايات المتحدة. هذه الدراسة هو بحث استكشافي وصفي نوعي EDQ، والذي يدرس التهديد المتزايد للأمن الوطني والدولي الناشئ عن ظهور مجالات جديدة للأمن السيبراني. تم إجراء تحليل إحصائي شامل لتحديد مدى فاعلية التعليم العالي في معالجة النقص في مجال الأمن السيبراني ومدى انخفاض الجرائم الإلكترونية, ولأن النقص المهني في الأمن السيبراني يمثل تهديدًا كبيرًا للأمن القومي الأمريكي؛ نفذت الحكومة مبادرات واستراتيجيات جديدة لتوسيع تعليم الأمن السيبراني وإنشاء شبكة للقوى العاملة المهنية في مجال الأمن السيبراني وهذا بالتنسيق مع الوكالات الفيدرالية في البلد، من أجل الحد من ضعف الولايات المتحدة في الفضاء الإلكتروني، وعليه يبحث هذا العمل في دور ومشاركة مؤسسات التعليم العالي والمؤسسات الحكومية في تعزيز برامج الأمن السيبراني، فضلاً عن تطوير اليد العاملة البشرية المتخصصة، والاستفادة من الخبراء في مجال الأمن السيبراني من خلال تجديد مسارات تعليمية جديدة في التعليم العالي، وفي الأخير خلصت نتائج هذا البحث إلى خلاصة مفادها: أنه على الرغم من أن برامج التعليم العالي ساهمت ووفرت مزيدا من القوى العاملة في مجال الأمن السيبراني ، إلا أنها لم تستطع التغلب على الجرائم الإلكترونية.

الكلمات المفتاحية: الأمن القومي، الأمن السيبراني، التهديد التعليم العالي، الجرائم الإلكترونية، السياسة.

List of Tables

List of Figures

List of Abbreviations and Acronyms

AI	Artificial Intelligence
BLS	Bureau of Labor Statistics
BRICS	Brazil – Russia – India – China –South Africa
CAE	Centers of Academic Excellence
CAE-CDE	Center of Academic Excellence in Cyber Defense Education
CAE-CO	Center of Academic Excellence in Cyber Operations
CAE-R	Center of Academic Excellence in Cyber Research
CD	Cyber Defense
CERT	Computer Emergency Response Team
CI	Cyber Counter Intelligence
CIA	Central Intelligence Agency
CIG	Central Intelligence Group
CIKR	Critical Infrastructure and Key Resources
CISA	Cyber security, and the Infrastructure Security Agency
CNCI	Comprehensive National Cybersecurity Initiative
CNSS	Committee on National Security Systems
CO	Cyber Operations
COI	Office of Coordinator of Information
CSSIA	National Center for Systems Security and Information Assurance
DA	Directorate of Administration
DCCC	Democratic Congressional Campaign Committee
DCI	Director of Central Intelligence
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DNC	Democratic National Committee
DO	Directorate of Operations
DoD	Department of Defense
DS&T	Directorate of Science and Technology
EAPC	Euro-Atlantic Alliance Partnership Council
ENISA	European Network and Information Security Agency
ERP	European Recovery Program
EU	European Union
FBI	Federal Intelligence Agency
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GWOT	Global War on Terror
HIPAA	Health Insurance Portability and Accountability Act

HSC	Homeland Security Council
HSE	Homeland Security Enterprise
I&A	Intelligence and Analysis
IA	Information Assurance
IACE	Information Assurance Curriculum Evaluation
IL	International Law
IS	Islamic State
ISIS	Islamic State of Iraq and Syria
IT	Information Technology
JCS	Joint Chiefs of Staff
KSAs	Knowledge, Skills, and Abilities
KUs	Knowledge Units
MS-ISAC	Multi-State-Information Sharing & Analysis Center
MTIPS	Managed Trusted IP Service
NATO	North Atlantic Treaty Organization
NCA	National Cyber-security and Communications
NCAE-C	National Center of Academic Excellence in Cyber-security
NCSC	National Cyber-security Center
NGOs	Non-Governmental Organization
NIC	National Intelligence Council
NICE	National Initiative for Cyber Education
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
NS	National Security
NSA	National Science Agency
NSC	National Security Council
NSC-68	National Security Council -68
NSD	National Security Directive
NSF	National Science Foundation
NSRB	National Security Resources Board
NSS	National Security Strategy
OCB	Operations Coordinating Board
OIA	Office of Integrative Activities
OISE	Office of International Science and Engineering
OSS	Office of Strategic Services
OUP	Office of University Programs
PNAC	Project for a New American Century
PRC	People’s Republic of China
PSB	Psychological Strategy Board

QHSR	Quadrennial Homeland Security Review Report
R&D	Research and Development
SFS	Scholarship for Service
STEM	Science, Technology, Engineering, and Mathematics
The U.S.	United States
TIC	Trusted Internet Connections
TKS	Task, Knowledge, and Skill
TRADOC	Army's Training and Doctrine
UN	United Nations
UNC	United Nations Council
UNSC	United Nations Security Council
WHO	World Health Organization
WMD	Weapons of Mass Destruction
WWI	World War One
WWII	World War Two

Table of Content

Introduction

Upheaval, altering patterns of state-to-state ties, and conflicts caused by information security risks characterize the world. In this new environment, the United States' national security policy priorities have become convoluted, often unclear, and even inconsistent—not because of the immediate threat of large conventional war, but rather because of the unpredictable, uncertain, and perplexing characteristics of cyber-attacks. Malware, breach ransomware, and Denial of Service assaults that are regularly carried out by rogue governments, terrorists, or criminals. Their impact on national security and the international arena left a gap in establishing national security policy. The United States (U.S.) organizations dependent on cyber capabilities, must be strengthened more than ever.

The key topic that motivates this thesis is the existing basic premises that comprise U.S. national security policy in the twenty-first century. Regarding what American national security policy went through since the 1940s and the progressive development it witnessed with American presidential administrations; national security became a mature policy well-contained by the American government. In perspective to what the American government and people went through at the start of the twenty-first century, the 9/11 attacks altered a new course of the U.S. national security strategy.

Cyber security threat has influenced American national and international policy-making. Cyber security/cybersecurity, as a new domain in American national security, the two terms will be used interchangeably. The U.S. government use the term 'cybersecurity' whereas other documents use the term 'cyber security' or separated by a dash 'cyber-security', in regards to this variety of use, I will use the terms interchangeably to refer to cyber security domain. This new threat prompt the U.S. to seek new paradigms and methods to fit the new era and secure the

threatened U.S. Surprisingly, its advancement made the American security system appear unsustainable, challenged, and vulnerable to the extreme Cyber intelligence's power. As a result, this research will be devoted to diagnosing the United States national security development, new tactics and policies, and the primary initiatives the United States is employing to handle the problem of an eminent cyber security threat.

American national security policymakers recognized the need to address the cyber security danger to the country's infrastructure, economy, and security. The government, in collaboration with agencies such as the Department of Homeland Security (DHS), the National Science Foundation (NSF), the National Science Agency (NSA), the Department of Defense (DoD), and the National Center of Academic Excellence (CAE), realized higher education and research in the field of Information Assurance (IA) education as the only solution to the problem of the overwhelming cyber security threat.

The new policy included a slew of sub-policies to prepare for the age of cyber danger. The process began with absorbing the new area and raising awareness before establishing and preparing for digital human capital in cyber security. This work will investigate the role and engagement of higher education and government organizations in promoting cyber security programs; it will also diagnose the process of developing a human capital/workforce of cyber security professionals and experts through new programs. The analysis of data collection on the available cyber security personnel will decide on the caliber of the contribution of higher education in solving this problem of the human resources shortage in the U.S. in the future; to overcome the shortage of cyber security professionals the U.S. is suffering from.

The central problem guiding this thesis is cyber security as a new danger to American national security and its consequences on American national and international policy. To address

the vulnerability of U.S. national security in cyber security and information infrastructure, the government began to consider new regulations to address the issue. They regarded encouraging higher education in cyber security as the first new policy for minimizing the problem by building a pipeline of competent cyber security workforce specialists capable of overcoming the challenge of cyber security. The responses to this threat address the following critical questions in comprehending and assessing the gravity of the situation:

(A) What are the foundations of U.S. national security? (B) How did National security policy emerge after the 9/11 attacks? (C) What are the new challenges to American security(D) What is cyber security's threat problem? (E) How did higher education promote and expand cyber security in education? (F)To what extent was the new policy of expanding cyber security in education and creating a Human Capital of qualified cyber security workforce implemented?

Expanding cyber security in higher education contributed positively to creating a pipeline of human capital (workforce of professionals) in cyber security.

Making a workforce of experts and qualified professionals in the field of cyber security succeeded in reducing the U.S. vulnerability in Cyber security.

To answering the research questions and the raised hypothesis, this work needs a necessary combination of methods. The study will be based on a thorough content analysis to provide a historical background of the development of American national security and the reform it went through after the 9/11 attacks. This work will explore the content of books, articles, magazines, and military, scholarly, and governmental reports investigating national security strategy. The method is also used to analyze governmental documents exclusively related to cyber security measures in U.S. policy and American national security.

An accurate analysis of government documents of the American National Security Strategy to perceive and diagnose the threat the American security is facing. Statistical analysis of data, a research method that may be applied aiming to effectively measure the cyber security skill gap, the threat of cyberattacks on U.S. infrastructure, and the impact of the shortcoming of cyber human capital specialized in countering cyber threats. The method focuses on maps, diagrams, graphs, and table analyses.

The type of this research is an Exploratory Descriptive Qualitative research EDQ. What makes the research exploratory is the qualitative data collected about the development of national security and cyber security in the 21st century and how it influences the finding of data collection. It is qualitative research as it explores a literature review of the existing sources and analyzes data of available governmental documents related to national security strategies, cyber security, and all governmental initiatives directed to this field. The thesis used descriptive research to evaluate and measure the effectiveness of the new programs adapted in higher education to expand cyber security education, train more professionals in this field, eradicate the immanence of cyber threats, measure the existing of professionals in cyber security, and how far they can overcome the existing shortage of cyber professionals.

The analytical part of this research investigates the role of higher education institutions and government bodies in tackling the major issues in cyber security crisis. With the rising of cyber-attacks each year and the human capital needed to combat them, the data analysis investigated the impact of higher education on the U.S. cyber security workforce and the country's vulnerabilities to cybercrimes. To achieve this goal, the collected data are a descriptive statistical analysis. This analysis aimed to determine the effectiveness of higher education in

addressing the shortage of skilled workers in cyber security and the extent to which it has reduced U.S. vulnerabilities to cybercrimes.

This research investigates the development of American national security policy from 1940 until now and the changes it underwent after the 9/11 attacks. New domains in cyberspace arose as a new threat to American national security; cyber security, with all the threats it covers, imposes new policies with new strategies to contain the threat. To discuss these ideas in a logical and structured manner, the thesis will be divided into six chapters.

The first chapter, entitled "The Evolution of U.S. National Security Policy (1940-1989)", establishes the foundation for understanding American national security. The chapter structure follows a chronological order of each president's national security agenda from 1940. Finally, this chapter delves into a historical and foundational set of data critical for framing national security research's historical evolution. It provides knowledge of the concept. Some of the definitions correlated to the description of the main concepts of this topic, as it provides contextual definitions of the theoretical concepts necessary for this study to clarify the relevance of the key terms used, such as the concept of National Security (NS), American National Security Strategy (NSS).

The second chapter, entitled "National Security Policy after the Cold War: New Policy for a New Century (1990-2009)", depicts the historical development of U.S. foreign policy strategies following the 9/11 attacks, as well as the new paradigm of U.S. foreign policy, which became the mirror image of American national security in the world. Exploring this aspect of U.S. national security reveals that the U.S. national security embraced new concepts, ideologies, and policies that were not previously thought to be part of its security system. The 21st saw the birth of a new age of security systems, particularly those centered around foreign policy. This

section thoroughly examines the Bush philosophy and policy of expanding freedom worldwide and everything it entails, both as a build-up and support. This part analyze the George W.Bush doctrine and the challenges faced the U.S. National Security in this period. Undeniably, we cannot surpass Obama's tangible touch on the American strategy of security after Bush Doctrine, a well-designed, varied strategies set solely to fit the post-2000 era.

The third chapter examines the binary consequences of the issues confronting American national security strategy at home and abroad, as well as the advent of a new field of cyber security, which poses a significant danger to national and international security. This chapter, "Cyber Security: A New Threat to American National Security," explores the main cyber-attacks in history that urged the American government to implement new laws and initiatives to promote and extend cyber security. The Comprehensive National Cybersecurity Initiative (CNCI), launched in 2008, and the International Strategy of Cyberspace, launched in 2011, are the cornerstones of U.S. policies aimed at spreading and prioritizing cyber security as a new domain that affects U.S. national and international security.

To increase in cyber security education and workforce, the United States recognize education as a crucial component of national cyber security readiness. The fourth chapter, "The Synergy between Federal Agencies and Higher Education in Promoting Cyber Security Programs" investigates the relationship between agencies and the system of education and how they lessen the threat of cyber security from overwhelming the workforce specialists and professionals in this sector. U.S. universities with designation began developing new programs and curricula to promote and expand cyber security programs.

To building a strong cyber security professionals: the U.S. government created the National Initiative for Cybersecurity Education (NICE), to improve the United States' long-

term cyber security posture. The NICE addresses awareness, formal education, professional training, and labor force structure. The National Institute of Standards and Technology (NIST) developed the National Cyber security Workforce Framework to assist this effort, providing a uniform language (lexicon and taxonomy) for academia, industry, and government use. Whereas the National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) certification program is a national quality standard for certifying and maintaining high-quality cyber security education and is co-sponsored by the U.S. National Security Agency (NSA) and the Department of Homeland Security (DHS). This chapter describes the connectivity between agencies and universities, the programs and their designated institutions, and how they developed a new paradigm in teaching cyber security specialists.

The final chapter, “Cyber Security Vulnerability: The Final Straw in American National Security”, analyzes and evaluates the role of education in creating a pipeline of talent workforces in cyber security to overcome the United States national security threat in this domain. This chapter intends to demonstrate how expanding cyber security in higher education has contributed to developing a pipeline of human cyber security capital. Furthermore, how has developing expertise and trained professionals in cyber security will contribute to reducing the United States’ vulnerability in Cyber security.

The conclusions shows that higher education has been crucial in reducing the lack of qualified personnel in the cyber security industry. The study found that higher education initiatives reduced the possibility of a labor shortage. Nonetheless, despite these efforts, cybercrime still poses a threat to the United States. The findings of the analysis demonstrate that while higher education initiatives have significantly helped to solve the problem of a skilled

labor shortage, they have not been able to completely eradicate or significantly lessen the nation vulnerabilities to cybercrime.

The current research is built on various print and electronic sources, including primary and secondary ones. Concerning primary sources, there are speeches, newspapers, reports, and conferences written by American and non-American politicians and authors. Secondary sources include diverse books by experts and articles from reliable journals. This rich literature helps simplify the understanding of issues treated in this subject.

After World War II (WWII), national security became important in U.S. national and international policy since it defines modern US transnational ties with the world's states. Robert G. Patman thought that the post-World War II era influenced the United States' new foreign policy initiatives against communism and gave birth to what is now known as NS, which differs significantly from the national defense envisaged in the military protection of the American continent. The idea of NS encompasses a broader range of security interpretations, particularly in the postwar policy. It incorporated numerous economic, political, and military issues that impacted U.S. interests.

According to Sarkesian et al., the definition of National Security includes 'objective competence and perception.' Accordingly, "US national security is the ability of national institutions to prevent adversaries from using force to harm Americans or their national interests and the confidence of Americans in this capability." This term is divided into two parts: physical and psychological. The physical dimension is a quantifiable capacity of the nation-military and its grandeur to competently protect the state's interests and objectives. It includes all economic, intelligence, and nonmilitary contributions to counter an outer threat successfully. The psychological dimension is subjective because it reflects Americans' attitude toward their

country's ability to protect the outside world. The American people demonstrate their ability and willingness to comply with any political agenda that may be implemented to advance their stability at home and abroad.

Looking at NS from a contemporary standpoint will include Cynthia A. Watson's definition of NS as a new challenging international system and the advent of a modern structural change signified by the 1947 National Security Act, concluding in 1991 with the Cold War's end. Even though international security is based on the indispensability of military cooperation among sovereign states, Former Secretary of Defense Harold Brown characterized NS as "the ability to preserve the nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to protect its nature, institutions, and governance from disruption from outside; and to control its borders."

John K Bartolotto identified the formation of national security strategy NSS as another administrative justification in his report, *The Origin and Developmental Process of the National Security Strategy* for the USAWC Strategy Research Project. It recognizes the commitment, identifies the nation's interests by categorizing them as priorities, and decides on the appropriate power tool to fulfill those aims. Earl H. Tilford conveniently described the NSS development as an "intensely political process" since it is an interagency structure in which the NSS plays a vital role. Other government agencies, on the other hand, operate on the periphery with fewer interactions. NSS, prepared annually and bears the president's signature, is especially significant since it shows the American aptitude, ability, and approaches to effect world change.

The Goldwater-Nichols Act of 1986 mandated that the President submit an annual comprehensive report on American national security to the United States Congress. In his study, *National Security Strategy of the United States: Grand Strategy Development,* Thomas P. Reilly

envisioned the NS report as the dominant document used to describe the United States' global interests, goals, and objectives. This paper seeks a comprehensive and descriptive overview of the United States' global foreign policy obligations and national security defensive capabilities. The neoconservative ideology that characterized the Bush doctrine envisions a world in which the U.S. is the unrivaled superpower, maintaining an empire above vulnerability and impervious to threats. They hold the United States accountable for behaving as a "benevolent global hegemon." America is an uncommon nation position to establish democratic, economically liberal governments in place of "failed states" or hostile regimes to the U.S. or its interests. Eventually, the Bush administration incorporated 'democracy promotion' into its 'war on terror' campaign.

The Bush administration's policies, according to Melvyn P. Leffler in his article "9/11 and American Foreign Policy." have more constancy than change. Bush's statements and actions have deep historical roots in American foreign policy. The possession of enormous power and the conviction in a worldwide mission can result in both great good and severe evil. In this explosive mix of power and principles, there is no replacement for wise judgment. While there have been considerable changes, there have also been significant continuities. The shift noted by Leffler represents a recalibration in the complex relationship between danger assessment, interest calculation, value pronouncement, and power mobilization. Unquestionably, national security, dangers, interests, principles, and power have all played a role in determining US foreign policy.

Adam Quinn, on the other hand, assessed the Bush ideology and administration within the historical context of U.S. foreign policy tradition. This latter contends that national-specific ideological characteristics are important in foreign policy. His book, *US Foreign Policy in Context: National Ideology from the Founders to the Bush Doctrine*, criticized the George W.

Bush administration's National Security Strategy, which many considered as a drastic and undesirable ideological shift from past policy and foreign policy, emphasizing liberal universalism and rejection of realism. A cumulative argument based on historical cases confirms this critique by attempting to explain the persistence and opposition of American leaders to the concept of realism. Quinn argued that there was a link between historically evolved ideological ideas and the character of the country's modern diplomatic strategy.

In a world where American power has been tested by the new emergence of other powers, such as the (BRICS)_ (Brazil – Russia – India – China –South Africa), Obama found it important to codify his doctrine to the new changes. In his NSS 2010, he differentiated his strategy from that of his predecessor by replacing U.S. hegemony with a "balance of power" policy and acknowledging the "relativization" of American strength. This idea has already been introduced by a famous foreign policy analyst Fareed Zakaria in his famous essay: "The Post-American World and the Rise of the Rest." The United States acknowledgment that it can no longer act in international wars alone; friends must be partners. Hillary Clinton, Obama's secretary of state, confirmed the change in the vision of the U.S.'s role and power in the world.

A new threat emerged in the contemporary era to become a permanent threat to American national security. America's expanding reliance on the internet has generated new weaknesses that have been exploited as quickly as the nation can respond. Cyber-attacks can bring economic harm, physical destruction, and even death. They pose a severe threat to American national security and require stronger attention from American officials. In a book entitled *America's Cyber Future: Security and Prosperity in the Information Age*, some of the world's leading experts on international relations, national security, and information technology, such as Robert E. Kahn, Mike McConnell, Joseph S. Nye, Jr., and Peter Schwartz, indicate that, despite

significant efforts by the U.S. government and corporate sector to boost cyber security, the rapid advancement of cyber threats continues to exceed development.

This work briefly investigates incidents of large international cyber-attacks: Estonia in 2007, Saudi Arabia in 2012, the United States in 2012, and the 2016 elections: Russian intervention in U.S. elections. When the U.S. government realized the importance of cyber security, President George W. Bush launched the Comprehensive National Cyber Security Initiative (CNCI) in 2008 to establish the groundwork for information security in order to keep the U.S. safe. President Obama expanded the project further by deciding that its actions should be integrated into a broader U.S. cyber security plan. This instruction was intended to address recent security concerns, anticipate future threats, and preserve both classified and unclassified networks' confidentiality, integrity, and availability. Initiative N8 from the CNCI aimed to expand cyber education programs. As the government realized that an information system is only as good as the people who run it. They started a cyber-education upgrade comparable to the science and mathematics upgrades since 1950.

The lack of a common language or lexicon to understand the work and skill requirements for IT security positions is hampering the demand for cyber security professionals to address the increased level of threats. To establish an effective security program, organizations must understand the tasks, knowledge, skills, and capacities. In her study, Anne Kohnke examined the NIST cyber security frameworks, namely the National Initiative on Cyber security Education (NICE) Cyber security Workforce Framework 2.0. She thoroughly mapped and discussed the NICE Cyber security Workforce Framework 2.0 duties in conjunction with the CSF Framework functions and categories to offer cyber security professionals with a comprehensive grasp of how to create and operate an efficient IT security program.

The National Centers of Academic Excellence in Information Assurance (IA) Education initiative was established by the NSA in 1999. The effort was created to assist intelligence community professionals in meeting the rising demand for cyber security skills. As it became obvious that cyber defense would become an increasingly critical component of national security, the program's goals grew to meet the nation's need for cyber security workforce development (CAE-CD 4-8).

The qualifications for designation under the National Centers of Academic Excellence in Cyber security (NCAE-C) program for Cyber Defense (CD) managed by the NSA are summarized below. The CAE Cyber Defense (CAE-CD) accreditation is awarded to regionally authorized academic institutions that provide cyber security-related degrees, majors, minors, and certificates at the Associate, Bachelor, and graduate levels. The applicant institution must demonstrate considerable community involvement, academic activities, and institutional cyber security practices, as well as one or more Program(s) of Study (PoS) under consideration that meet the standards outlined in this document. The NCAE-C program promotes and funds high-quality academic programs that assist in the training of the nation's cyber workforce.

The goal of the National Centers of Academic Excellence (NCAE) program is to build and oversee a college and university-wide initiative to improve cyber security education by raising the bar in terms of both course content and staff and student expertise. This program integrates cyber security practice within the institution and across academic disciplines and actively seeks answers to cyber security education concerns (CAE in Cybersecurity Community 12-13). The success of the NCAE program is largely due to federal departments and agencies working together closely on cyber security workforce education and development. Close

collaborators include the National Science Foundation (NSF), the National Science Agency NSA, the DoD, and the DHS, in addition to the Program Office PO cooperation with the DoD.

The Comprehensive National Cyber Security Initiative (CNCI), initiated by the Bush administration and supported by the Obama administration, has allowed the U.S. to improve cyber defense in the academic sector. The success of the United States Government's efforts to defend its cyber infrastructure will depend not on the billions of dollars spent on cutting-edge technology, but on the people who have the expertise to put that technology to use. However, more government and commercial sector cyber security experts are required to implement the CNCI and establish a robust Federal cyber security employment field. While the existing cyber security training and human development programs are beneficial, they are limited in breadth and might benefit from better cooperation. Eventually, the United States will need to build a highly competent and cyber-savvy workforce, as well as a fertile stream of future experts, in order to sustain U.S. technical superiority and future cyber security.

The federal government of the United States requires a sufficient number of cyber security workers. Given the continued growth of cyber dangers, the United States requires a workforce capable of securing cyberspace. One possible entry point for national government cyber specialists. While this is true, as Tony Coulson et al. point out in their book *Cyber Capability Plan and the Need for an Increased Cyber security Workforce*, this workforce is not large enough to handle the current level of cyber threats, the cyber security workforce needs to gain the necessary competence and skill in this subject. A pipeline of CS professional can bridge the gap between the United States currently understaffed cyber workforce and the cyber skills that it demands. The NICE Framework can improve cyber capabilities planning by providing a foundation for training, developing, and retaining cyber security skills.

This methodology focuses on establishing a human resource in cyber security that is knowledgeable and skilled. Scholarship programs offer additional possible sources of K-12 education and talent pools from which college students may be recruited to work for government organizations and the military. However, these programs must be strengthened in order to close the cyber security employment deficit in the United States. Academia developed its cyber security programs in collaboration with bodies that certify CAE schools. Such initiatives could lessen the cyber security workforce shortage.

The CNCI will need to be upgraded and pursued further in the future. It was an important first step in making the United States a safe environment to use cyber, and it can be expanded in the coming years. Expanding cyber security in higher education and preparing professional employees in the field is a first initiation the government started with and will keep reinforcing in the coming years with other flexible and adaptable programs such as the NICE Framework and the CAE program. The new government policy in creating a pipeline of workforces was to target the shortage that the public and private sectors are suffering from in terms of professionals in the field; the achievement of this objective is based on how the threat of cyber security on U.S. national security contained before and after 2010? Moreover, to what extent was the new policy of creating the Human Capital of a qualified cyber security workforce implemented?

Chapter One:

The Evolution of U.S. National Security Policy (1940-1989)

In the second half of the twentieth and early twenty-first century, the U.S. has already moved to a new era of a global security strategy. This latter was created to contain the threat of communism imposed by the former Soviet Union after WWII. This global security strategy shaped the new foreign policy of containment. To endure the challenges of the new global geo-political order and protect the U.S. interests, especially after the emergence of the Soviet Union as an imminent threat to U.S. security, U.S. changed its ideology of national security. This chapter focuses on the transformations and evolution of national security under certain presidential administrations. First, the chapter gives an introductory section to define the concept of security in relation to American policy and strategy. Then, it underlines each president's administration and its contribution to improving the measures, forms, and strategies of American national security.

1.1. The Concept of National Security (NS)

National Security became a vital concept in U.S. national and international coexistence after WWII since it has marked modern U.S. transnational relations vis-a-vis the world's nations. The post-WWII era shaped the U.S. new foreign policy strategies against communism and gave birth to what is now called NS. The concept of NS has a broader perception of different interpretations of security, especially in the post-WWII policy. It amalgamated many economic, political and military factors with an impact on U.S. interests (Patman 6).

The definition of NS contains both 'objective capability and perception'. Accordingly, "U.S. national security is the ability of national institutions to prevent adversaries from using force to harm Americans or their national interests and the confidence of Americans in this capability"

(Sarkesian et al. 2). This definition has two dimensions: a physical and psychological one. The physical dimension is a measurable capacity of the nation-military and its grandeur to defend the state's interests and objectives competently. It encompasses all economics, intelligence, and nonmilitary contributions to withstand an outsider threat successfully. The psychological dimension is subjective as it mirrors the American position towards their state's ability to provide security against the external world. American people show their aptitude and readiness to cooperate with any political policy that may provide them with total security assets and advance their stability at home and abroad (Sarkesian et al. 2).

Looking to NS from a contemporary standpoint, it will play a role in a new challenging international system and the advent of a modern structural change signaled by the 1947 National Security Act, culminating after the end of the Cold War in 1991. Though international security is based on the indispensability of sovereign state military interaction, former Secretary of Defense Harold Brown gave a very fundamental definition of NS: "National security, then, is the ability to preserve the nation's physical integrity reasonable terms; to protect its nature, institutions, and governance from disruption from outside; and to control its borders" (qtd. in Brown 4).

The U.S. changed its national security and intelligence organization ideology. The U.S. government revealed that the post-Cold War era exposed U.S. national security policy to new challenges that called for reform. The need for contemporary adjustments in the U.S. national perspective of American national security connected America to the world by linking national security to politics, economy, psychology, and military services. This made NS a wider and more vital element in assuring and achieving nations' security.

1.1.1. American National Security Strategy in Perspective

'Strategy' is a very contesting word in meaning and application. However, the fundamental meaning of the word strategy is "a plan of action that organizes efforts to achieve an objective". Though this definition lightens the massive complexity of the word strategy, contextualizing the term in the contemporary framework makes it the most challenging to define. However, it is much more accurate and descriptive to consider strategy as "a complex decision-making process that connects the ends sought (national objectives) with the ways and means of achieving those ends" (Drew 13).

National Security Strategy reports contain the fundamental components of any vital discussion about American strategic security. The first report in NS was in Reagan's Administration in 1987. This report contained sections that outlined the process, objectives, and means used to attain the final NS goals. It was made clear in Reagan's saying, in a section titled 'An American Perspective', that they had already "laid the foundation for a more constructive and positive American role in world affairs by clarifying the essential elements of U.S. foreign and defense policy." Furthermore, the administration declared their potential in resetting and adapting U.S. policies to reflect the "dynamics of a complex and ever-changing world" (Reilly 12).

Leadership perspective was one of the essential elements revealed in the American NSS; the administration highlighted this new role of American policy after WWII and its readiness to crown its policy with this challenging mission in the future (13). The 1987 report established a principal concept based on the following: "National interests as a guideline and a pathway to US strategy. The report detailed one of the primary objectives to sustain the national interests of the

United States by emphasizing the former Soviet Union being the "most significant threat to U.S. security and national interests" (*National Security Strategy of Engagement and Enlargement* 07).

NSS is a process that starts with assessing the given situation as the crucial point to ignite the hierarchical process of achieving the goal of preserving and promoting national interest. Those ends impose a political aim and specific objectives that must be attended to achieve the final political goal. Therefore, NSS marked a transitional stage of the problem, from the state of current conditions to the expected and wanted state of affairs using the political frame as a mediator. The section on U.S. Foreign Policy in NSS, 1987, expressed the U.S. commitment to fostering American foreign policy through spreading democracy and international economic vitality. This section adequately focused on the areas of engagement as the fundamental goals and elements of power in foreign policy, international economic policy, political and informational elements of power, and domestic policy. However, the key player in this section was the military instrument of power and its contribution to NS (*National Security Strategy of Engagement and Enlargement* 1-7).

Each NSS represents an administrative rationale; it acknowledges the commitment, identifies the nation's interests by classifying them into priorities, and decides on the adequate instrument of power to achieve those interests. Conveniently, Earl H. Tilford assessed NSS development as an 'intensely political process'; it is an interagency policy that plays a central role in government procedures. NSS, initiated annually, is also the nation's most important element of power. It plays a prominent role in interconnecting agencies. It serves as a check on interagency systems, an interpretation of the president's agenda, and a systemic policy regarding the convincing and appropriate political language used in administrations. Thus, NSS is a 'political design' of the president's agenda of national security (Bartolotto 1).

1.2. Instruments of Power

American NS and interest arose as its national policy's eternal and decisive identity. The three essential interests that constitute the American policy and NS are physical security, promotion of values, and economic prosperity. These three instruments of power are considered the theme of U.S. policy to achieve peace and prosperity at home and worldwide (Jablonsky 4). Physical security sets measures to preserve the nation's territory from foreign attacks, secure people, and assure their healthy existence within their protective institutions. It has always been the government's responsibility to pursue these security measures. James Madison refers to security as "security against foreign danger."

Throughout U.S. history, the security of the American hemisphere was invincible. However, 1945 marked a new beginning to a global security frontier: the atomic bomb jeopardized this safety line between nations. Ballistic missiles and long-range bombers threatened the world and U.S. invulnerability. After WWII, the US reinforced the idea of expanding the area of security to include other vital sectors of national power. The new requirements surpassed the military sector, as *Life Magazine* wrote in 1945 "we are in a different League now", "How large the subject of security has grown, larger than a combined Army and Navy." (qtd. in Yergin 195). Eventually, the NS has grown broader than being exclusively limited to the two sectors of the Army and Navy. Ferdinand Eberstadt, the architect of the new U.S national security system, saw, in agreement with policymakers, that . . . foreign policy, military, and domestic economic resources should be closely tied together" (Jablonsky 6).

The concept of NS was easily defined after WWII when the United States had the most substantial military arsenals and the largest economy that promoted its leadership in the world. American interests are vitally linked to factors like the economy and military interests in

American international politics. Since 1940, the U.S. has based the creation of its diplomatic policy on the "open door" policy. It started first in the Western Hemisphere and then in Eastern Europe, Asia, and the Persian Gulf. The open-door policy is a liberalization of trade and the economy. The rendering of the Open-Door policy contains the recognized components of fair trade, little governmental involvement in the concerns of the firm and the individual, and the liberal outlook's abhorrence of power politics. Economic expansion, minimal governance, and political isolation were all combined to form a cohesive totality (Ninkovich 190).

The ultimate objective of the American national and international security strategy is to create a beacon for its widespread ideology of a structural system, which rests on spreading democracy and liberal values worldwide. The economic side is envisioned through the openness of the international economy. The economic factor was chosen as the beating heart of the U.S. grand strategy because it is crucial to U.S. security. In addition to military capability in maintaining security and economy, this latter topic was prominent in three parts of the NS debate. Firstly, the economy provides funds for the military. Secondly, the economy is a security source for the nation's well-being. Thirdly, the economy provides an arena for interaction, exchange, and mutual benefits between nations (Nanto 5). Eventually, economic power was used to reconstruct the American international system after WWII as a strategy to use "America's preponderant economic strengths."

The political open-door policy manifests realism, exceptionalism, idealism, and liberalism in international politics through the American NS policy. Essentially, NS is the mirror reflecting national objectives, which target the achievements of the nation's interests. The most prominent national interests the NS aims to protect are:

1. The United States has survived as a free and independent nation, with its essential ideals and institutions intact.

2. A strong and expanding US economy.

3. The expansion of freedom, democratic institutions, and free market economies around the world, united by an open and fair international trading system.

4. A world that is stable and secure, with no substantial threats to US interests.

5. The strength and vitality of U.S. alliance connections (Section 4 of the National Security Strategy for Engagement and Enlargement).

American NS objectives are the fundamental provisions to advance NS goals. These objectives are applied in a variety of ways. However, they form a fundamental plan to guide the developmental process of NS policy supported by elements of power. The main national objectives of American interests are:

1-In coordination with its allies, the U.S. preserves global security for its homeland and its allies. It sets a preemptive defensive strategy to deter aggression and threats on U.S. territory.

2- Safeguarding and guiding the economy's interdependence as global economic growth threatened the tranquility of the global system vulnerability. The U.S. provided Europe with economic growth programs after WWII. However, it only solved some of the unresolved problems that may affect U.S. interests (National Security Strategy of Engagement and Enlargement 5).

3- Democracy is the new vehicle to spread freedom and civil liberties worldwide. American foreign policy advocated a national struggle for freedom and democracy worldwide. American strategic policy valued the security of freedom and democracy and considered them the pillars of its heritage to be respected, preserved, and secured worldwide. As it emphasized, the insecurity

of democracy around the globe endangers the status and security of the U.S. at home and abroad (5).

1.3. National Security Policy under the Truman Administration (1945-1953): The Containment Ideology

Secretary of the Navy James Forrestal appointed Ferdinand Eberstadt, a pioneer in Wall Street mutual fund activities, as a committee chair on the postwar organization for NS. In 1945, Eberstadt announced a new strategic function and unification for the U.S. services in NS, emphasizing "A complete realignment for our governmental organization" (Jablonsky 9). Eberstadt, in his suggestions, advocated the separation of powers and administrations: "Separate departments provide a greater representation of specialized knowledge; they provide a greater aggregation of experienced judgment and ensure representation of varying viewpoints." (9). The Council of Common Defense (CCD), later called the National Security Council (NSC), was charged with providing permanent assistance to the Executive Branch with highly qualified advisory advocacies. The leading role of this board of advisors was the mutual exchange of information, data, and opinions for the primary sake of framing the post-Cold War policy of NS and setting the cornerstone of its foundation (Nelson 267; Jablonsky 9).

Eberstadt recommended in his 1945 report the formal establishment of the Joint Chiefs of Staff (JCS) and the National Resources Board (NRB) to link and build an inter-exchanging infrastructure between the industrial and military sectors. The Eberstadt committee helped to establish a Central Intelligence Agency (CIA) that only targets foreign threats, as well as three coordinated services (NUS, Congress, Senate, and Committee on Naval Affairs) ("National Security Act of 1947," sec 102). The 1947 NS Act was based on the Eberstadt report, establishing compromises between the Executive Branch and Congress. "Separate departments

provide a greater representation of specialized knowledge, a greater aggregation of experienced judgment, and ensure representation of varying viewpoints," according to the collaboration. The separate departments aided in broadening the scope of NS's purview. To meet security requirements after 1947, the tendency and new positions of services created an autonomous defense policy and a much more developed NSS ("National Security Act of 1947," sec 201).

There was an increase in militarization of the U.S. government and the power granted to the Executive Branch and the president in wartime and its aftermath. The State Department targeted state stability and military security, especially during the Korean War. The same reorganization and restatement of the priorities of American interest took place in the White House; the effect of this change was seen in the creation of the National Security Council (NSC) as the first step of the new organization in the early Truman years. The Chief Executive exclusively used this office; however, after 1950 (NSC) became the government's core. Their primordial role was to assist and provide help to the president regarding NS policy decisions (Jablonsky 13).

By the 1950s, the dominant positions in Washington included the heads of the State Department, the DoD, the CIA, and the Joint Chiefs of Staff (JCS), the President's NS Adviser. This domination led to the developing form of the U.S. government after the National Security Act of 1947. The Act set a structural framework to end the Cold War, creating four agencies to complement the old ones; the National Military Establishment, the CIA, the NSC, and the National Security Resources Board (NSRB). Their principal role was to solve the surviving problems in the aftermath of WWII. One of those agencies, NSRB, disappeared in 1953 (Nelson 269).

After WWII, there was an apprehensive disagreement and fear in public and media about the future course of the U.S., duly clarified by Michael Hogan, who announced the emergence of two dynamics at work after 1945, “one associated with an older political culture” and the second,”. . . with the new ideology of NS.” (Nelson 266). Eventually, after 1947 the U.S. launched an era of preparedness and continuous aptitude to face the international threat of the former Soviet Union and to protect its core values and national interests in security, promotion of values, and economic prosperity. Truman made it clear in his statement in 1948: “the loss of independence by any nation adds directly to the insecurity of the United States and all free nation” (Patman 6). The policies adopted by the U.S. to curb communism and further containment, confrontation, and intervention- were considered new strategies that could make the world a better place. The new state of protectiveness and caution led to the creation of what Daniel Yergin and other scholars called America’s ‘national security state’ (6).

1.3.1. The Truman Doctrine

Truman recognized that only the United States could handle the problem at hand. In February 1947, the British government announced its shortage and deficit in carrying its economic and military support to Greece and Turkey. The newly declared resolution was invoked by the private Secretary of the British Ambassador Lord Inverchapel to General George Marshall, informing him that by April 1, all aid would be cut to Greece and Turkey (Satterthwaite 74-75). The deteriorating state of Greece’s economy and security with British abandonment obliged the U.S. to bear the burden. Undoubtedly, the innovative mission fell on the U.S. shoulders, and President Truman had no escape but to take it. The U.S. government realized that it was an American duty to take on the responsibilities of the British government as

both Greece and Turkey offered haven to communist partisans supported by the Soviet government (Satterthwaite 74-75).

By 1947, the ideology of supporting Turkey and Greece had already started. The U.S. government issued a new consensus to inform Congress of the mission threshold the United States government was about to engage in. Dean Acheson, the U.S. Secretary of State (1949-1953), saw that the U.S. should react to the new changes and that "the world faced the greatest polarization of power since Athens and Sparta, and a choice between American democracy and individual liberty or Soviet dictatorship and absolute conformity" (qtd. in Offner 07).

Loy Henderson, a U.S. Foreign Service officer and a diplomat, announced his concerns to speed the process to fill the vacuum left by the British government; he viewed the withdrawal of Britain from Greece and Turkey as a tremendous threat to U.S. Security in the world, precisely in Eastern Europe. The Eastern Communist partisans supported by Yugoslavia and Bulgaria would take control of Greece and create a haven for Communists. Anxiously, Henderson proclaimed that even Turkey, with the strongest army in the area, would be in an unsustainable position against the Communist drive. Thus, the calamities that could emerge from the Communists' control of the area would be disastrous unless these areas were safely contained (Satterthwaite 75; Weiner, 21-22). Eventually, the President met with his advisers with the Congress members, and after a sensitive hearing, they approved the project of containing the calamity in Eastern Europe (Satterthwaite 76).

By passing the United Nations (UN) was heavily debated in Congress; the Bill signed on May 22, known as Public Law 75, abridged the United Nations Security Council (UNSC) prerogative. UN Ambassador Warner Austin assured the UNSC that the primary objective of the Bill was not to oppose the UN's will in international affairs; the Bill was passed under a fair

amendment that supported the willingness of the U.S. to withdraw its aid if this Act was not desirable by the UNSC or the General Assembly (79). The Act, however, surpassed General James K. Crain, Deputy Chairman of the policy committee on arms and armaments, who strongly opposed the Bill and believed that the U.S. was repeating the same mistake Britain did.

President Truman appeared to inform the American people about the U.S.'s new policy to implement and adapt in Europe. On March 12, 1947, in the House of Representatives, President Truman delivered his historic speech 'live', where he asked Congress to provide him with 400 million dollars to assist Greece and Turkey financially, economically, and with military armaments (Xydis 255). The historic speech not only launched a new era of reform in Europe; furthermore, it triggered a new post-war foreign policy of the U.S., for he declared that "I believe that it must be the policy of the United States to support free peoples who are resisting attempted subjugation by armed minorities or by outside pressures" (Truman). The president's message to the world proved the U.S. readiness to stand by any nation under domestic or international threat. American involvement in keeping security and peace around the globe was President Truman's Doctrine, a doctrine that would become the policy and strategy of the United States of America.

Truman Doctrine set a basis for later intervention in any foreign conflict. George Kennan, the U.S. Ambassador to the Soviet Union, explained that the doctrine of 'Open Doors' is an unlimited military intervention. In his thorough essay "the Source of Soviet Conduct" (1947), he clearly explained that Soviet strength had gone beyond a military threat to an ideological one. Kennan called for a strict and meticulous U.S. policy of "containment" by applying "counterforce" to stop the Russian geo-political foundations. Consequently, containment became the keyword of the Truman Doctrine, which emphasized unlimited global strategic confrontations, whether overt or covert (9).

Though President Truman disliked the term ‘Doctrine’, he introduced declarations of a common policy as an American foreign policy that would mark the shift from being a state on the periphery to being at the center of the world’s stage. After joining the UN in 1947, ending the ‘epoch of isolation’, the U.S. began a new era as a democratic country. American ideals and values were solely set to preserve, protect and spread freedom around the globe; by spreading democracy, the U.S. stood against a totalitarian or tyrannical government. Thus, in its policy, shortly, America was likely to be independent of any nation that sought predominance in the world (Xydis 261).

1.3.1.1. The Importance of the Marshall Plan

As the Cold War began, the U.S. and the Soviet Union formed a paradoxical and antagonistic world axis. In 1947, President Truman assigned George C. Marshall; a well experienced military, as a new Secretary of State. The crisis in Greece and Turkey was Marshall’s first mission in his new office. Based on what happened in Eastern Europe and the economic crisis, Kennan sent a report to Marshall on the state of postwar Europe and suggested that the U.S. should contribute to rebuilding “the economic health and vigor of European Society” (Marshall).

The Marshall Plan was directed to aid and end European famine and tyranny. As Marshall stated, “Our policy is directed not against any country or doctrine but against hunger, poverty, desperation, and chaos.” (Marshall, Speech 2). This plan, known as the European Recovery Program (ERP), was the largest amount of humanitarian aid ever made by the U.S. to Western Europe (Payne and Thakkar 133). The ERP is also considered the greatest strategic project in history since it aimed “to preserve America’s vital tactical interest” in Europe (135). ERP was a strategic pathway and a reconstructive plan for governmental infrastructure and

European integration. Effectively, Europe became part of the Atlantic Alliance Partnership Council (EAPC), the North Atlantic Treaty Organization (NATO), and a multilateral strategy aimed at maintaining peace and stability (140).

The new foreign policy was the genesis of a multilateral strategy to free the world. First, the US started to forge a comprehensive policy in Europe and later in the world more broadly. The main objectives of this plan were to reconstruct and integrate European nations and spread peace in Europe after centuries of wars in the area. Thus, the plan was a new US -Europe ideology in foreign policy that opened a new era, leaving behind the traditional policy of isolationism. Spreading freedom and peace in Europe, as Winston Churchill described the Marshall Plan is 'the highest level of statesmanship' (Marshall, Speech 4).

1.3.1.2. The Creation of the National Security Council (NSC)

The early 1940s was a new era of World War II that underscored the importance of cooperative policy with allies. This led the U.S. to rethink the functions of national security decisions and its policy-making to assure a successful and comprehensive implementation of policies between the sectors of government, the State, War and Navy departments, and to embrace the responsibility to make effective decisions concerning very specific and common objectives. Thus, the indispensable need for a new organizational pattern to assist the president in policy decisions became an important policy instrument (Best 5).

General George C. Marshall, Army Chief of Staff, suggested that Congress unify the military institutions. In 1944, Congress considered the idea with the approval of the army. However, unlike the army, the navy opposed it and adjourned this investigation until 1945. James Forestal, the Secretary of the Navy, emphasized the necessity of including the State Department in the national security apparatus. He called for Ferdinand Eberstadt, a New York

attorney and banker with high qualifications and expertise. Eberstadt was trusted with the creation of a common body of the National Security Council that would serve U.S. national security effectively: “What form of postwar organization should be established and maintained to enable the military services and other governmental departments and agencies most effectively to provide for and protect our national security?” (Best 5).

The creation of the NSC in 1947 brought diplomatic and military personnel together to serve the body of the Council in analyzing and interpreting the post-WWII era proceedings (Best7). The first Council was held on September 26, 1947. Its significant contribution was to assert a spirit of cooperation between departments and agencies, to serve American security matters (John 233). The following stated the purposes of NSC, as it appears in section 101 of Title I entitled “Coordination for National Security”:

> (a)... The function of the Council shall be to advise the President concerning the integration of domestic, foreign, and military policies relating to the NS to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security.
>
> (b) In addition to performing such other functions as the President may direct, for more effectively coordinating the policies and functions of the departments and agencies of the Government relating to the national security, it shall, subject to the direction of the President, be the duty of the Council.
>
> (1) To assess and appraise the objectives, commitments, and risks of the United States to our actual and potential military power, in the interest of national security, for the purpose of making recommendations to the President in connection therewith.

> (2) To consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security, and to make recommendations to the President in connection therewith. (Paragraph 402)

The President has nominated a civilian executive secretary to oversee the NSC's office personnel. The CIA was founded in 1947 as a branch of the NSC, which was itself founded by the National Security Act. The Act also established a military department at the national level consisting of the Army, the Navy, and the Air Force, all of which report to the Secretary of Defense (Best 6).

As the U.S. and the Soviet Union clashed over the fate of Berlin, President Truman and his advisers used the NSC to handle the crisis at hand for the first time in 1948. This Executive Council had an impact as it temporarily extended to include the president as a chairperson and The Joint Chiefs of Staff (JCS) to provide influential decision-making between the White House, State Department, and the military institution. The Berlin case gave essence to the creation of the NSC by using correlated institutions sources in a time bounding crisis. Eventually, the NSC became one of the U.S. strategic services in the Cold War era.

President Truman forged new directions in the NSC, which were implemented in January 1949. First, the President asked the Secretary of the Treasury to participate in all NCS meetings. In August 1949, new national security amendments were passed (P.L. 81-216) to reconsider the council membership. This latter consisted of the following members: The President, Vice President, Secretaries of State and Defense, and Chairman of the National Security Resources Board. This Act also designated the JCS as "the principal military advisers to the President. Finally, in August 1949, via Reorganization Plan No. 4, the NSC became part of the President's Executive Office (Best 7).

The president's main objective was to protect the nation's interests. Eventually, he wanted to bring together civilian experts and military advisers in a conventional partnership to provide the NS with constructive insights into the crisis. As a result, the president kept the Council small and informal with his infrequent attendance. The first executive secretary of the Council was Rear Admiral Sydney Souere, his safeguard and voice in that Council (Stewart 233).

President Truman saw the NSC as a board of advisers but not as policy decision-makers, as one scholar has concluded:

> Throughout his administration, Truman's use of the NSC process remained entirely consistent with his views of its purpose and value. The president and his Secretary of State remained completely responsible for foreign policy. Once policy decisions were made, the NSC was there to advise the president on matters requiring specific diplomatic, military, and intelligence coordination. (Best 6-7)

1.3.1.3. The Creation of the Central Intelligence Agency (CIA)

The U.S. developed its first intelligence agencies on July 11, 1941; President Franklin D. Roosevelt formed the Office of Coordinator of Information (COI). In June 1942, The COI was reviewed to form the Office of Strategic Services (OSS). Both the COI and OSS were created to serve the country in WWII. Their main objectives were to collect data about the war and the axes of powers, analyze them, and make and plan clandestine missions for intelligence benefits. The OSS' missions produced considerable intelligence; this information was communicated in various forms, including reports, maps, telegraphs and memos (Heaps 287-288).

After WWII ended, Harold D. Smith, Truman's budget director, warned the President about dismantling the OSS, as it risked returning the U.S. to a pre-Pearl Harbor state of

innocence (Weiner 21). By executive order 9621 in October 1945, President Truman dismantled the OSS and transferred the Agency's personnel and records to strategic services housed in the War Department (Heaps 299-300). Though Truman dismantled the Wartime Office of Strategic Services in October 1945, he never saw the urgency of creating a substitute agency; instead, he wanted to integrate intelligence services into the armed forces. Therefore, he created the Central Intelligence Group (CIG) to accomplish what the OSS left incomplete. However, in 1946, the CIG gained new authority and confidence in its potential: Congress believed that a new, contemporary American intelligence system should be established quickly. On July 22, 1947, Congress passed the National Security Act, which Truman signed into law.

The attacks on Pearl Harbor in 1941 had a tremendous effect on President Truman and Congressional members. They agreed that Pearl Harbor represented atrophy in the intelligence system of the U.S. They believed that the shocking attack could have been halted if departments and agencies had practiced cooperative and mutual exchange of information to sustain the country's international interests. For this reason and many others, the president and his advisors saw the need to re-establish command and unification of the agencies by issuing the National Security Act of 1947 (Nelson 274). The Act gave birth to the CIA as "an independent, central agency, not an autonomous one it would be both rivals and compliment the efforts of the departmental intelligence organizations" (Weiner 6-2). The War, Navy and State Departments fund the CIA, to which it reports all intelligence.

The National Security Act of 1947 was the fruit of the post-war change in US policies correlated to national and international security. The Act authorized the creation of the NSC as an advisory council to the president, the CIA, the Department of Defense (DoD), and The Joint Chiefs of Staff (JCS) as central institutions of the nation. Thus, the Executive Branch's power

was increased because of the newly adopted policies. NS was considered the president's exclusive purview with the assistance of his advisors and military professionals (Patman 7).

The CIA was founded as an independent agency under the command of the NSC. Its main objective was to "correlate and evaluate intelligence relating to NS and provide for the appropriate dissemination of such intelligence within the government". Furthermore, the CIA was primordially set to protect the U.S. from threats (Hastedt 370). The NSC gave the CIA the right to collect and assess all national intelligence related to all departments and intelligence agencies. One of the vital roles that the CIA played, with expertise and proficiency, was collecting intelligence from human informants.

The division of CIA into four major directorates: The Directorate of Operations (DO), The Directorate of Intelligence (DI), The Directorate of Administration (DA), and the Directorate of Science and Technology (DS&T); in each Deputy Director heads each division. The DO, or Clandestine Service, collects foreign intelligence from human sources ("assets") worldwide and conducts covert action programs. The DI comprises analysts who prepare "all-source" assessments of foreign incidents and individuals based on intelligence collected by the DoD and other agencies. The DS&T houses several technical collections programs (including the Foreign Broadcast Information Service, a supervisor of foreign print and broadcast media) and provides technical support to the DO. The DA supplies administrative support for the entire Agency. The DCI is the legislative head of the CIA. Although the DCI is also the head of the Intelligence Community, most DCIs spend the volume of their time managing the CIA. Throughout its history, the CIA's senior management also has included an Executive Director, a non-statutory position that varies in duties and importance. The current DCI has delegated

extensive responsibilities to the Executive Director and has directed the CIA's four Deputy Directors to report through (U. S Government Publishing Office GPO 62).

Section 102 of the 1947 National Security Act stated that the power of the Director of Central Intelligence DCI was scrutinized "for correlation evaluation and dissemination". In addition, section 102D of the National Security Act of 1947 announced, "it shall be the duty of the agency, under the direction of the National Security Council... to correlate and evaluate intelligence relating to National Security". In parallel, the same section declared the involvement of the other agencies in "continu[ing] to collect, evaluate, correlate and disseminate departmental intelligence" (Stewart 259).

An autonomous CIA was a matter of time. In 1949, the Central Intelligence Act released the Agency from its normal duties (Reichard 262). After that, the CIA showed great potential for collecting intelligence and conducting clandestine operations. Subsequently, during Eisenhower's term (1953-1961), and with Allen Dulles as the head of the Agency (1953-1961), the Agency showed potential accomplishments. Accordingly, the CIA became a vital operational organ in Eisenhower-Dulles' foreign policy (262). The CIA finally expanded its sphere of operations and autonomy as Harry Howe Ransom declared in 1950:

> "The real operating constitution of the CIA is not so much the statutory authority given by Congress in 1947 and 1949 but a score or so of super-secret National Security Council Intelligence directives, which only a few high government officials have ever seen. These directives, after accumulating for a dozen years, were 'codified' in 1959". (262)

1.3.1.4. The National Security Council-68 Document (NSC-68)

The Department of Defense (DoD) drafted the National Security Strategy (NSC)-68 to advocate for a drastic increase in the size of the U.S. armed forces, both in terms of conventional and nuclear capabilities. It asserted the rebuilding of American defense to fight and overcome wars and attacks with advanced weapons and forces. This Act was meant to reduce the intensity of the former Soviet Union attacks and take control over Eastern Europe. In other words, it represented a new strategy of containment (Offner 12-13). The major objectives of NSC-68 are to strengthen and boost American capabilities in dealing with domestic and international threats. Second, to strengthen the nuclear power arsenals and strategies to shape a powerful and invulnerable position against aggression. Third, to assist European allies and strengthen their military potential against the communist threat (Drew 15).

President Truman used many of Kennan's theories between 1947 and 1949. The exclusive ideas of the containment policy were Kennan's most strategic contribution to American international policy. In February 1946, Kennan sent "The Long Telegram", considered the original source of U.S Cold War policy. In July 1947, his "X" article in *Foreign Affairs* outlined the containment policy that became U.S. policymakers' agenda. The ideas of Kennan, the Kremlin expert diplomat, were that the containment strategy was meant to:

> Counter the fear brought about by the Soviet military presence in Europe and Northeast Asia not by buildup of countervailing military force, but by relying on United States economic aid to rehabilitate war-shattered economies in Western Europe and Japan, thereby creating the self-confidence that would allow those countries to resist the Russians on their own. (Gaddis80)

This ideology shaped the postwar international policy by introducing new strategies of containment: a new strategic response towards the Soviet Union, the foundation of the Marshall Plan, the global battle against communism and the creation of the CIA (Weiner 21). However, Kennan did not expose his systemic containment strategies in a referential report or document; after WWII, his notion of containment was still employed to suit modern American foreign policy. One of these critical concepts was that insecurity might show in ways other than physical ones and that psychological uneasiness could be readily formed. This unanswered notion was portrayed as the impending burst of fire that military action could not handle. This type of insecurity could be in the form of intimidation, humiliation, or even loss of credibility of the USA in the world (Gaddis 89-90).

Though the NSC-68 was not emancipated to the American community until 1975, this document still embraced all the strategies and containment processes to set the foundation for new U.S. security strategies at home and abroad. This document was debated for supporting militarization; Acheson described it, metaphorically, as a "partisan infighting as bloody as any in our history" since it supported the increase and not the decrease of military spending at that time. However, NSC-68 defined American security policy as a document that set the basis for the realization and adoption of new American policy (Drew 1-6).

1.3.1.4.1. NSC-68 Analysis

The concept of freedom and its implication in constructing a long-lasting societal order was rhetorically explained in NSC-68. The American purpose of this document was to raise awareness about the abridgements of the Kremlin policies to the freedom of societies. The U.S. considered the Kremlin policy and ruling to challenge its morals in a free and peaceful world where individuals can live freely. Furthermore, the consideration of the Soviet regime in NSC-68

to be a threat to American security as they held thermonuclear capacities that could be used against the U.S. This perilous military capability made the U.S. strengthen its air, marine and ground forces face a threat posed by the Soviet Union (Drew 60-64).

The NSC-68 document stated the main ideologies to apply with the Soviet threat. First, the major threat to American security is the Soviet Union. Second, the rivalry that the Kremlin is waging has tremendous negative effects on American status in world politics. Third, the U.S. should be prepared for a military attack led by the Soviet Union, though it was far from happening. Fourth, the political and strategic domination of the Soviet Union in Eurasia would severely weaken the U.S. position. Fifth, the U.S. would seek to decrease the Soviet Union's authority so it would not threaten other nations. Sixth, to bring the Soviet Union in line with the norms of international relations established in the United Nations and, seventh, the U.S. must strengthen its military forces to face the unpredictable threat of communism (60-64).

A free society is respected for its resilience in defending those ideals and ensuring the sanity of these values in a sound environment. To preserve the 'material environment' where these values flourish, the United States ended up considering the Soviet Union not only a threat to its values and the physical capacities providing for these values to Flourish. Consequently, one of the major objectives stated strongly in NSC 68 was to strengthen the military forces of the United States to encounter any threat:

> 1-Thus, we must make ourselves strong, both in the way, which we affirm, our values in the conduct of our national life, and in the development of our military and economic strength.
>
> 2-We must lead in building a successfully functioning political and economic system in the free world. It is only by practical affirmation, abroad as well as at

> home, of our essential values, that we can preserve our own integrity, in which lies the real frustration of the Kremlin design.
>
> 3-But beyond thus affirming our values our policy and actions must be such as to foster a fundamental change in the nature of the Soviet system, a change toward which the frustration of the design is the first and perhaps the most important step. Clearly, it will not only be less costly but more effective if this change occurs to a maximum extent because of internal forces in Soviet society. (Drew 10)

1.4. National Security Policy under Eisenhower (1953-1960): The "**New Look.**"

The President's action was seen as an ideological boost for the National Security Council's ability to make choices and formulate Cold War strategy. Under the direction of the NSC, he founded the Psychological Strategy Board (PSB). One of the primary goals of this agency was to direct extensive strategic study of military operations against the Soviet Union. He also set up the NSC Planning Board, whose members conducted research, made policy recommendations, and drafted preliminary documents for NSC coordination, and the NSC Operations Coordinating Board (OCB), whose members oversaw the implementation of the council's policies (Best 7). The importance of the NSC's regular sessions was bolstered by Secretary of State John Foster Dulles. These met regularly, and in addition to Eisenhower and the other required members, often included the Secretary of the Treasury, the Director of the Budget, the Chairman of the JCS, and the Director of Central Intelligence (7). A greater amount of control over joint staff was delegated to the JCS Chairman by President Eisenhower in 1953.

The Operations Coordinating Board is the second major staff agency of the NSC after the Joint Chiefs of Staff. The OCB "arose like a phoenix out of the ashes of the old Psychological Strategy Board." The Eisenhower administration believed that psychological strategy was

indispensable to national security. The new OCB's main purpose was to act as 'an integrating arm of the NSC in executing all NSC policies (Falk 421). President Dwight Eisenhower placed the NSC at the 'top of the policy Hill' (Stewart 241). He promised a 'New Look' for NS policy. His strategy directed U.S. strength toward Soviet weaknesses with minimal fiscal costs (Hemmer 64).

President Eisenhower had always been ready to use military action against the Soviet Union if they showed any direct or primitive threat to the U.S. Preventive measures and acting unilaterally, as options, were considered a necessity a situation dictates. Eisenhower and Dulles focused on defeating "local communist aggression" like civil wars and conflicts. However, they acted very carefully in dealing with the case of Indochina in 1954, while they rejected intervention under any circumstances to avoid a general war. Nevertheless, the Eisenhower administration emphasized in a determined way that the U.S. "must be determined to take, unilaterally, if necessary, whatever additional action its security requires, even to the extent of general war, and the Communists must be convinced of this determination." In other words, the Eisenhower administration did not want to become mired in the war on the Asian continent. They expressed their willingness to act preventively against communist China without deliberately provoking war. President Eisenhower and Dulles were convinced that this war was a lost cause because the world would be against US intervention in another country (Leffler 399-400).

1.5. National Security Policy under the Kennedy and Johnson Administrations (1961-1968): The Flexible Response Strategy

The Kennedy and Johnson administrations (1961-1968) tended to be more flexible towards the external environment, as this era witnessed a change in both international settings

and advanced technology. The Soviet Union's possession of nuclear weapons made it an unconcealed threat to American dominance in the world, not to mention the Cuban Missile Crisis over the installation of nuclear-armed Soviet Missiles in Cuba in 1962. On the other hand, China emerged as a new power with its assets and capacities. The progressive dispute between Russia and China aggravated the possibility of any anticipatory containment of both forces. The technological advancement in weapons and nuclear arsenals caused the U.S. to reconsider its European strategies (Jordan et al. 51). On top of that, the Soviet Union and China were financially supporting wars of national independence throughout Asia, Africa, and Latin America. It would be hazardous to try to handle all the intricacies by resorting to retaliation, and it would not be very effective anyhow.Thus, technology was no longer the 'panacea' of a successful containment; power was shifting from reliance on nuclear power to investing in military power (51).

Kennedy's Secretary of defense, Robert McNamara, when he came to office in 1961, was committed to re-establishing U.S. military forces. He believed that the armed services should be independently allotted a fair share of the budget; furthermore, these services should be able to develop their programs autonomously within their budget regardless of other services' enactments. Though national security strategies were agreed on in an official document called the Basic National Security Policy, an imprecise manuscript which did not set any specific basis for strategy. General Maxwell Taylor summarized the document's weaknesses: "The sharp issues in national defense . . . have been blurred . . . the Basic National Security Policy document means all things to all people and settles nothing." (Jordan et al. 51).

Since the document did not outline a precise program, each service continued to develop its programs. McNamara made a few changes to the US forces' structure. He sped up

manufacturing of the Polaris submarine-launched ballistic missile, and increased the number of Minutemen intercontinental ballistic missile. Because of the reforms, the Army, Marine Corps, and Air Force all grew. McNamara wanted to swiftly improve and expand the military's fighting capabilities while also formulating a new military strategy (51).

President John F. Kennedy was against using force against the Soviet Union, as it would be a suicidal act. However, at the National Security Council, Secretary of Defense McNamara advised the president regarding the use of force against the Soviet Union:

> "In the many studies I have had done for me," he told Kennedy, "I have not found a situation in which a pre-empt alert condition would be advantageous. Under no circumstances able to get US casualties under 30-million . . . . They can destroy weapons and we can do the same to them. Therefore, pre-emptive advantageous for either side." (Leffler 400).

Accordingly, the measures taken by President Kennedy were more prudent based on strengthening the non-use of military intervention in the Soviet Union, but, meanwhile, Kennedy announced that intervention was not foresworn. Instead, it would be reserved for more insurgencies. Though the emerging threat of China's nuclear capabilities was one of Kennedy's concerns, he desisted further action in this area. He wanted Soviet President Khrushchev to take action to deter China. Eventually, President Kennedy was reluctant to use force against China as it was not a good alternative for fighting the emergence of China as a communist nuclear threat (400).

The Kennedy administration enlarged the military forces to absorb any strike and to be able to respond immediately. These advances gave the president the power to respond to challenges with the appropriate forces; the 'flexible response' strategy provided policy decision-

makers with a strategic nuclear posture to deter any strike or attack. The modernization and empowerment of the armed forces can determine the flexible response strategy's success. Eventually, the U.S. army upgraded from twelve to sixteen divisions; in other words, the United States acquired the capacity to fight many wars simultaneously in different regions of the world (Jordan et al. 52). However, the implementation of the flexible response doctrine faced popular dissatisfaction and economic crisis, especially when the United States installed ground combat troops in the Republic of Vietnam, in 1965 and interfered in civil turmoil in the Dominican Republic, in 1965. Moreover, the doctrine of intervention had no clear establishment and guidelines for use; the essence of intervention and use of force was not determined (52).

1.6. National Security Policy under President Nixon (1969-1974): The Rhetoric of China

Richard Milhous Nixon became a distinct figure in politics in a very short period. After his political successes in 1946, Nixon was elected to the House of Representatives; his victory increased his reputation and nurtured his role in the House. He was known for his hatred of communism 'the communist-hunting member of the Congress. Nixon reached his pick of victory in 1950 candidature to the Senate. He marked the political domain with his famous speech "Checkers", which became a reference to politicians. His famous saying about the "little cocker spaniel dog" given to his daughter: "Regardless of what they say about it, we're going to keep it.", made of him the republican political fighter who will be nominated as the Republican Party's presidential nominee in 1960 and 1969. However, he had a prominent role in deterring communism (Greenstein 92-93); being a vital member of Congress and politically skilled, he ended up in a serious debatable position during his terms of presidency from1969 until 1974, which ended with his resignation (Greenstein 92-93; Gormley 493).

As a President, Nixon called for “an administration of open doors, open eyes, and open minds”; he appointed the Democrat Daniel Patrick Moynihan, his domestic advisor and the conservative Arthur Burns as his economic Counselor. His openness to other political thoughts made his administration open to other political thoughts. However, President Nixon chose his specialized staff, who advised him and shielded him from the other counsels in his administration. He had a very centralized foreign policy; however, he followed the path of President Eisenhower’s experience in debating issues with his NSC, and he needed to be more committed to the decisions made in his Council. Instead, Nixon made his foreign policy and national security decisions with his special assistant in national security, the Harvard scholar in international relations, Henry Kissinger (Greenstein 99-100).

Nixon’s presidency was loaded with complications and paradoxes. In his Address to the nation, he denounced his readiness to end the turmoil and take the country to a valley of peace: “to lead the world at last out of the valley of turmoil and onto that high ground of peace.” He addressed the Kremlin in his first week with a very expressive message enunciating that the true power is not to struggle for leadership and prominence but to gain more power for the only sake of security to secure the nation’s territory, citizens, and interests. The president also reached out to the Vietnam President Nguyen Van informing him that the U.S. would withdraw from Vietnam (100). Eventually, President Nixon planned to inaugurate new terms in international relations and foreign policy; when he publicized these decisions, he initiated a new strategy. The historian John Lewis Gaddis saw it as a “complex, subtle, and closely interwoven strategy like that of Nixon and Kissinger required, for its implementation, precise coordination and control” (Gaddis 299).

Unfortunately, the Nixon address cherished by the American public did not find its way to the peace agenda of the Nixon administration. In 1970, President Nixon deployed American troops to Cambodia to deter Communists in the area (Greenstein 101; Gaddis 338). Though he openly confessed, “we respect Cambodia’s neutrality,” he dispatched troops to fight in Cambodia to prove that the United States is a strong country that cannot be defeated as a “pitiful helpless giant,”. Bombarding Cambodia led not only to new unprecedented congressional decisions in response to broadcasting his announcement of attacking Cambodia from the Oval Office but also ignored the protocol of reporting the decision to the Pentagon as a military act (Gaddis 338). Furthermore, President Nixon’s decisions led to chaos in the country when students all around the country manifested; four students were killed at Ohio’s Kent State University by the national guards, a “nationwide paroxysm”, as Greenstein put it, spread out all over the country. President Nixon was forced to soften his policy and retrieve his outburst plans; he stated that he withdrew 115,000 troops from Vietnam and ordered the removal of 150,000 troops sooner (Greenstein 100).

An unprecedented protest intensified against the war pushed Congress to react against the war in Cambodia and stop the bombing in August 1973. Unsatisfied by President Nixon’s abuse of Executive power, Congress took a bolder action by passing the War Powers Resolution in November 1973. The War Power Act, as it is referred to, was an obligation; the president was compelled to inform the Congress of any military action within forty-eight hours before he took action. Furthermore, the Act obliged the president to withdraw military troops within sixty days unless Congress allowed him an extension. The president wanted more than this resolution, as it gave an overhead plan to the enemy forces to plan for their aggression in the regions as they already had an idea of the preliminary strategy of the American forces, said Nixon. He saw the

Congress Act as an obstacle to any president's power. Indeed, Congress passed the Act of War to curve the president's entangled use of power in the war in Vietnam; in addition to the public opposition to the President's decision, Congress found it an obligation to stop the growing authority of the president over the Executive Branch with total denial to Congress assents (Gormley 497-498).

1.6.1. The Nixon Doctrine in China and Vietnam

"A statesman" was an achievement that President Nixon wished to reach as a title during his presidency. He was passionate about foreign policy, though its history was not a bright side of his career as a president. Though he ended the Vietnam War and normalized U.S. relations with China, what was underneath his policy overwhelmed his successful part (Bostdorff 31). Nixon declared a new agenda for his new foreign policy in January 1969. His foreign policy was known as the Nixon Doctrine, as it underlined the pathway of his foreign policy toward the Vietnam War and China/US relations. On July 25, 1969, in his conference in Guam, after his public speech and comments, President Nixon's doctrine manifested in ending the war in South Vietnam and withdrawing 70,000 of the American troops from Vietnam, as the first step of a final withdrawal, under the slogan of "Vietnamization" (Gaddis 296; Kimball 60-65). In expressing the danger of "National Communism" in Vietnam, President Nixon admitted that the US played a tremendous role in containing communism in the region. He stated that Vietnam had "imposed severe strains on the United States, not only militarily and economically but socially and politically as well" (Bostdorff 41).

President Nixon stated in his writings that the United States would no longer react unilaterally against communism in turbulent regions in the future, "other nations must recognize that the role of the United States as world policeman is likely to be limited in the future"

(Bostdorff 41). The withdrawal of the American forces from Nixon and Kissinger's perspective should be considered a positive change in American foreign policy strategy towards this region in the Pacific. Nixon and Kissinger's smart move was to convey a strategic message to their adversaries:

> The fifth major element of their strategy—can be found in this technique of covering strategic withdrawals with tactical escalations: the idea was to show that the United States could act if it chose to and thereby create questions in the minds of adversaries as to whether it would or not . . . became a deterrent . . . "retaliation" strategy. (Gaddis 297)

Nixon and Kissinger agreed that President Johnson deeply involved the United States in the Vietnam War. However, Kissinger believed that the war in Vietnam should end; he narrated that to a group of university presidents in 1972. He showed his concerns "We think . . . that it is important for the health of the society and the stability of the international system that we get out with some dignity", The strategy of unpredictability was the instrument of Nixon and Kissinger's strategy in ending the war in Vietnam with "dignity" and "honor". Both Nixon and Kissinger were more worried about the credibility of the United States and its commitment to providing security to its allies and the American self-confidence that: "would suffer irreparable harm" if it was not well preserved. As Gaddis described, it was a distinctive approach to isolate and centralize the policy decision under their main power, the Executive Branch (Gaddis 299).

Nixon and Kissinger had different perspectives on the applied strategy toward the war in Vietnam. Nixon supported the use of force rather than negotiations, whereas Kissinger preferred negotiations; he was the leader armor of negotiations for President Nixon as he was Nixon's negotiator. Eventually, the purpose of Kissinger and Nixon's strategy was not focused only on

ending the war in Vietnam with honor; the real honor for them was to win the negotiation intended to keep Saigon ruled by President Thieu. President Nixon and his Counsel had a different policy from their predecessors; that is how they saw it. The Nixon doctrine for Vietnam's "Vietnamization" was not an approach to sustain the American hegemony; rather, it was an implementation strategy aimed at compelling the adversaries to accept their policies (Kimball 66-67).

The rhetoric of Nixon's strategy in foreign policy showed new terms and a foundation for a new policy. These changes were interpreted in a foreign policy report published in 1970 and 1971 under the Nixon administration. The report discussed in detail the imperative adaptation to the U.S. American Foreign policy with the world policy's changes. According to the 1970 Report addressed by President Nixon to Congress: "The postwar period in international relations has ended" (197), the communist threat has lost its vitality, and it is no longer the US's responsibility to secure the Asian territories anymore; instead, Nixon's showed the emergence of the Asian allies to protect themselves. The President stressed the importance of negotiation with Communist countries such as the People's Republic of China.

Undeniably, approaching the People's Republic of China (PRC) was President Nixon's second target in pursuing the pathway of his doctrine and the rocking move in his foreign policy strategy. His opening to China and re-establishing mutual relations between the two countries affected the direction in which Nixon's policy may be directed afterwards. His visit to China in 1971 was American diplomatic policy's most unexpected presidential Act. On July 15, 1971, President Nixon broadcasted his willingness to seek the normalization of relations between the U.S. and the PRC. President Nixon welcomed this surprising initiation in both Houses and public opinion. It was interpreted as a smart policy move. In support of Nixon's visit to China, the

democrats: Senate Majority Leader Mike Mansfield and former Vice President Hubert Humphrey, solicited the idea, and so did Republican leaders Barry Goldwater and Hugh Scott (Bostdorff 32).

Kissinger and his deputy Alexander Haig initiated a few secret visits to China in 1971 and 1972 before the presumed visit of President Nixon in February 1972. The American representative in China introduced the U.S. foreign policy and strategy to the Chinese, composed of key elements undeniably primordial to the American coexistence and cooperation with other countries, including the PRC. The major elements that were explained were: the American strategy in foreign policy was a realistic strategy that served U.S. interests; the strategy stood against any hegemonic conflict of supremacy and supported the PRC to stand against any country that threatened its security and hegemony, such as the Soviet Union (Goh 478-482).

In his rapprochement with the PRC, Nixon affirmed that the United States was looking for a harmonized relationship between the USSR and PRC. The President reaffirmed the American nonintentional conspire with the USSR against PRC, neither looking for an ally to stand against the USSR. Instead, he emphasized that Washington would sponsor any goodwill attempts to create better relations between the Soviet Union and China. As Kissinger's staff clarified to the Chinese Government, the U.S. would be reluctant to embrace an "overt pro-PRC policy" for the major "big concrete business" it had with the Soviets. Furthermore, the Washington-Beijing relations were relatively new to embark on a total PRC policy endorsement. President Nixon and Kissinger were planning to rise the Chinese expectations in the Sino-American opening relations; However, it looked like rhetoric created to serve the moment; President Zhou responded that they had no opposition to a well-established relationship between the USSR and the US (479).

According to Kissinger's model of triangle politics, the Americans would not benefit from a better Sino-Soviet relationship; it was true that the U.S. sought a better relationship with PRC but never wished for a better relationship between PRC and USSR. Kissinger believed that the U.S. would advantage from the new rapprochement with the PRC only if Beijing and Moscow considered each other rivals. The Kissinger/Nixon strategy toward China was to convince the leaders of China that the U.S. would be a close friend to Beijing and that it would never be part of any conspiracy against China. Eventually, Kissinger, in the opening meeting, expressed the U.S. intentions for a mutual exchange of benefits and interests and that the "the United States and China had "no conflicting interests at all" in great power relations, the United States would be "your supporter and not your opponent" (Goh 480).

1.6.2. The Watergate Scandal

President Nixon was about to start his second term and was involved in the Watergate Scandal. The scandal overwhelmed the last two years of the Nixon administration. Congress was on the stand during the second term of Nixon; they wanted to ensure that the president would not abuse presidential power. This period in Nixon's presidential term and the Congress scrutiny marked that period's political, foreign policy, and executive decisions. After he visited China in 1972 and the summit meeting with the Soviet Union, President Nixon ended by signing a treaty defending any production of the antiballistic missile system. A few weeks later, after the President's Soviet visit, a security guard at the headquarters of the Democratic National Committee caught four burglars at the HQs in Washington D.C. the unexpected happened; one of the arrested Burglars, was a member of Nixon's second presidential election, an incident that would convict Nixon's involvement in the scandal (Greenstein 102-103; Gormley 499-500).

The scandal was a scoop; for the media, the president criticized the scandal and denied White House involvement by claiming that the White House has no role whatsoever in this specific issue. as was mentioned in the June 22, 72 Presidential Statement. However, the closest members of his administration and counsel were involved in the Watergate affair. The campaign manager, John Mitchell, and Attorney General Richard Kleindienst resigned, White House Counsel John Dean was fired, and Chief of Staff H. R. Haldeman and Chief Domestic Advisor John Ehrlichman were prosecuted for participating in a cover-up of the affair (Gormley 500). Nixon hired the highly esteemed Elliot Richardson as the attorney general; on the other hand, Richardson appointed Archibald Cox to inspect the Watergate scandal and find the underlying cause of it. (Greenstein 104).

The Watergate affair grew wider and involved other political figures, including President Nixon, who could not escape the scandal. Surprisingly, the Senate Committee found out the existence of the president's recorded tapes. The president was asked to hand over the recording tapes of the White House recording system, but Nixon refused to hand over the tapes to U.S. District Judge John J. Sirica (Gormley 500). Cox ordered the president to hand over the tapes, but the president refused and denied the justice accessibility to this right according to the principle of separation of power. In a "Saturday Night Massacre", as it is known, President Nixon ordered Richardson to end the duty of Cox; Richardson disobeyed the president's order and resigned from his position. The president made it the mission of Robert Bork, the third official in the Justice Department, and he did. By dismissing Cox, the president created a public disorder that was not calmed only when he released the transcripts of many tapes (104).

Nixon released the transcripts of the recommended tapes on April 30, 1974, but insisted on keeping the recorded tapes claiming that he had nothing to hide in these tapes (Gormley 501).

The case of the tapes reached the Court in the spring of 1974 when the president's counsel, James St. Clair, proclaimed that the Court had no jurisdiction over the case as long as the president was in power. James St. Clair asked the Court for fair constitutional conduct in the case. He saw the impeachment as an alternative to be dealt with as a congressional matter but not to convict the president or diminish his power as long as he was in office. The Council insisted on considering the matter as a 'political question' and waiting for the House decision concerning his impeachment. From a narrow angle of St. Clair president's defense, Nixon has the right to keep the tapes as they represent and contain secret information and communications related to his power as the executive chief, the right to protect the tapes, put it St. Clair "constituted an overriding public interest; such materials, he maintained, required confidentiality" (Gormley 501).

Though the president's counsel St. Clair tried to influence the Supreme Court decision in the case of Watergate and the involvement of Nixon in the recorded tapes affair, both Nixon and St. Clair knew that they could not defy the Supreme Court decision in the case matter (502). The Supreme Court Committee voted for impeachment, but the House and two-thirds of the Senate voted for his resignation from office. After losing his supporters in the Committee after the *United States vs. Nixon* case, Nixon found himself obliged to leave the office deliberately. On July 24, information was deducted from the original tapes: "smoking gun" proving Nixon's guilt in a cover-up of Republicans involved in the Watergate scandal. An act that made the Judiciary Committee regret not voting for impeachment for such a criminal act (Greenstein 103).

In his address to the nation on August 8, 1974, President Nixon announced his decision to resign as President of the United States. He expressed himself and was willing to leave the office for the main interest of the United States, as he could no longer exercise his powers as a

President, especially after the Watergate incident, which convicted him tremendously in Congress. President Nixon addressing the American people, said:

> Throughout the long and difficult period of Watergate, I have felt it was my duty to persevere, to make every possible effort to complete the term of office to which you elected me. In the past few days, however, it has become evident to me that I no longer have a strong enough political base in the Congress to justify continuing that effort. . . to leave office before my term is completed is abhorrent to every instinct in my body. But as President, I must put the interests of America first. . . Therefore, I shall resign the presidency effective noon tomorrow. (Nixon, "Address to the Nation Announcing Decision... 1974)

Richard Nixon and Kissinger's foreign policy and approach to securing American international security and interests differed from previous Presidents. Regardless of what he inherited from the White House "Watergate scandal" and his tempered character, and bold and vindictive personality, President Nixon left touch and contribution to changing the path of American foreign policy. Together with his brilliant strategists Henry Kissinger, they reoriented American diplomacy toward powerful relations with superpowers; they contained, in a different way, the Soviet Union using a new strategy based on the peaceful constraint of military power and diplomacy made through coordination and mutual exchange of interests. As they planned for diplomatic coordination with superpowers and prioritized relations over other aspects of foreign policy, President Nixon and Kissinger regarded both USSR and China as two great powers rather than two ideological enemies of the US. As a result, of this interpretation of the strategy, there would be a possibility to reconsider the US/ PRC/ USSR relations. This new paradigm in American foreign policy was a step forward to change the perception of the other ideological

powers in American foreign policy, a policy that was ignited under Nixon's presidency (Dueck 142-155).

1.7. National Security Policy under the Carter Administration (1977-1981): Reassessing NS

The Soviet Union was growing more powerful in nuclear forces, which pushed President Carter, after taking office in 1977, to ask his administration for immediate reconsideration of national security policy. The appraisal of the two powers, China and Russia, led the Carter administration to reassess the international policy of the U.S. The emergence of Soviet nuclear capability marked a turning point in international policy as the most prominent power, and the People's Republic of China was the main nuclear danger. The U.S. saw the importance of arms control for international dynamics. In addition, the new administration was very suspicious of how the U.S. and the USSR had interpreted the notion of 'détente', which aimed to weaken the clash between superpowers at the global level. However, the USSR interpreted this 'détente' as a laissez-faire policy, allowing it to extend its sphere of influence.

Many factors structured the international environment and paved the path to reassess and regulate the stability of nuclear powers worldwide. The continuous growth of the nuclear and military empowerment of the Soviet forces, the development of technology, and the invention of multiple new nuclear weapons, such as cruise missiles and antisatellite capabilities, threatened the stability of the conventional force balance between the U.S. and the Soviet Union. Consequently, as a reassessment of the mutually developed strength of the U.S. and Russia, in 1977, the Carter administration set up its main guidelines for a new strategy in the form of announcements and initiatives. It stressed the necessity of stable nuclear power in the world and continued to depend on 'mutually assured destruction as a deterrent to nuclear conflict. In the

context of essential equivalence, in 1979, President Carter and Secretary Leonid Brezhnev signed a treaty in Vienna to define the upper limits of essential equivalence (Jordan et al.52).

The Carter administration strongly approved the SALT II treaty talks to limit the total of both nations' nuclear forces to 2,250 delivery vehicles and to place restrictions on installing strategic nuclear forces. Though the U.S. Senate did not ratify the treaty, the United States continued to use the terms of this treaty as an instructive document of essential equivalence. The United States also paid more attention to the Persian Gulf by creating a healthy atmosphere for American-Soviet relations. The Carter administration started a soft diplomatic relationship with the People's Republic of China, which appreciated the act of the Carter administration. The harmonized new relationship was represented by the visit of Deng Xiaoping to the United States in 1979 (52).

However, the 1970s ended with an unexpected act of military aggression: the Soviet invasion of Afghanistan. The Kremlin's main purpose for invading Afghanistan was to stop the United States from approaching a geostrategic location like Afghanistan and use it as a locale to watch and threaten Soviet territory. Though Afghanistan played an important role in the East-West competition, the Soviet Union was not eager to occupy Afghanistan or to stimulate a socialist revolution, not to mention the impossibility of controlling the tribal composition of this country. The main objective of the Kremlin's invasion was to deny the U.S. access to this geostrategic location. However, the Soviet invasion of Afghanistan embraced the Russian triumph of communism. It marked the beginning of the end of the Cold War: "The Soviet Union could have collapsed even if the intervention had succeeded or had never been attempted. However, the ten years of occupation and war that followed the invasion took an enormous toll,

adding to the economic exhaustion and strain of empire from which the Soviet Union was beginning to buckle" (Gompert et al. 129).

Even with very calculated strategies set by the Kremlin policymakers, the invasion was 'counterproductive'; the Soviet Union entered this East-West competition unprepared for the exhausting military engagement in Afghanistan and, in comparison, to American military spending, which grew from 155$ billion in 1979 to about 400$ billion in 1989 the year the Soviet Union finalized its withdrawal from Afghanistan. Consequently, the conventional military buildup of the United States is incomparable to the devastating Soviet military loss in Afghanistan (Gompert et al. 130).

1.8. National Security Policy under the Reagan Administration (1981-1988): The Structural Review of the Pentagon

1.8.1. The Goldwater-Nichols Act of 1986

The Packard Commission, a federal government commission by President Reagan, was created by executive order 12526 to study several areas of management functionality in the U.S. Department of State. The Commission recommended a package of reforms to meet the deficiencies the Pentagon suffered from at the time. Officials and military leaders were convinced that the Pentagon's structure should be reconsidered as it was no longer meeting the needs of its operational design. The idea was confirmed by the Chairman of the Joint Chiefs, David Jones, who confessed that the Pentagon had neither an effective operational structure nor an effective strategy to stand against the challenges that the Department of Defense faced. The Armed Services Committee engaged in a structural review of the Pentagon. Eventually, Congress came to the vital conclusion that the Department of Defense, as it was organized at that time, was

structured fundamentally to serve and prioritize military services. The absence of inter-department cooperation led to failures in leading operations (Quinn 9).

By 1980, it was very clear that the system of the Department of Defense was not productive and suffered from insufficiency, prioritization of the military interest over the other joint forces, a very weak position of the Chairman and a very weak Joint Staff. The Goldwater Nichols Act addressed these problems by:

> Making the Chairman, rather than the collective Joint Chiefs of Staff, the principal military advisor to the President, creating the position of Vice-Chairman of Joint Chiefs of Staff, making the Joint Staff responsible to the Chairman of the Joint Chiefs of Staff, and creating career incentives for officers to acquire experience working in joint environments. (11)

The Goldwater-Nichols Department of Defense Reorganization Act of 1986 is considered the most inclusive defense reform bundle since the National Security Act of 1947. This Act was the fourth major revision of the National Security Act of 1947 and the third post-WWII reorganization of the DoD. One of the new and potentially far-reaching changes contained in the Goldwater-Nichols Act was the requirement for the President to submit an annual report to Congress detailing the NS strategy of the United States (Bartolotto 3). The Act required the President to submit an annual NSS report to Congress containing a very detailed and precise description of the following:

- The United States' international interests are vital to its NS.
- US international engagement and potential in foreign policy and defense against threats to its security and what its NSS required for implementation.

- Short-term and long-term uses of the nation's elements of power to endorse the interests and secure its global achievements·

-An evaluation of the balance among the U.S. capabilities of all elements of national power and NSS.

- Each NSS report shall be transmitted in classified and unclassified forms (Reilly 4).

In his second 1988 NSS document, President Reagan signalled a transition period in international security affairs. The transitional period was marked by the emergence of the Soviet Union as a strategic and superior power in Eastern Europe with an escalating influence in unstable third-world regions. The massive build-up of the Soviet Union's military forces by 1980 was estimated at 15 to 17% of its annual GNP, providing the Soviet Union with a quantifiable force and an internationally deployed navy. Consequently, this Soviet military advancement was considered a pivotal point for U.S. NSS and a growing threat to American security and its allies for years to come (A National Security Strategy 1988, 7).

In conclusion, the evolution of U.S. national security policy from 1940 to 1989 was marked by significant shifts in focus and approach. From the early days of World War II, when the country was focused on the fight against fascism, to the Cold War era, when the U.S. had to contend with the threat of nuclear war, to the Reagan years, when the U.S. sought to reassert its global leadership and end the Cold War, U.S. national security policy has been shaped by a variety of forces and considerations. The changes in U.S. national security policy over the past decades demonstrate the complexity of the international environment and the importance of responding to it with an informed and thoughtful strategy.

Chapter Two:

National Security Policy: A New Policy for a New Century (1990-2009)

The United States of America has an art of employing strategies and ideologies that emerge to be the source of its predominant status in the world. The Bush and Obama foreign policies surfaced to frame the American policy of the 21st century as it appeared to be a different path than previous U.S. president. Both presidents launched a new national security policy doctrines. The Freedom Agenda, or "Bush doctrine," was a manifestation of a new turn in U.S. foreign policy, which emphasized full-scale militarization and unilateralism to defend the U.S. hegemony in the world. The Obama Doctrine, on the other hand, was a soft power policy that shifted gradually from adopting the "Superpower and leadership" ideology to the "Balance of power and partnership" ideology. In addition to the Obama and Bush doctrines, this chapter discusses presidents George H. Bush and Bill Clinton's policy towards national security and how they contributed to changing U.S. grand strategy in the 21st century.

2.1. National Security Policy under President George H. W. Bush (1989-1992): A New Policy beyond Containment

"As Commander in Chief, I can report to you our armed forces fought with honor and valor. And as President, I can report to the Nation aggression is defeated. The war is over".

GEORGE H. W. BUSH, ADDRESS BEFORE

A JOINT SESSION OF CONGRESS ON THE

CESSATION OF THE PERSIAN GULF CONFLICT,

March 6, 1991

George Herbert Walker Bush Presided in a period torn between an inherited legacy of Reagan politics to be accomplished and a transitional phase as the Cold War ended. Two

diverging and challenging directions to his first year in the White House. He was elected the 41 President of the United States (1989-1993). He served as the Vice President of President Reagan for eight years, which postured his tight connection to Reagan's political policy, leadership management and conservative values. George Herbert Walker Bush was a President for one term after losing the second term to Bill Clinton in 1992; he is still remembered as an internationalist and a skilled president in preserving America's foreign policy supremacy (Gormley 558).

The president's political career was marked by the outstanding positions he served the country with, from the youngest navy pilot during WWII to the Vice president of President Reagan. In between, President George H.W. Bush served as a member of Congress, as a VIP diplomat in China and as the head of the CIA. This military and political career made him one of the most qualified presidents in foreign policy in American history. President George W.H. Bush was an internationalist in his policy; he sought to spread democracy in the world without any risk of war; he was named the "Guardian of Reagan's legacy" as he believed in peace and international democracy (Greenstein 429).

President George H. W. Bush senior was a wise president in managing the country's policy decisions; he was more allied with the federal government with much reliability on his council's experience in policy decisions. Though most politicians and analysts believed President Bush senior was following President Reagan's agenda in foreign affairs and politics, Bush viewed many of Reagan's policies as non-matching with the new international arena and saw alternatives to those policies, including his conduct with the Soviet Union (Dueck 236).

2.1.1. The End of the Cold War

Bush senior believed that Reagan's policy towards the Soviet Union was waved from a challenging policy in his first term to an engagement policy with a submissive belief in a Russian

American friendship led by Mikhail Gorbachev. Alternatively, President Bush believed that successive international relations between superpowers should be based on a realistic policy. By entering the White House, the president halted any act of détente against the USSR (Dueck 236). As Reagan's Vice President, Bush was against President Reagan's premature statements about the anti-Soviet Union. In his first term of presidency, the anti-Soviet Union of President Reagan suddenly changed to a warm sympathy and enthusiastic readiness to resettle U.S./USSR relations. Another disquiet issue that pushed Bush to be more skeptical about the intention and the readiness of both presidents Mikhail and Reagan was how far they intended to settle the U.S./USSR turmoil that lasted for more than four decades (Greenstein 164).

After taking office On January 20, 1989, President George H. W. Bush resumed negotiations with the Soviet Union in May 1989. He suggested "sweeping cuts in NATO and Warsaw Pact forces in Europe" (165). Eventually, the Cold War trajectory went through unexpected changes, especially in the countries of Eastern Europe that revolted and forced out the communist government. By 1989, the communist supremacy in Poland, Hungary, Bulgaria, Czechoslovakia, East Germany, and Romania had been replaced by free governments. Unprecedently, the changes that took place in Eastern Europe affected the Soviet Union's powerful position in this area and weakened its chances of remaining among the first military powers in the world. The Soviet Union, led by Gorbachev, was considered to revive the political deal proposed by President Bush (165).

President Bush senior handled this rapprochement with wisdom and expertise in dealing with international affairs and perilous circumstances with flexibility and professionalism. In his first summit conference with Gorbachev, President Bush senior conveyed a message through his conference on the U.S. and Soviet naval warships of Malta. He smartly set the foundation for a

stable and recognized relationship with Gorbachev; his engagement with the Soviet leader was more neutral, with a steady caution not to embarrass or triumph over the unification of Eastern and Western Germany and the fall of the Berlin Wall in November 1990 (Greenstein 165). The mutual relations grew up to reach other domains, such as the military domain, when President Bush and Gorbachev met on July 31, 1991, in Moscow to sign the Strategic Arms Reduction Treaty (START I). They limited the number of warheads in both countries to six thousand. Furthermore, the United States prioritized the Soviet Union/ U.S. commercial relations and ranked them as the best trade relations (Dueck 236-246).

In a short period after the Berlin Wall collapsed and the START I agreement, the Soviet hard-liners launched a coup against Gorbachev; the ill-conceived coup failed, and the leader Gorbachev regained his position again. He was very committed to ending the communist political party's influence and hegemony on the Soviet government. Eventually, Gorbachev ended this monopoly and gave freedom to the Baltic states. By December 1991, the Soviet Union no longer existed, and the former USSR parted nations (236-246). December 31, 1991, marked the end of the Cold War and the fall of the former communist USSR, a turmoil of diplomatic, political and military relations that lasted for more than four decades. As a recognition, President George Herbert Walker Bush triumphed the American foreign policy by disbanding the Soviet Union in1991, ending the war in Kuwait after the American military victory in Operation Desert Storm in 1991, and the crumbling of the Berlin Wall in 1989 with the unification of eastern and western Germany (Dueck 236-246).

2.1.2. The Gulf War

The Middle East was unstable; President Bush senior inherited a barbed relationship with Iraq from President Reagan onwards. The long Iraq bloody war with Iran made it a crucial

problem in the American international sphere and a major threat to American interests in the Gulf region and the Middle East. The U.S. ambassador David Newton put it plainly in 1985 that "an Iranian victory would have been catastrophic" for American interests in the Persian Gulf. He also confirmed, "The longer the war drags on, the more likely an Iraqi collapse becomes". That may hit American interest in the area; heavily. Victorious Iran will bring another dominant power to the Gulf region, including total control of oil, the dominance of Iraq and undertaking a few governmental regimes such as Kuwait and Bahrain. Newton asked the White House for immediate support to the Iraqi government and provided President Saddam Hussein with military equipment, satellite pictures on an Iranian basis and war settlements (Little 64-69).

Surprisingly, in parallel with the U.S./Iraqi exchange, the White House conducted secret negotiations with Iran for the release of seven American hostages held in Lebanon by Iranians; the deal of releasing the hostages was conditioned with the selling of antitank missiles to Iran to use them against Iraq. It was surprising news to the Iraqi President of the American double standards and betrayal of their mutual relations. Saddam Hussein branded the Americans as 'Conspiring bastards. He never regained his trust in American Government and believed the Reagan Administration would coalesce with the Iranian government against Iraq. Though Iraq emerged after winning the war on Iran as the supreme military power in the Persian Gulf region, still, it was a very important equation to settle for a harmonious US/Iraqi relationship in the area (Little 64-69).

In 1989, Georg H.W. Bush's team communicated the existence of a quasi-relationship between Iraq and the Soviet Union. It was not an easy decision for the Bush administration; whether to consider Iraq a 'distasteful dictatorship to be shunned' or to recognize its potential as "a more responsible, status-quo state working within the system, promoting stability in the

region." The president and his administration were convinced that Iraq was undeniably the strongest military power in a turbulent region of the Persian Gulf but a partner to the US. Bush spent more than nine months drafting the U.S./Iraqi political policy that may secure a beneficial and mutual partnership (64). In October 1989, the president passed the National Security Directive NSD-26, which dictated the new policies that would normalize and moderate Iraqi/U.S. political relations. The NSD-26 was set to "promote stability in both the Gulf and the Middle East" and to generate "opportunities for U.S. firms to participate in the reconstruction of the Iraqi economy, particularly in the energy area". By adhering to these incentives set by the U.S. government, American Iraqi relations would be based on more economic and energetic beneficial exchanging rather than a susceptible fragile relation threatened by military intervention.

A checkered movement took place in the Middle East and the Persian Gulf where American interests were fatally threatened, especially after the U.S. unstable supply of oil and the insurgent attacks of Saddam Hussein on Kuwait on August 1991: an American ally located between Iraq, Saudi Arabia and the Persian Gulf. As a reaction to this belligerence, President Bush senior deployed more than 100,000 troops to Saudi Arabia in what was known as 'Operation Desert Shield' in 1990. Using his skillfulness in foreign policy, Bush convinced the United Nations to support the U.S. military intervention; by November 1990, the UN authorized the U.S. intervention in Iraq to remove all Iraqi forces from Kuwait. The president declared to Congress that the intervention was not meant to be a military intervention under war terms; instead, it was meant to protect Saudi Arabia, the ally of the U.S., from any Iraqi aggression in the area. Though the president made it clear that issuing a buildup without Congress's

permission was only a measure of protection and not a declaration of war, few members of Congress still consider his act unilateral (Gormley 563).

With congressional and UN approval, President Bush senior was authorized to use military forces against Iraq to force its armed forces to withdraw from Kuwait. The president strongly believed in his authority as a Commander in Chief of the Armed Forces of the United States, which enabled him to take necessary measures to secure the countries' interests abroad. Based on this conviction, on January 14, 1991, President Bush senior issued and signed a statement that gave him the right to declare war when American interest was at stake. Three days later, on January 17, 1991, President Bush senior ordered the U.S. forces to attack Iraq. This air forces operation was called 'Operation Desert Storm'; the operation undertook modern measures and tactics of warfare using new sophisticated arms to hit the Iraqi forces. After a month of attacks on the Iraqi forces, the U.S. troops liberated Kuwait. The President, feeling his mission ended by securing Kuwait and his ally Saudi Arabia, decided to withdraw and ordered a cease-fire on February 27, 1991 (Duck 236-246, Greenstein 167).

President Bush senior never intended to overthrow Saddam Hussein before the cease-fire; he had no national or international authorization for toppling a government, especially without the consent of the UN, which ordered the liberation of Kuwait with fewer casualties (236-246, 167). The president believed the Iraqi people would overthrow Saddam Hussein. The President saw the danger of an Iraq potential in the Iranian hands as a threat to American interests and a fatal weapon against their Israeli allies in the region. President Bush senior was criticized for not ordering the American forces to overthrow Saddam. However, he intelligently avoided any negative and misinterpreted intervention in the Persian Gulf because he was convinced there would be no benefit from invading Iraq (Dueck 236-246).

2.2. U.S. National Security Policy under the Clinton Administration (1993-2000): The Beginning of American Primacy.

2.2.1. National Security Strategy of Engagement and Enlargement

The first NSS Report published in June 1994 by the Clinton Administration represented the first concept of U.S. security strategy after the Cold War to reconsider international physical security in the changing global landscape. The Clinton administration's reestablishment introduced changes to the American ideology and process for its final goals and achievements. It also established the three central goals found in all seven Clinton Administration NSS Reports: the credibility of sustaining American security with military forces, support for America's economic revitalization, and promoting democracy abroad. Eventually, the 1994 Report reveals the emergence of a new era: "the end of the Cold War and the dissolution of the Soviet empire brought about a radically transformed security environment" and a "corresponding period of great promise, but also great uncertainty."(A National Security Strategy of Engagement and Enlargement 1994).

Interests through Engagement and Enlargement is a vigorous section in the 1994 Report. This part of the strategy determines the diplomatic approaches and the administration's philosophy. The Clinton administration prioritized preventive diplomacy and selective engagement as the primary tools for achieving U.S. goals and objectives. The uncertain threat to American security marked the beginning of vulnerable security at home and abroad. The Report stated that "protecting our people, our territory, and our way of life" will be the main objective of US National Security, as well as taking advantage of "opportunities to make the nation safer and more prosperous". Using the dual strategy of preventive diplomacy and selective engagement, the 1994 NSS report met the intent of the Goldwater- Nichols Act by providing a 'grand

strategy' that was the ultimate goal of U.S. policy after the Cold War. As defined by Colin Dueck, 'Grand strategy' involves a self-conscious identification and prioritization of foreign policy goals; identification of existing and potential resources; and a selection of a plan which uses these resources to meet those goals" (Dueck 512).

For the Clinton administration, the resolution was to "create a more secure, prosperous and democratic world for the benefit of the American people". To accomplish this objective, the Clinton administration came up with the following agenda:

-First, "secure peace; deter aggression; prevent, defuse, and manage crises; halt the proliferation of weapons of mass destruction, and advance arms control and disarmament".

-Second, "expand exports, open markets, assist American business, foster economic growth, and promote sustainable development".

-Third, "protect American citizens abroad and safeguard the borders of the United States."

-Fourth, "combat international terrorism, crime, and narcotics trafficking".

-Fifth, "support the establishment and consolidation of democracies, and uphold human rights".

-Sixth, "provide humanitarian assistance to victims of crisis and disaster".

-Seventh, "improve the global environment, stabilize world population growth, and protect human health" (Leffler, "9/11 and American Foreign Policy"397).

In sum, the Clinton agenda was similar to other presidents in general terms; however, Clinton focused more on humanitarian intervention to boost human peace and aid countries suffering from regional conflicts and disasters. His policy was more humanitarian (Leffler, "9/11 and American Foreign Policy"397).

2.2.2. The Project for the New American Century

After the election of Bill Clinton, the neoconservative elites supported the Clinton administration to advance American primacy in the world. They formed organizations and lobbied to advocate this main objective. These neo-conservative thinkers published books and articles on *The Project for a New American Century (PNAC)*. The 2000 report on *Rebuilding America's Defenses* was an outcome of a long struggle to implement the PNAC. Rebuilding American military strength was seen as a primordial objective of the American security system because the hegemonic role the U.S. gained from the Cold War would not be an everlasting position; instead, the U.S. should develop its military strength and political position in the world. The PNAC plan was an overt determination to afford continuity of Cheney's defense department planning in the first Bush administration entitled 'The Defense Policy Guidance'. This guide was drafted in early 1992 and provided a concrete proposal for maintaining U.S. pre-eminence in the world (Dalby 4-11).

The priority in the PNAC document was homeland security. However, spreading democracy around the world was more entrenched in this document. American prosperity was more about a new world system with no regional conflicts. The enemy of American security was no longer the Soviet Union; the post-Cold War era saw a new rivalry in Asia. This latter was a new geographic and geopolitical terrain for U.S. defense policy, requiring a new strategy for the new category of challenges and oppositions. The PNAC did not focus on terrorism as a major threat to American defense power; the focus was only on rival states and ignored foes that manifested as non-state actors, a threat that passed unnoticed. Eventually, the PNAC document focused on military revolution and reinforcing American technological capabilities to face the forthcoming threats to American national and international security (Dalby 4-11).

Drawing on the historical and institutional development of American national policy and its strategic adjustment would clarify existing policies and their implementation in national and international dynamics. The United States policies have shifted from a state of the cold war to a state of supreme policy. The emergence of the U.S. marked this as an unrivalled power after the fall of the Soviet Union. The enemy of the U.S. was no longer the Soviet Union, and new challenges appeared to be more lethal than the Russian threat, like the superpowers arising in Asia, Iran, and the Middle East. The U.S. took the lead in entrenching a new policy for a new dynamic in the world system to spread freedom and democracy. However, the focus of American national policy and security has always been on rival states and non-state actors, a threat that impeded U.S. policy decision-makers. These foes rose as a fatal threat to the U.S. in the 21st century and changed its national security perspective and policy (4-11).

2.3. U.S. National Security Policy: The George W. Bush Doctrine in Perspective

There is no denying that power contributes effectively to history in general and international politics in particular. International Law (IL) and governing norms do exist. American policymakers were particularly interested in promoting and spreading liberty because it was and will continue to be the core value and identity of the American creed. Samuel Huntington argued in his book *The Third Wave, Democratization in the Late Twentieth Century* that: “The United States is the premier democratic country of the modern world, and its identity as a nation is inseparable from its commitment to liberal and democratic values”. Thus, spreading freedom and liberal values in American politics was generally considered an expansion of human liberty.

American foreign policy focused on containing the ‘rogue’ states, namely North Korea, Iraq, and Iran. Not only was the focus on the rogue states before the 9/11 attacks, but also on

China and Russia's foreign policy and the continuous debate raised in national security about the ballistic missile defense system developed in the Middle East in Iraq. The debate swung between agreement and disagreement on an economic sanction against Saddam Hussein's economy. The American NS Advisors and officials prioritized containing the rogue states by using new strategies and frameworks, but they had never foreseen the escalating threat of radical Islamic terrorist groups. Richard Clarke and the CIA director George Tenet had been desperately alerting the officials about the gravity and the imminent threat of terrorism, but the officials, including President George Walker Bush; Condoleezza Rice, National Security Adviser; Collen Powell, Secretary of State; and Donald Rumsfield, Secretary of Defense, underrated the danger of terrorism led by Osama Bin Laden (Leffler, "9/11 In Retrospect: George W. Bush's Grand Strategy, Reconsidered"34).

President Bush, Address to the nation after the 9/11 Attacks focused more on a 'new revolution in military affairs.' His presidential campaign fostered both modest foreign and reconfigured defense policies. His interest was also more based on domestic affairs, which kept him far from the upcoming challenges to American security (34). As never expected, the 9/11 attacks on Americans shocked President Bush and his administration. He condemned the attacks and described them to be "the despicable, evil acts of terror," and declared war on terror: a war that "will not end until every terrorist group of global reach has been found, stopped and defeated" (Bush, *Selected Speeches of President George W. Bush* 55).

The U.S. urgently needed a new strategy to carry out the war on terrorism and deal with this emerging threat. The word 'grand strategy was the right word to define the new American NSS adopted to defend its territories, people, and interests from any external threat. The new strategy was distinctively different from the Cold War strategy that emphasized containment of

the communist threat. The new strategy aspired to protect U.S. interests and deter the forthcoming danger of Islamic extremism (Korb 5). The new threat of radicalism to the U.S. geopolitical position mired the galvanization of the new policies terms. Though the new strategy had a distinctive policy formula, it still endorsed policies and ideologies that shaped the Cold War in a very distinctive way. Like past policies, the new strategy endeavored to protect American interests (Quinn 141).

The manifestation of the Bush doctrine guided and moralized the 'war on terror', which was not an act of aggression that could be defeated by soft diplomatic diplomacy; it was to be confined with new measures and military power. Therefore, a radical change was brought to the traditional terms of war and diplomacy. One of the significant terms of Bush doctrine is the 'no neutrality stands' which was allowed to nations all over the globe; as he made it clear in his speech addressing the nation in 2001, "every nation, in every region, now has a decision to make, either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime"(Bush, *Selected Speeches of President George W. Bush* 69).

President Bush, in the aftermath of the 9/11 attacks, envisioned U.S. supremacy and leadership as the best way to defend American interests. The doctrine adopted was much like a policy of an emerging empire; as Robert Jervis mentioned, 'it was much like an empire' (365). According to Jervis, the doctrine has four major components:

> The doctrine has four elements: a strong belief in the importance of a state's domestic regime in determining its foreign policy and the related judgment that this is an opportune time to transform international politics; the perception of great threats that can be defeated only by new and vigorous policies, most notably

> preventive war; a willingness to act unilaterally when necessary; and, as both a cause and a summary of these beliefs, an overriding sense that peace and stability require the United States to assert its primacy. (Jervis 365)

The doctrine used the war of self-defense as a response to the terrorist attacks as a pathway to eradicate the existence of terrorism. An alteration strategy that made and set Bush's foreign policy from 2001 to the end of his administration (Dalby 03).

In order to have a lasting and resisting strategy for a war that may last for decades across deferent landscapes, Bush, in his doctrine, employed direct and indirect approaches to military intervention; the direct approach intervention was the one seeking regime change involvement, and the indirect intervention was to help countries gaining their independence or toppling an authoritative regime and installing a democratic one (Donnelly and Monaghan 2). Furthermore, the doctrine has no tolerance towards its opponents, whether state or nonstate actors; primacy and strength were no longer enough to address a world wild, challenging threat to U.S. NS. The U.S. policy became involved in conflicts far from the American continent for the sake of American national security; they were taking the battle to the graves of terrorism, as President Bush emphasized in his famous saying, "... If we wait for threats to fully materialize, we will have waited too long ... We must take the battle to the enemy... and confront the worst threats before they emerge." (Bush, *Selected Speeches of President George W. Bush* 128).

2.3.1. The Elements of the George W. Bush Doctrine

After the 9/11 attacks, Bush told one of his closest advisors, "we have an opportunity to restructure the world towards freedom, and we have to get it right" (qtd. In Jervis 368). Bush believed in making peace and democracy in the world; this belief was vibrant in his answer to a reporter's question about his Conservative policy and lack of international experience. When he

answered, “history has given us a unique opportunity to defend freedom, and we are going to seize the moment, and do it” (qtd. In Jervis368), he declared firmly that “we understand history has called us into action and we are not going to miss that opportunity to make the world more peaceful and freer”. These declarations of President Bush and his persistence in spreading freedom, democracy, and liberal values were the core values of his liberal doctrine in organizing societies (368).

It has always been part of the American political discourse to value freedom and liberal values. However, in the Bush administration, it was more of a centered task policy measure in new American foreign policy. President Bush’s speech on September 17, 2002, at the White House declared his willingness and determination to stand by any nation ready to build its societal organization based on the creed of freedom, democracy, free trade, and free-market enterprise. Those individual states that were ready to lift their economic status from poverty to prosperity will be assisted by the United States to reach that level of economic freedom; “The United States will work with individual nations, entire regions, and the entire global trading community to build a world that trades in freedom and therefore grows in prosperity” (A National Security Strategy 2002, 17). As elaborated in the NSS, 2002, the widening of the world economy and its unification was an undistinguished element of the NSS after the 9/11 attacks.

The Bush Administration differed from the other administrations in their commitment and perseverance in changing the structure of the world’s economy to a global free market and free trade. “Economic freedom” has been a fundamental value of the new changes acknowledged by President Bush: “all states are responsible for creating their economic policies” (A National Security Strategy 2002, 17).

The aspiration for endorsing economic freedom is to create a haven for American-constructed capitalism in these regions. Eventually, the main purpose of invading Iraq was to demonstrate the presumed emergence of a new capitalist economy after the toppling of Saddam Hussein's regime; Bush confirmed, "A new regime in Iraq would serve as a dramatic and inspiring example of freedom for other nations in the region" (Bush, "Remarks on the Future of Iraq", 170).

Bush's ambition was to spread freedom and beat Iraq and Afghanistan; he saw that: "a liberated Iraq will show the power of freedom that vital region, by bringing hope and progress into the lives of millions" (168). This idea of broadening the potential of democracy to involve other regions suffering from tyranny and instability became one of Bush's agendas. The Bush Administration believed that the pursuit of freedom and prosperity undertook the allies' contribution to creating a peaceful setting for freedom. He also assured that progressive freedom was a fatal weapon to undermine the widespread terror and tyranny. Condoleezza Rice was very supportive of the president's argument; she reasserted it ideologically "the fever swamps in which they [terrorists] grow can be drained"(Rice, "The Road Map to Peace"). The regional expansion of freedom was galvanized in 2003 when the Bush administration continued with an unprecedented plan for the greater Middle East after their achievement in Iraq. In November 2003, Bush launched his "forward strategy of freedom in the Middle East" to promote freedom and democracy in this region. He expressed his plan clearly:

> Advancing freedom in the greater Middle East, we help end a cycle of dictatorship and radicalism that brings millions of people misery and brings danger to our own people … As recent history has shown, we cannot turn a blind eye to oppression just because the oppression is not in our own backyard. No

> longer should we think tyranny is benign because it is temporarily convenient. (Bush, “Remarks on the Future of Iraq”).

Bush conveyed a thorough message of his new policy in the Middle East by toppling tyrannical governments and establishing better-secured countries in the world. He called transparently for this strategy in his inaugural address when he declared his willingness to exterminate any act of tyranny and terrorism worldwide. He saw that the only way to save the world from this fatal threat of terrorism would never be possible without the liberation of the entire world from these oppressors of freedom and security; “it must be the policy of the United States to seek and support the growth of democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in the world” (Bush, “The Second Inaugural Address”, 273).

Last but not least, American national security after 9/11 set freedom at the core of its policy and recognized international liberal democracy policy as the principal of the nation’s worldwide security policy. The purpose of this distinctive policy was not just to preserve a common standard of peace between nations but also to customize American liberal values with the world political system (Quinn 149).

2.3.1.1. Unilateralism and Hegemony

It is noticeably agreed on by scholars, mainly Jervis and others, that the landmark of the Bush doctrine was his unilateral action; as unprecedented, the Bush Administration confidently declared the nation’s readiness to act pre-emptively against any perceived threat with less consideration to the Allies’ consent or disapproval. The Bush administration unveiled its readiness to use U.S. military dominance to spread freedom, liberal democracy, and a free market (Tarzi 28). Unilateralism complemented the Bush doctrine of preventive war on terror;

this latter was a fatal insurgency that demanded an immediate act of pre-emption by a superpower.

The history of the U.S. acting unilaterally has its roots in American politics; it was part of the Reagan and Bush administrations. After the 9/11 attacks, the U.S. government acted unilaterally and paid little attention to public opinion. Thus, the administration saw the shared leadership as a hinderer to obtaining tangible international results since none of the participating nations would accept to take the lead and the responsibility to act; "At this moment in history, if there is a problem, we are expected to deal with it", affirmed Bush (Jervis 375). Eventually, toppling Saddam Hussein's dictatorship and waging war on Iraq without the allies' and the UN's consent was a U.S. demonstration of its unilateral action. It showed the world that it would act pre-emptively without consideration for the allies' objection if it were a U.S. necessity to attain its objectives and secure its interest.

Ideological supremacy was the U.S. slogan after the 9/11 attacks. Bush Administration adopted hard power imperialism. The main objective of the U.S.' new system was to introduce a new strategy of hegemony to the world; the main intention was military dominance and unchallenged power (Quinn 157; Dalby 03). In the NSS, the U.S. extroverted its intention to have invincible global military control. Its strategy of dominance is not ordained to be exclusively U.S. legitimacy. In a pivotal attempt, the U.S. included cooperation with other nations as part of this strategy; The role of allies in addressing American international policy was marginalized by the U.S.'s overwhelming superiority in policy decisions (Quinn 156). Condoleezza Rice, the Bush Administration's National Security Advisor, stated unequivocally:

> the United States will build and maintain twenty-first century military forces that are beyond challenge. We will seek to dissuade any potential adversary from

> pursuing a military build-up in the hope of surpassing, or equaling, the power of the United States and our allies. (Rice, "Dr. Condoleezza Rice Discusses President's National Security Strategy")

The other side of the doctrine is how the primacy of one nation over the others can affect leadership and order; the Bush administration did not see the intervention in Iraq to secure any Weapons of Mass Destruction (WMD) threat to American security without the consent of the UN or the allies as an act that would encourage other nations to do the same if similar circumstances arose. On the contrary, the U.S. believed that unilateral leadership was required to ensure global stability and liberal democracy. The anti-proliferation policy aimed to protect the United States from any WMD threat. This predisposed the U.S. acts differently and distinctively than other nations. The Bush Administration was obstinate about the need for a unique and strong leadership to re-establish the world order, and it was only fulfilled when the U.S. acted hegemonically (Jervis 367).

Many scholars like Jervis were surprised by the American-launched policy in the aftermath of the 9/11 attacks. However, to dig deep into American foreign policy and NSS since WWII, it would be very clear that the adopted policy by Bush had its roots in American international politics during the Cold War. In early WWII, the U.S. believed itself to be the upcoming political power and the 'prime architect' of the new political order; to maintain peace and order in the world.

2.3.1.2. Preemptive and Preventive War

The 9/11 attacks were estimated as a global war on the United States' national security and the world at large. Such an unequivocal threat has one interpretation; it is a 'war'. The two noncontroversial terms 'war' and 'global threat' were highly qualified to spark a new American

foreign defense policy after the 9/11 events (Butler 7-8). The U.S. applied a strategic, operational plan, against the terrorist attacks and the involved states, as an act of pre-emption to deter terrorism and the unperceivable evil of their intentions. Anticipating the threat before it occurred was a very inventive strategy that the Bush Administration planned to exterminate any terrorist threats with WMD use. Resoundingly, the stem of the Bush doctrine was a "preventive war against terrorism" based on military primacy and superiority (A National Security Strategy 2002, 14-15)

Though 'pre-emption' and 'preventive' were two distinctive actions, the NSS 2002 used the term interchangeably in different and similar contexts: "The United States has long maintained the option of pre-emptive actions", "the United States will, if necessary, act preemptively", ". . . nor should nations use preemption as a pretext for aggression" (A National Security Strategy 2002, 15). The terms 'preemption' and 'preventive' were used ultimately as they both represented a forthcoming threat that was not instant and should be contained before it struck.

Defining the terms 'pre-emption' and 'preventive' requires understanding their military implication in American national defense. The pre-emptive war was "a military attack or war launched in anticipation of a serious military threat that can be reasonably construed as an imminent attack. It is a form of self-defense, or in some cases defense of a third party". It would seem that the existence of an imminent danger is what categorizes military measures as preventative war (Butler 7-8). Preventive war, at its core, is the use of force and military action to avert the occurrence of a future conflict whose cause and conditions are as yet unknown. Consequently, it was a strategic move taken in reaction to a persistent threat, with the aim of thwarting the further spread of a potentially devastating weapon by countering the dominant

aggressive force it represented. Even if there was no visible proof of a first strike, the preventer may still take steps to protect the "margin of safety provided by the preventer's military superiority" (qtd. in. Brailey 2).

On the same margin of prevention diameters came another 'pre-emption', defined as an act of defensive military action against an alleged, recognized, and dangerous threat that compels a primordial deterrence. Levy defined it as "A pre-emptor has a perceived incentive to strike first, which is further intensified by military technology favoring the offensive or by the existence of military doctrines emphasizing the offensive" (90-92). The main reason for acting pre-emptively is to prevent any possibility of the enemy from initiating the attack. In the definition of pre-emption, the U.S. DoD specified that the threat must be unquestionable and imminent to have the jurisdiction to launch a justifiable pre-emptive war (Mueller et al. xix-xx).

In the antecedents of American foreign policy, the terms 'pre-emptive' and 'preventive' exist and are applied in different circumstances with different strategic typologies. Unlike the Bush administration's use of the terms, President Theodore Roosevelt may be concerned with this act of pre-emption and prevention in his Monroe Doctrine' 'corollary' when he prevented any other interference in the American sphere. In a nondifferentiated policy, President Franklin Roosevelt defended his alternative option of acting preventively against the German ships set on the Atlantic shores of the United States in WWII, considering this an imminent threat to his country and security. He illustrated this idea with a striking snake idea; "when you see a rattlesnake poised to strike, you do not wait until he has struck before you crush him" (Leffler, "9/11 In Retrospect: George W. Bush's Grand Strategy, Reconsidered."40).

In the 60th, President John F. Kennedy expanded the embargo imposed by Eisenhower on Cuba to prevent the Soviets from having any military bases close to the American shores.

Imposing a quarantine on Cuba along with 'The Missile Crisis' was clarified by Kennedy as an act of 'preventive step' to secure and protect the American territories from any Cuban threat. In the aftermath of the Cold War, President Bill Clinton, as an act to preempt and deter any act of terrorism, stated that "The United States shall peruse vigorously efforts to deter, apprehend and prosecute . . . individuals who perpetrate or plan to perpetrate such attacks". Unsurprisingly, the Bush doctrine was close to the traditional political strategies of presidents earlier in the twentieth century. However, now it was under a new cover of the war on terror (Leffler, "9/11 In Retrospect: George W. Bush's Grand Strategy, Reconsidered."40).

The Bush administration saw the prevention of terrorist attacks and the isolation of rogue nations as essential tenets of its foreign policy strategy. The United States had strong convictions about its ability to make the globe a safer place. Bush agreed that swift action was necessary to counter this threat before it escalated further. In his speech given at West Point on June 1, 2002, he said:

> Today, our enemies see weapons of mass destruction as weapons of choice. For rogue states, these weapons are tools of intimidation and military aggression against their neighbors. These weapons may also allow these states to attempt to blackmail the U.S. and our allies to prevent us from deterring or repelling the aggressive behavior of rogue states. Such states also see these weapons as their best means of overcoming the conventional superiority of the U.S. (A National Security Strategy 2002, 15).

According to Bush, the new threat to American security could not be contained as the Cold War and the Soviet Union threat. This threat of terrorism is fanatic and should be eradicated. A preventive war must be waged, expressed Bush, against an escalating threat to the United States and its allies; this evidence of an approaching threat made the preventive war

doctrine a pathway to American new strategy to protect its territory and maintain supremacy as a new key to its foreign policy.

The Bush Administration was considered a new start to American foreign policy; Jeffrey Record stated that it was “the most significant American foreign policy departure since the Truman administration”, as it embraced a doctrine of an anticipatory military strike as the core of the foreign policy. Three types make immediate anticipatory strikes (from near to medium) justifiable. According to Mueller. et al. the attacks are justifiable if they fall under these three crucial circumstances. First, ‘Preempting cross-border aggression against vulnerable allies’ can be in direct military attacks or coercive acts against these states, such as North Korea against South Korea or China against Taiwan. Striking against imminent aggression in another state is a nonconventional choice since the threat will not be contained from the first attack; instead, it is starting a war than deterring a threat. Second, ‘striking first against terrorist attacks’; is to arrest or kill the terrorist cell before it commits any act of aggression. To pre-emptively act in this case is also justifiable to prevent further attacks or to retain arms of mass destruction. This action is likely to take place if there is enough information about the terrorists’ identities, locations, or any fatal plans to be carried out. Third, ‘owning WMD’ or being in terrorists’ hands is a threat to all humankind; attacking other states to prevent the spread of WMD is the most tolerated kind of an anticipatory act (Mueller. et al. xix-xx).

2.3.1.3. National Security Strategy as the Sound of Reason in George W. Bush Doctrine

Following the 9/11 attacks, the United States pulled the core of its National Security Strategy from a series of remarks and speeches on the topic that would come to be known as the “Global War on Terror” (GWOT). Bush’s central tenet for the new millennium was revealed to be “The National Security Strategy of the United States of America” in September 2002. It not

only highlighted methods and policies to be aimed towards rogue nations and terrorists, but also projected the American language of the 'city upon a hill' as an identity with a new nationalism interlaced with dominance and power. The NS grand strategy was the face of U.S. supremacy and unilateral policy. President Bush, in his speech in West Point, addressed this issue, saying, "America has and intends to keep military strength beyond challenge. . ." (Bush, "West Point Commencement", 125).

The 2002 NSS document elaborated on the landmarks of the American strategy for a new century, a distinctive document from the others in many different ways:

> First, the NSS raises global terrorist networks and outlaw regimes to first-order or existential threats to the security of the United States and the stability of the international political system.
>
> Second, the new strategy makes it clear that our military forces must remain dominant for the foreseeable future . . . the United States should not only attain and maintain military dominance but should also project it with a worldwide network of forward operating bases. Third, the new strategy emphasizes cooperation among the Great Powers in order to preserve a unified front in the war on terrorism. It advocates that this cooperation be carried out under the aegis of US leadership. Fourth, the security strategy enunciates, for the very first time, a policy that specifically calls for removing the root causes of terrorism and tyranny. (Korb, 21-23)

Pre-emptive military action would be the only response to these enormous dangers to global security, and the consequences would be incalculable if the terrorists gained access to WMD, but the NSS suddenly no longer believed in deterrence by containment or any other

conventional policy. As a result of these events, the United States decided that a clear defensive fight against terrorism was necessary.

The 2002 NSS was also more comprehensive in its understanding of the factors that would help sustain the world political and economic system. For the latter, the manifesto advocated for unrestricted business activity. It placed them in the NSS universal category and provided a thorough illustration of the United States' desire to assist and support the countries assumed to approve this model of free economy and business. As the American territory was no longer safe and vulnerable to external attacks, the NSS strengthened its homeland safety by creating many assets to protect its people, territories, and interests. This act of expanding the U.S. security organization started with the creation of the Department of Homeland Security as a U.S. protector, allied with different countries in the world and unified to exterminate any terrorist threat that existed or merging ones, not to mention spreading democracy all over the world as American Creed and as a part of the Bush ideology.

2.3.1.4. The Creation of the Department of Homeland Security

The 9/11 attacks resulted in the reconfiguration of the American security system. In less than 14 months, Congress passed the new antiterrorist Act and created a federal antiterrorist bureaucracy. The federal tribunals were restored, and operational and with authority granted to the intelligence agencies like the FBI; to scrutinize information and strengthen its surveillance system. Furthermore, to protect the homeland and American citizens from any external threat led to the creation of a new DHS; the DoD, on the other hand, initiated new military measures of protection to secure the homeland (Jordan et al. 124; Platt and O'Leary 8). Eventually, the government responded quickly to the imposed threat on American land; it created vital assets in its system, which were primordially directed to protect the homeland (Jordan et al. 125).

On September 20, 2001, President Bush announced the creation of a new office of Homeland Security to direct all the homeland security measures and operations by one organization. On November 25, 2002, DHS was officially created under the Homeland Security Act. This department unified about 22 organizations that are oriented to serve security measures.

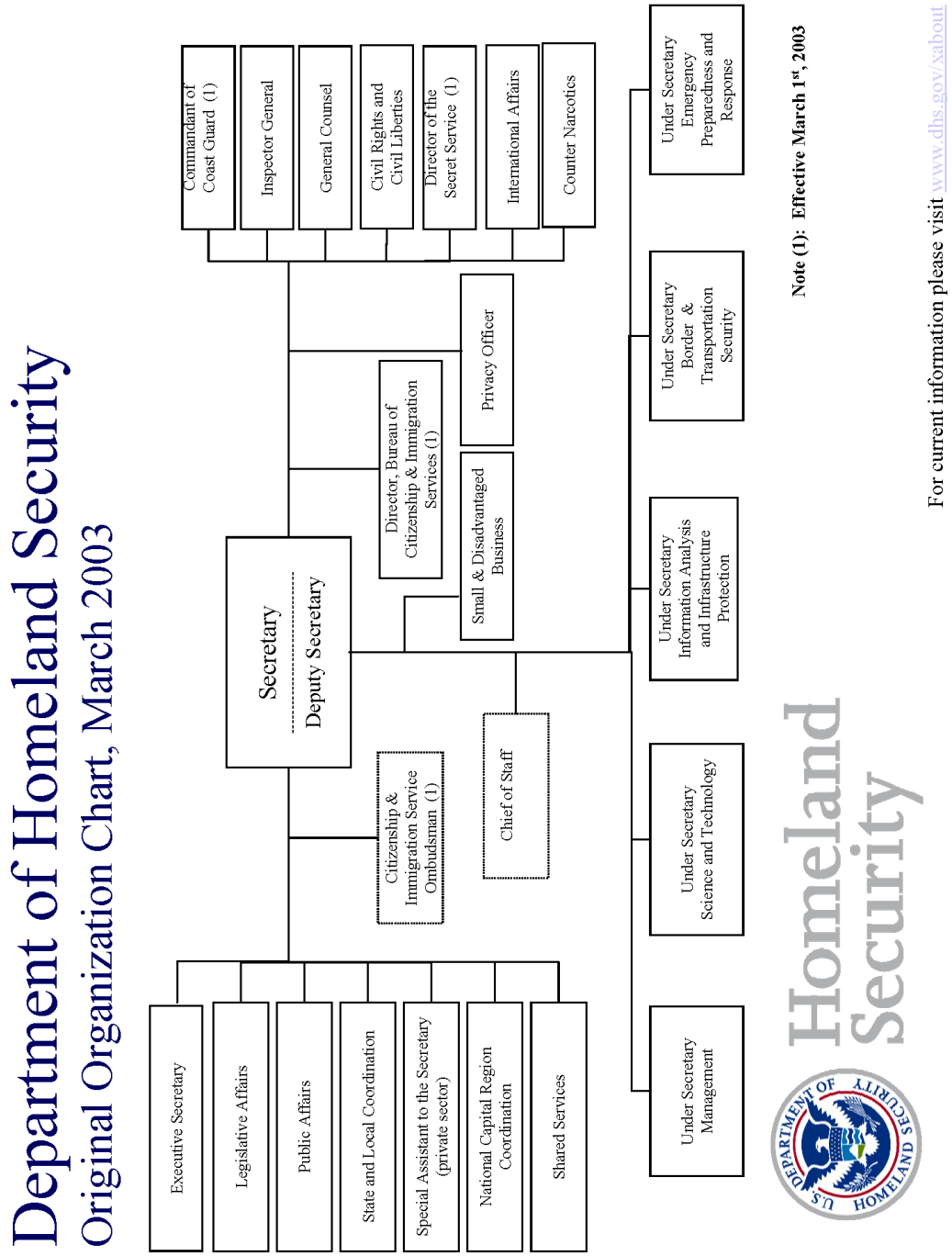


Fig. 1. Department of Homeland Security. *Hsdl.org*, https://www.hsdl.org/?view&did=234684. Accessed 28 April. 2020.

U.S. Coast Guard with over one hundred eighty thousand employees. This department was the third largest department in the U.S. government. The department prompted, more importantly, to "prevent terrorist attacks within the United States, to reduce America's vulnerability to terrorism, and to minimize the damage and recover from attacks that may occur." The Homeland Security Act created a Homeland Security Council (HSC) to interchange and implement the collected information and to advise the president on national security matters (Jordan et al. 126).

Congress strengthened the antiterrorist legislation by passing new legislation to seize and block any terrorist threat to the American homeland. The U.S.A Patriot Act, signed into action by President Bush in November 2001, gave more freedom to the government to conduct research, deport, and suspect cyberspace and control any financial transactions to hinder terrorist financing (Platt and O'Leary 8). The Patriot Act has more contributions to security measures: "the Patriot Act expanded government authority to fight terrorism by easing some restrictions on foreign intelligence gathering in the United States, facilitating information sharing between the intelligence and law enforcement communities, defining new crimes, and streamlining processes for prosecuting terror-related crimes" (Jordan et al. 128). The Act has an overwhelming jurisdiction prerogative that opponents mostly interpreted as an abusive Act that prioritized security over individual privacy in a massive way.

If there were anything that Americans might cherish, it would be their freedom, a fundamental principle that the United States was founded up on. The Patriot Act jeopardized this principle of the amount of authority given to the government. The Constitution of the Act was perfectly set to prevent any pre-empted terrorist attacks, but meanwhile, it threatened civil liberties. Davis, Darren W., and Brian D. Silver, in their article, "Civil Liberties vs Security:

Public Opinion in the Context of the Terrorist Attacks on America", discussed the jeopardized civil liberties after the 9/11 attacks. They brought to the forefront the dilemma that threatened American civil liberties; they wondered whether people would tolerate restrictions on their freedom for security and personal safety. The no equilibrium between civil liberties and national security protection became controversial in the U.S. governmental, political, and public sectors (29).

2.3.1.5. Critique of George W. Bush Doctrine

George Walker Bush's policy toward the Middle East disappointed the international community. Looking to the American values towards establishing democracy and self-determination in other nations under the controversial slogan of 'Freedom Agenda'. The "Freedom Agenda" was an unsuccessful attempt to foster democratic transformation in Iraq, both in terms of its conception and its execution. When compared to President Bush's rhetoric, actual implementation fell short. U.S. participation did not lead to greater democracy in the area. The government creation did not clarify the character of the Iraqi state. A key roadblock to the progress of Iraq's political transition has been the question of how to divide up power (Katulis 11). Hence, "the use of torture, extraordinary rendition, black sites, the carceral regime at GTMO, also cast doubt on the veracity of claims that the U.S. was interested in promoting democracy and especially human rights". The promotion of democracy and human rights remained weak in the Middle East.

The Cold War strategy did not exclude pre-emptive and preventive acts; however, they were the last option the U.S. security may depend on. In his Strategy, Bush stated, "The United States will not use force in all cases to prevent emerging threats, nor should nations use preemption as a pretext for aggression." The pre-emptive policy was never a first-choice policy

for the United States, but it was considered an alternative that should be used when necessary (Leffler, "9/11 and American Foreign Policy."286). "The preventive warfare doctrine" allowed the preventer state from attacking another sovereign state without any direct attack by the latter. The U.S. authorized its government to identify and anticipate any threat and take the initiative to pre-empt without any sense of aggression from the other country. Bush's military doctrine as his armament in different sovereign countries, like Iraq and Afghanistan, destroyed governments and toppled regimes that they thought posed a threat to American security. The results of U.S. intervention were fatalistic; they failed to reconstruct a democratic government. Spreading democracy and liberal values in these regions was only a shadow of a failed policy (Dalby 20).

The Freedom Agenda or "Bush doctrine" following the terrorist attacks of September 11, 2001, has been generally defined as a turn in U.S. foreign policy. It was marked by full-scale militarization and unilateralism meant to defend U.S. national security (Dimitrova 2). A National Intelligence Council (NIC) argued that Bush made three main changes to the U.S grand strategy "Reducing Washington's reliance on alliances and international institutions, expanding the traditional right of pre-emption into a new doctrine of preventive war, and advocating coercive democratization as a solution to Middle East terrorism" (2)

Bush's primary subject in his speeches was the expansion and defeat of terrorism, which led to inflated expectations in the Middle East, the Arab world, and elsewhere over the effectiveness of the political reform. The Bush administration implied that its promotion of democracy and individual liberties was motivated by a desire to alter other countries in order to benefit the United States. Madeline K. Albright, the Secretary of State, discussed the idea of a "Indispensable Nation" in an interview with NBC's "The Today Show" with Matt Lauer, and the harsh strikes on Iraq exemplified this notion. Abuse of its "imperialistic" authority and self-

concerned foreign policy were shown by the opposition of its allies and the lack of a UNSC mandate to lawfully approve military action in Iraq. As a result, this fueled growing anti-American sentiment, particularly among Muslims (2).

Bush doctrine foreign policy irregularities included acting unilaterally and without the approval of the international community. By invading a Middle Eastern country without the sanction of the UN Council or the U.S.'s cooperation, major European allies or Muslim governments fashioned a global icon of American strategy in the twenty-first century. After 9/11, the United States' activities abroad were seen as those of an egocentric power that used force to further its own national interests without giving due thought to the legality of such acts. In doing so, the United States depicted itself as a forceful, dominating nation rather than the champion of democracy and "spreading liberal values" it often portrays itself as (Tarzi 36).

2.4. The New International Challenges to American National Security Policy

2.4.1. Obama Doctrine in Perspective.

President Obama pointed out in his speech that the 'New Beginning' raised questions about the U.S. foreign policy and strategy issues at the top of his international agenda. He was committed to openness toward the Middle East and overcoming religious and ethnic barriers. In his speech, he hoped for mutual benefit between the two regions and a friendly based relation:

> To join together on behalf of the world that we seek— a world where extremists no longer threaten our people, and American troops have come home; a world where Israelis and Palestinians are each secure in a state of their own, and nuclear energy is used for peaceful purposes; a world where governments serve their citizens, and the rights of all God's children are respected. Those are mutual

> interests. That is the world we seek. But we can only achieve it together. (Obama, *A New Beginning: Speech at Cairo University*, 1)

Strategic and rational thinking was Obama's vision of warfare and his efforts to make a positive change in American policy after Bush's era. This ambitious and mindful president was described by Secretary of Defense Robert Gates, who served Bush Sr., George W. Bush, and Obama as "the most deliberative president I worked for" (Suri 202).

Obama confessed that his policy was directed to "bury the last remnant of the Cold War" and "extend the hand of friendship" (Obama, *Address to the People of Cuba*, 2). He was against using force, primacy, and military insurgencies to solve conflicts. His stand altered the U.S. traditional school of primacy and hegemony since 1945. The President was fascinated by American policymakers' perception and interpretation of policy, law, norms, and international application. Obama favored multilateral sanctions, an international system ruled by law, and joint police action worldwide. He wanted to set a constitutional foundation for an international system based on norms, law, adjudication cooperation, and friendship. He appeals for a world without nuclear weapons (201).

2.4.1.1. Soft Power

Obama's doctrine differs from the Bush doctrine; it can be differentiated by analyzing the instruments of power used by both presidents. The Obama strategy was not associated with hard power, as was President Bush's policy, but rather with soft power. Joseph S. Nye Jr., one of the famous writers in public diplomacy, defined the concept of soft power as: "the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment. A country's soft power rests on its resources of culture, values, and policies" (94). President Obama contended a pursuit of peace in the region of the Middle East and the rest of the world by

using diplomatic and economic tools to facilitate the democratic transition. He advanced an economic program such as the "Enterprise funds" to invest in Tunisia and Egypt as he promoted a comprehensive trade and investment partnership initiative to simplify the trade enter-exchangeability within these regions. This new program could be regarded as a new Marshall Plan for the Middle East and North Africa (Dimitrova 3).

In a world where American power has been tested by the new changing and emergence of other powers such as the (BRICS)_ (Brazil – Russia – India – China –South Africa), Obama found it important to codify his doctrine to the new changes. In his NSS 2010, he differentiated his policy from his predecessor's by replacing the US hegemony in the world with a "balance of power" policy and the recognition of the "relativization" of American power. This idea has already been introduced by a famous foreign policy analyst Fareed Zakaria in his famous essay: "The Post-American World and the Rise of the Rest". The relativization of American power is the U.S.' acknowledgement that it can no longer engage in international conflicts alone; allies must be partners. The change in the vision of the U.S. role and power in the world was confirmed by Obama's Secretary of State, Hillary Clinton:

> Today, we must acknowledge two inescapable facts that define our world: First, no nation can meet the world's challenges alone. The issues are too complex. Too many players compete for influence, from rising powers to corporations to criminal cartels, from NGOs to al-Qaida; from state-controlled media to individuals using Twitter. Second, most nations worry about the same global threats, from non-proliferation to fighting disease to counterterrorism, but also face very real obstacles – for reasons of history, geography, ideology, and inertia. They face these obstacles and they stand in the way of turning commonality of

> interest into common action. (Clinton, "Foreign Policy Address at the Council on Foreign Relations")

The second major factor in Obama's doctrine was the change in the perception of the U.S.A. on the international scope. America was no longer seen as an "Indispensable Nation" but rather as an indispensable leader", "as just no nation can meet the challenges alone. No challenges can be met without America". Thus, U.S. commander in chief defined the new U.S. leadership in terms of partnership: "We must lead not in the spirit of a patron but in the spirit of a partner" (Obama "A New Beginning: Speech at Cairo University"). Thus, the Obama administration was advocating the use of diplomacy, partnership, and development to achieve U.S. foreign policy goals in the world, a policy that was based on the new typology of power as Joseph S. Nye Jr., one of the most influential international relations scholars today called it "soft policy" (Dimitrova 4).

2.4.1.2. Smart Power

The smart power of a country is a combination of soft power and hard power; it was "A smart power strategy combines hard and soft power resources" (Nye 94), as it was defined by three elements" its culture, its political values and its foreign policies. Some think tanks adopted the concept of smart power and used it as a preparatory idea for a new area of research in foreign policy and strategic diplomacy for the new administration. CSIS, the Center for Strategic and International Studies, adopted the concept of smart power in a tentative to create and direct the President's administration to new strategies; eventually, the commission directed by Joseph S. Nye Jr. and Richard Armitage, in a report entitled, *A Smarter More Secure America*, published in 2007, introduced a diplomatic pathway to be followed in a new world of challenges; the new

smart power strategy to the U.S. This Report defined the main elements of the American smart strategy needed to achieve an effective foreign policy (Nye 96).

The principal elements that foreign policy should implement to fulfill the requirement of smart power were enacted in the Commission Report, 2007 as follows: "partnership and alliances, global development starting with public health, public diplomacy, economic integration, and technology and innovation" (CSIS Commission on Smart Power et al. 5). Ultimately, as planned, the Report reached the new administration, and smart power became Obama's core foreign policy. It was first used by Secretary of State Hillary Clinton, on January 13, 2009, in her Confirmation Hearing at the Senate Foreign Relations Committee:

> I speak often of smart power because it is so central to our thinking and our decision-making. It means the intelligent use of all means at our disposal, including our ability to convene and connect. It means our economic and military strength; our capacity for entrepreneurship and innovation; and the ability and credibility of our new President and his team. It also means the application of old-fashioned common sense in policymaking. It's a blend of principle and pragmatism. (Clinton, *Transcript of Hillary Clinton's Confirmation Hearing*).

The elements of smart power discussed in the Commission's Report *A Smarter More Secure America*, published in 2007, were recognized and put into practice in Obama's foreign policy as a smart power strategy. This strategy was seen in practice in different cases under the Obama administration, starting with the intervention in Libya, called 'humanitarian intervention,' a coalition authorized by the UN, supported, and initiated by the U.S. allies. The Security Council Resolution 1973 approved the intervention in Libya as a "responsibility to

protect" as it was seen as "burden sharing." The operation was not a U.S. mission to accomplish alone but to share the responsibility with its allies (Dimitrova 6).

Obama's smart strategy in the case of Libya was visible in how he mobilized the international community to participate in the intervention in Libya and made it a global cause instead of a U.S. mission. France and Great Britain led the coalition in Libya as an implementation of the U.S. partnership position and not a leadership one:

> American leadership is not simply a matter of going it alone and bearing all of the burden ourselves. Real leadership creates conditions and coalitions for others to step up as well, to work with allies and partners so that they bear their share of the burden and pay their share of the costs, and to see that the principles of justice and human dignity are upheld by all. (Obama, *Address to the Nation on Libya*, 6)

Obama's foreign policy stood for the three 'Ds'; defense, diplomacy, and development. Obama's smart power policy was invigorated in his strategy to defend the U.S. interests through diplomacy and integrated development; this latter was part of an Obama plan in the Middle East and North Africa to sustain and promote economic exchange in this region. The plan was part of his smart power policy; his goal was to reorient American foreign policy to a more normative and liberal internationalist policy based on partnership, development, and democracy.

Obama consistently condemned military force campaigns and saw them as a non-useful uprising as they did not have legal or moral values. He disqualified military interventions. This was seen in his passiveness toward Syria when Obama did not undertake any military measures to stop the genocide in the area or to stop the authoritative regime of Bashar al-Assad and the Iranian Russian implication in the Syria conflict. Though Obama could deploy forces to different parts of the world, like in Iran, he was hesitant to use force in Syria against the coalition of

Bashar al-Assad -Iran-Russia. He was more focused on what he considered the real threat to the United States of America. The president perceived terrorist groups—associated with Al- Qaeda, other networks, and later the Islamic State of Iraq and Syria ISIS—as the real threat to the U.S. (Suri 197).

Being reluctant to use the traditional way of war, Obama alternatively emphasized using law as legal enforcement of his policies. His rationale for controlling from the White House rather than from the battlefield gave him more potential to exercise presidential power at the cost of traditional institutions like Congress. Obama's expertise in the law made him more reliable in analyzing and assessing all the repercussions of his pre-emptive engagements; he relied on military leaders and civilian agencies to manage his targets. Consequently, by being less accountable to American democratic institutions, Obama was, as any predecessor, the executive chief of many military operations. This latter was interpreted as a 'covert warfare' galvanized with legal interpretation and the courts' authorization (199).

2.5. Obama's Realistic Policy

The beginnings of Obama in office were different from his predecessor; he was not obsessed with the global war on terror years of dominance, hegemony, and unilateralism. He was more engaged in using international norms and political strategies. He wanted to shape his terms with a new policy based on moderation and balance between force and diplomacy. He was more committed to lawful responses showing looseness towards force and normality. On the other hand, he was seen as a president who wielded much unilateral power. Thus, his policy is a step toward a new policy (205).

Obama introduced an international liberal vision focused on three precise dimensions: multilateralism, negotiation, and disarmament. He had a distinctive defense system and a

military policy that differed from President Bush's. He adapted a 'standard defense' of American power: "The United States of America has helped underwrite global security for over six decades. . . with the blood of our citizens and the strength of our arms . . . adhering to standards, international standards, strengthens those who do, and isolates and weakens those who do not." (Obama, *Speech at West Point on Troop Increase in Afghanistan*, 8). He expressed his opposition to the war in Iraq, the use of torture, and unfair trials against the prisoners at Guantanamo Bay. Obama promised a safe world with a combination of collective security and American power to maintain this security, not in a unilateral form but a multilateral one (Suri 196-197).

President Obama approved that the United States has inherited, by playing the heroic role in the world, an exceptionalism that Obama extrovertedly affirmed. He emphasized that he would use this power to settle for peace and law enforcement worldwide. The president was convinced that cooperation and negotiation with adversaries was a better strategy rather than military confrontation:

> The promotion of human rights cannot be about exhortation alone. At times, it must be coupled with painstaking diplomacy. I know that engagement with repressive regimes lacks the satisfying purity of indignation. But I also know that sanctions without outreach—condemnation without discussion—can carry forward only a crippling status quo. No repressive regime can move down a new path unless it has the choice of an open door. (Obama, *Nobel Prize for Peace*, 03)

Eventually, he worked hard to build diplomatic alliances and cooperative negotiations with his adversaries worldwide.

President Bush's years of administration were defined by military engagement and a war on terror agenda, leading to the deterioration of the American image in the world. In Bush's eight years in office, the U.S. administration was portrayed as an engaged country with a unilateral military force. Unlike him, President Obama was committed to restoring the American image of liberal leadership in the world: "Agreements among nations. Strong institutions. Support for human rights. Investments in development. All these are vital ingredients." Ending the war on terror and engagement in a liberal world was part of Obama's agenda: "This war, like all wars, must end. That is what history advises. That is what our democracy demands." Unlike Bush's avowed policy, Obama adopted liberal internationalism as a constructive alternative to Bush's unilateralism. His legacy in his foreign policy was law over war and partnership over leadership. He called upon his Allies for more cooperation in dealing with international conflicts and issues and was more open to change (Suri 197).

2.5.1. Obama's New Beginning Policy in the Middle East

Obama is a son of a Muslim father from Kenya. He carries a Muslim middle name of "Hussein" and attended school in Indonesia, the most populous Islamic country. In his inaugural address, Obama spoke directly to the Muslims in the world, promising "Mutual interests and mutual respect." When Barack Obama became the new U.S. President, one of his many concerns was restoring America's image worldwide, especially after the eight years of the Bush administration. The U.S. image was negatively viewed amongst the Muslim countries, and anti-Americanism had intensified in the Arab world and spread from Nigeria West to East to Indonesia. A distinct change in the tone of the United States' public diplomacy occurred with Obama's administration, and special attention seemed to be directed to the Middle East and the Muslims of the Arab world (Zaharna 1).

Obama granted his first interview to an Arab satellite channel in the White House and appointed two special envoys to handle the Palestinian-Israeli and Afghani-Pakistani conflict. Hillary Clinton, the new Secretary of State, included Indonesia in her first international trip. These dynamic acts were refreshing and comforting as Obama's new policy toward the Middle East unfolded. In his speech in June 2009 in Cairo, President Obama sent a message to the Middle East about his intention to change American policy towards this region and to make a new start in this area:

> I have come here to Cairo to seek a new beginning between the United States and Muslims around the world, one based on mutual interest and mutual respect, and one based upon the truth that America and Islam are not exclusive and need not compete. Instead, they overlap and share common principles—principles of justice and progress, tolerance, and the dignity of all human beings. (Obama, *A New Beginning: Speech at Cairo University*, 2)

He defined Islam as he learned it and as a religion of peace, and he promised to change the prevailing stereotypes of Islam in the United States. He praised the Muslim community in the U.S. and how they contribute effectively to American society. Unlike President Bush, President Obama did not mention war or terrorism in his speech as an essential core of his policy toward ending the war on terror era.

Regarding the rhetoric of Obama's policy, as expressed in his speech in Cairo, he created a new contextualization of the discourse of coexistence, cooperation, and reconciliation between the Muslim nations in the East and Christians in the West. The new beginning in the Obama administration ignited a spark of hope and expectation in the Muslim world that there would be a new beginning to the US Middle East policy (Gerges 302). Obama promised to bring

Palestinian-Israeli peace in his speech: “Lasting peace will involve two states for two peoples. Israel as a Jewish state and the homeland for the Jewish people, and the state of Palestine as the homeland for the Palestinian people; each state enjoying self-determination, mutual recognition, and peace.” **(**Obama, *On American Diplomacy in the Middle East and North Africa*, 10).

Regarding these expectations and steps that Obama’s administration was expected to accomplish, ‘Zero’ action was made. This would be enlightened by the visit of Israeli Prime Minister Benyamin Netanyahu to the White House, where Obama showed frustration towards the lack of any peace progress in the area. Obama’s rhetoric about peace in the region and building Palestinian statehood faced disagreement and rejection by Netanyahu, who declared that a “Palestinian state should not be established at the expense of Israeli’s existence” (Obama, *On American Diplomacy in the Middle East and North Africa*,10).

Obama’s foreign policy agenda was heavily loaded with the hostility he inherited from U.S. policy towards the Middle East: the wars in Iraq and Afghanistan, alliances with oppressive autocrats, unquestioning support for Israel, and serious challenges posed by Iran and Pakistan. The impact of this policy made it an uneasy task for the United States to remodel its foreign policy in the area, not to mention the economic recession that hit the U.S. and made the president more concerned with bringing equilibrium to the American economy. Although the president promised a new start of interrelations between the East and West, the Pacific Ocean and Asia’s rising powers hindered rethinking Middle East policy as Obama had planned (Gerges 302).

2.5.2. The Empty Talks in the Case of Iran

Obama’s strategy with Iran was one of his famous quagmire policy achievements. Iran emerged as a massive threat to American security with its nuclear empowerment. Obama promised diplomatic negotiations with Iran within the first few months after his inauguration

(Gerges 318). President Obama declared the unwillingness of the U.S. to approve any Iranian nuclear power acquisition. He expressed his intention to reach out to the Iranian government and persuade them to dispense with its nuclear ambitions. In 2009, the president sent a letter to the leader of Iran, Ayatollah Ali Khamenei, suggesting 'corporation in regional and bilateral relations' with stress on mutual coordination to end the Tehran nuclear empowerment. President Obama was also concerned with the Iranian people's engagement in this issue, as they would be the first to be hurt by any measures taken against their country. He addressed them in a recorded video during their new year celebration on March 20, 2009. He showed his interest in prioritizing peace in the Middle East, beginning with Iran, as it is fundamental to settle in the region (Suri 202).

President Obama believed that the United States and Iran remained two contesting rivals in nuclear weapons acquisition. His intention by devoting his first months to an American-Iranian negotiation was to anticipate new internal changes towards a new trustworthy era of collaboration based on primordially institutionalizing a peaceful foundation between the two nations. The president was determined to create a new balance of power in the region of the Middle East. He emphasized a dual partnership mostly concerned with eradicating terrorism, generating a prosperous economy, and ending the economic sanctions that Iran endured because of its nuclear policy (202).

However, despite his idealistic engagement in coordinating healthy and advantageous negotiations with Iran, President Obama has always maintained Iran under economic sanctions to hold up the pressure (Gerges 319). Eventually, the reaction of the Iranian leader was a predictable response to Obama's dual-track policy. Supreme Ayatollah Ali Khamenei did not consider any of Obama's rhetoric to constitute policy toward Iran. He believed that to flatten the

curves between the two countries, they must have a dual contribution of both countries based on realistic coordination and negotiation rather than a dual-track policy. Ayatollah Khamenei disregarded the president's speech and considered it "empty talk": "they say they extended their arms towards Iran. What kind of hand? If it is an iron hand covered with a velvet glove, then it will not make any good sense . . . you will change and we will change our behavior, too" (qtd. in Gerges 319).

Despite Obama's rhetoric, his administration wielded economic sanctions against Iran. In December 2011, Congress issued a defense authorization bill that included bilateral sanctions on the bank of Iran. The United States, with its allies, waged direct war against the economic existence of Iran. The sanctions imposed on the Tehran government were directed at its oil and banking system. The sanctions had a fatal impact on Iranian society; people suffered inflation and a currency decline. The Obama sanctions of 2011 were the most massive sanctions on Iran (319).

An escalation took place in 2013 on the Iranian nuclear intentions, where the Tehran government, due to the fatal sanction levied on its economy, signed a short-term agreement called the Joint Plan of Action in November 2013. This agreement halted its nuclear program to loosen Iran's economic sanctions (319). In April 2015, the framework shortened (but did not end) Iran's nuclear capability for 10 to 15 years for a total release of economic sanctions. The agreement could delay Iran's progressive intent toward developing nuclear weapons but at the cost of legitimizing its status as a nuclear threshold state (Gompert et al. 18).

The American government emphasized a realistic policy to deal with the case of nuclear weapons in Iran: the Obama administration, and so his policy, had very limited purposes behind the actions taken towards the Iranian case of nuclear weapons. Obama did not want Iran to hold

any potential of having or developing this power in this region because it directly threatened American allies like Israel and the European countries. The United States used sanctions and diplomacy to prevent Iran from reaching its nuclear goals to contain this threat. As Iran is not a direct threat to the U.S., Obama focused on sanctions and negotiation instead of military strikes (Gompert et al. 19).

Undeniably, the Obama administration's "dual-track" Iranian policy of negotiation and economic sanctions was not a success. The Tehran government or the U.S. Congress did not endorse his policy. The suspicious relationship between the two countries, spurred by the events of 1979 and toughened by the American sanctions on Iran's economy, would not regenerate a healthy environment for negotiation or accord between the two governments. The apparent engagement of Iran in abandoning its eagerness for nuclear weapons was seen by the US Defense Department and the intelligence community as a falsified map to puzzle the US government while developing nuclear weapons under cover (Gerges 320).

2.5.3. Back to Afghanistan

Obama came to office in January 2009 with a conviction that the policy toward Afghanistan after the 9/11 attacks was a war of necessity. He always believed that Afghanistan and the Taliban regime were the real threat to U.S. security, and the president decided to re-confront and topple the Taliban regime. In a December 2009 speech at West Point, President Obama declared an additional deployment of 30,000 American troops to Afghanistan to finish the unaccomplished mission. He loosened the tension of this news by promising a withdrawal by July 2011. This operation's main purposes were to destroy El Qaeda, deny the Taliban access to the country's new regime, and allow the Afghan government to develop its forces and manage its government (Gompert et al. 22).

The United States' surge led by the American and NATO forces in Afghanistan helped to minimize violence in this region as it stopped the Taliban temporarily from further advancement. Being optimistic about having these results, the Lisbon NATO Summit in 2010 declared that it was time for the Afghan government to handle their war which was estimated to be transferred to them by the end of 2014. However, any predictable U.S. date to leave Afghanistan vanished when the Taliban remerged, and the U.S. lost more than 1,700 soldiers between the start of the "surge" in December 2009 and February 2017. Unfortunately, the Taliban regained influence in the region, and the annual number of civilians killed increased by thousands. Nonetheless, President Obama envisioned withdrawing definitively from the region by 2016, regardless of the outcomes of his actions (Glaser and Thrall).

Obama's policy in Afghanistan was under his rhetorical dimension of the realistic model. Obama believed in using hard power only for a primordial and grave situation. His administration's international engagement in the killing of Osama bin Laden was one of the parts where Obama used hard power to deter a prominent threat to American National security. Though Afghanistan could be a haven for the Taliban and a threat to American security, it could still be considered a peripheral cause. The 30,000 troops sent to Afghanistan could not contain the Taliban insurgency in the area because there was no background for this operation to succeed: the Afghan government was as corrupt as ever, Pakistan was harboring the Taliban, and the Afghan leader Hamid Karzai was neutral with a very weak and non-pivotal contribution. Obama was certain there was no need to shed more innocent American blood on a lost cause. Effectively, Obama withdrew all his forces from Afghanistan as he saw it realistic to not waste more resources in 'unworthy prize wars' (Gompert et al. 22).

2.5.4. The Humanitarian Intervention in Libya

President Obama's speech addressed the nation on March 28, 2011, intended to explain to the American people the reasons and the nature of U.S. participation in the international coalitions in Libya. This speech was a key political discourse: "the clearest explanation made so far of Obama's foreign policy doctrine." In his speech, Obama explained to his people that the main purpose behind this intervention in Libya was to protect civilians from El Kaddafi's forces. The instrument of power used in Obama's intervention in Libya galvanized a new foreign policy strategy different from the one practiced by President G.W. Bush.

The case of Libya was a clear implementation of Obama's strategy. The president defined The U.S. engagement in Libya as a "Humanitarian Intervention." According to Joseph S. Nye Jr, A well-executed power strategy example, as seen in Libya. Obama waited for the Arab League and the UN resolutions to establish their credibility before constructing a strong soft power narrative. If the U.S. had invaded a third Muslim nation, the headlines would have read "U.S. invades third Muslim country" from Morocco to Indonesia. Instead, it was portrayed as part of a concerted international effort to carry out the UN's mandate to safeguard people (Glaser and Thrall).

Obama's decision was, temporarily, smart by sharing the burden with his allies and NATO to avoid boots on the ground. After all, Libya was in Europe's backyard, and it was smart to encourage the Europeans to take the lead there. However, the mission was redirected to attain other major objectives, like to topple the regime of Gadhafi. This mission ended by killing El Gadhafi, the ex-leader of Libya, and bringing a radical change to the country's regime. The irony that escalated after this intervention was the inevitability of unexpected consequences after the intervention: the Obama administration did not bring any positive change to the area, which was

ravaged by civil conflicts and jihadist militants, and the worst was the open door they provided to ISIS to flood to the country. Admittedly, Obama called the quagmire intervention in Libya a "mess" (Glaser and Thrall).

2.5.5. Critique of Obama Doctrine

U.S.-Russian relations deteriorated to Cold War-era levels. The Russian government under President Putin resumed his challenges to NATO forces in Europe. Russia invaded its neighboring state Ukrainian province of Crimea, supported dictator Bashar al -Assad in Syria, and gave asylum to the American computer intelligence Edward Snowden, who leaked classified information to the media. Furthermore, Putin vigorously interfered in the American presidential election to support the candidate, Donald Trump. Eventually, Putin surpassed his predecessors in his adventurous engagement in making Russia a military and cyber threat to democracy in America. Putin raised Russia to the status of a perilous rival to American security (Suri 207).

Obama's eight years of office were far from reaching his policy goals for the country. He fought for a judicious and engaging foreign policy with Russia. However, his soft policy of reconciliation with Russia was disastrous for American welfare. With this pact of compromising with the Russians, the Obama administration gave the latter a malign power to impose on Europe, the Middle East, and other regions. Furthermore, this escalation and the re-emergence of Russian power increased the possibility of a nuclear power insurgency. Russia's audacious moves threatened the U.S. with the possibility of a new war, and it also surpassed the tension it created in Europe to reach Eastern Europe and Central Asia. Since 2014, Russian marine forces have deliberately led inflammatory operations very close to NATO bases. As Russia ended all its nuclear weapons agreements with the U.S., it enormously elevated its nuclear armament. It

opened a renewed U.S./Russia nuclear arms competition, possibly opening doors to a nuclear weapons war (207).

The ‘New beginning’ speech of 2009 in Egypt did not mark the new beginning that the world expected. Obama’s withdrawal from Iraq and Afghanistan left a huge gap for new terrorist organizations to arise in these areas. Eventually, ISIS, an allegedly ‘Islamic’ extremist organization with poor Islamic education, formed a political network to destroy western supremacy. ISIS used the governmental power vacuum gap of the region and the lack of law enforcement to control and take advantage of the military region to serve their diabolic plans. Unfortunately, Obama and his allies did not act to contain this new rising threat to the Middle East region and the U.S. His realistic engagement policy, when necessary, did not figure any way out of this intervention. The same policy was followed by Putin and his quagmire in Europe and Asia: the U.S. did not initiate any preemption to halt the Russian leader from his rebellious acts. Obama once wisely said: “There are going to be times where either because it is not a direct threat to us or because we just do not have the tools in our toolkit to have a huge impact that, tragically, we have to refrain from jumping in with both feet.” (Goldberg) It was a rational answer from a liberal internationalist leader, but it did not fit the criterion of a liberal country like the U.S.

International thinkers thought, “War is the last resort policy to any conflict.” Obama was one of them; his international strategy in dealing with conflicts was the same. He believed in solving problems through diplomacy and imposed norms and laws instead of military escalation. Obama hesitated in confronting Putin, Iran, and ISIS because he saw that the use of violence would not end the conflict. Furthermore, it has international repercussions on innocent people who have already been through much turmoil in wars and disasters. Though Obama’s legacy was

contradictory to maintaining the U.S. position in the international political system, he undeniably was a ‘deliberative’ president, as the Republican Robert Gates described him. Obama has an extensive international ambition, but he was committed to fulfilling it through peace, negotiation, law, and order but not with any force (Suri 202).

The 9/11 attacks on the United States in 2001 profoundly impacted American foreign policy. The Bush and Obama administrations both responded to the threat of terrorism with strategies that sought to protect national security while also promoting American values abroad. While there are similarities between their policies, each president took a different approach that was shaped by their unique perspectives. Inclusively, it is clear that both Bush’s and Obama’s foreign policies were aimed at protecting America’s national security after the9/11 attacks while also pursuing a path of promoting American values abroad through military force or diplomatic means, depending on the context of the issue at a time. Although their approaches differed, they shared a common goal of safeguarding the nation’s national security from future terrorist threats and promoting peace worldwide through cooperation among nations.

Chapter Three:

Cyber Security A New Threat to American National Security

Cyber security has become a major concern in today's increasingly interconnected world. With the increasing dependence on technology, cyber-attacks have become a significant threat to national and international security. The United States, in particular, has been affected by several high-profile cyber-attacks, leading to significant losses of sensitive information and data. This chapter aims to examine the current state of cyber security as a new threat to American national and international security. It will analyze the impact of cyber-attacks on U.S. national and international security. Additionally, it will explore the measures taken by the U.S. government to address this threat and the challenges faced in doing so. The chapter will provide a comprehensive overview of the current state of cyber security and its impact on American national and international security and the efforts to address the growing threat of cyber-attacks.

Political leaders and observers are newcomers to terms with this game-changing technology. Until recently, cyber security was a realm of computer professionals and specialists. When the internet was developed forty years ago, it was a tiny group of people who knew each other, and they constructed an open system with no regard for security. The commercial Web has existed for two decades but has grown from 10 million users in the early 1990s to almost two billion. This growing interconnectedness has brought huge possibilities and severe weaknesses that strategists still need help with. Strategic studies of the cyber domain are historically equal to the nuclear revolution in military affairs but conceptually more equivalent to 1950 (Burns and Price 48-49),

3.1. Cyberspace as a New Domain in National Security

3.1.1. Cyberspace in Perspective

Cyberspace presents a new setting in which a new set of resources might permit new kinds of power behavior. As a sort of power derived from the availability of information, cyber strength is not novel. Cyberspace may be understood on many different levels, and it has been variously defined. Initial approximations paint it as "a unique hybrid regime of physical and virtual qualities" but this is far from accurate. Current political rules about sovereign jurisdiction and control are strongly tied to the physical infrastructure of Cyberspace (Nye, "The future of power", p. 69), as are existing economic laws regarding competing resources (where usage of a product impacts the experience of others utilizing the same good) and growing marginal costs.

Cyberspace's virtual or informational layer is distinguished by economic characteristics, such as growing returns to scale, and political characteristics, such as difficulty in exercising jurisdictional authority. Attacks from the informational domain, where resources are scarce and expensive, can be conducted against the physical domain. Control of the physical layer, on the other hand, can have both territorial and extraterritorial impacts on the informational layer. Cyber power, as defined behaviorally, is the ability to achieve desired results by exploiting the cyber domain's electronically networked information resources. Cyber supremacy can be exploited to achieve targeted objectives in cyberspace, or it can be used to produce desired consequences in realms outside of Cyberspace (Kahn et al. 8).

3.1.2. National and International Threat Challenging U.S. Cyber Security

The United States faces a diverse range of dangers to its national security in the21st century. However, the greatest threats are those aimed at the easiest-to-penetrate parts of

the cyberinfrastructure. Specifically, distributed denial-of-service (DDoS) assaults, malicious software, and computer viruses have been the major target of attention (Kahn et al. 27-28). Over the past two decades, the greatest threats to Cyberspace have shifted from tactical actors whose effects were merely operationally annoying (shutting down public-facing websites) to finance (credit card -identity theft and fraud) to terrorist groups and nation-states whose strategic planning was to stimulate long-term damage to the economic well-being and national security of the United States. Cyber-attacks are projected to become more frequent and severe as more of the American economy and culture moves online via initiatives like electronic medical records, telemedicine, and "smart grids" (27-28).

An enemy enjoys the advantages of stealth, anonymity, and unpredictability in Cyberspace, where the internet enables worldwide connectivity and access to a rich array of valuable assets of strategic relevance. Every year, the increasing sophistication of computer-based attacks on civilian and military networks around the world raises the bar for cyber security, as does the exponential increase in information volume and the decrease in time distance limits. (Kahn et al. 27-28) Cyberspace has specific qualities and challenges, like land, sea, air, and space. The United States has become more reliant on the cyber domain in many areas, including industry, trade, finance, security, intellectual property, technology, culture, policy, and diplomacy (27-28).

The internet's phenomenal expansion after the 9/11 attacks has created enormous potential for the United States to better its global strategic position: Almost every aspect of American power has been improved by the Internet. On the economic front, the McKinsey Global Institute has predicted that the internet will remain the dominant driver of American economic growth for the next decade. In addition, developing sophisticated social networking

and fundraising platforms has aided the formation of dynamic groups dedicated to furthering the public good. Finally, from a military standpoint, America's mastery of Internet-based communications and weapons gives its forces considerable advantages in modern conflict (Burns and Price 48-49).

In cyber security, defense is far more complicated than offensive. The difficulty of enhancing the United States' cyber defenses is so complex and multifaceted that top national security minds naturally gravitate to more appealing offensive concerns, such as retaliation and first-use policies. Moving forward, it would be beneficial to think thoroughly about innovative approaches for the United States to establish policies that strengthen its cyber defenses. While 'active defense' is an essential aspect of cyber security, even the finest attack cannot compensate for poor defense. As will be discussed further below, many of the policymaking difficulties in Cyberspace are not directly related to traditional areas of national security policy. Instead, important technological and economic policy concerns will contribute significantly to developing cyber security policy (Price 48-49).

In sum, safeguarding information assets in Cyberspace is a national and international interest; the Internet may be America's modern-day counterpart of Clausewitz's 'center of gravity'. Both state and non-state actors recognize that a strike that cripples the nation's networks would be the most damaging blow to the U.S. Fortunately, such a blow is unlikely to occur in the next decade. U.S. opponents and rivals understand that Cyberspace's pervasive and open nature allows them to strike the United States on a modest but considerable scale daily (Burns and Price 48-49).

3.2. Strategic Problems as a Cyber Menace to National Security

For centuries, Mankind only used the land and the sea as their primary domain of operation. The land and the sea were exploited by technology; Humans used technology to make the land and the sea operational. Starting from the creation of the wheel and the war chariot to the main battle tanks. The transformational change erupted the two ordinary domains by adding a third domain, ‘aerospace’. The aerospace birth was just a century ago, but it enormously impacted military, economic, and social aspects. A fourth domain was added in 1957 when outer space was added to the other domains. It was not a very pervasive domain like air space, but still, it had an essential role in linking multiple operations and activities in other environments.

Cyberspace is the fifth domain with a difficult spectrum to define; this new dimension is very complicated to be measurably secured. The national security analogy in the twenty-first century is no longer the same. Current thinking about cyber security as a new domain and as an artificial environment made the community of national security analysts rethink the implications of these new technologies and their impact on the defense system of American national security. The Characteristics of Cyberspace opened a new dimension to another domain of security that should be dealt with in contemporary American security.

3.2.1. Cyber Crime

In 2007 Estonia was attacked not by the military empowerment of any other country but by expert hackers who parallelized its cyber system by distribution denial of service. The act led to panic and severe loss estimated by millions of dollars. This act of disrupting an internet system or software using malicious technical services is an act of cybercrime. This latter is getting highly used and advanced by hackers, terrorists, and many extremists. These cyber-criminal groups use updated software that can secure access to the latest software and their

security codes and hire highly qualified engineers in their organization to ensure the efficiency of their operations. Their resourceful playground is Cyberspace or the internet; they direct, remotely control and deny service to legitimate customers and users using large networks and software. This new stealthy and malicious cybercrime strategy is considered a contemporary threat to national security as it expanded beyond law enforcement to be a benign cradle to cyber terrorism (Nat'L Defense Univ Foundation 416).

The concept of cybercrime or Computer Crime is a crime processed or affiliated with computer use. It could be as simple as fraud, hacking a system, murder, child pornography, and anything that lies between. It is an act that involves the use of a computer to accomplish a task. In current times, this would mean just about every crime committed. The Encyclopaedia Britannica defines computer crime as any crime committed using special knowledge or expert computer technology. Cybercrime or computer crime includes different types of crimes that differ and vary according to the area of the attack and the domain of the assault. It includes "robbery, burglary, larceny, fraud, embezzlement, extortion, sabotage, espionage, kidnapping, and murder, not to mention the crime of child pornography" (6-7).

One of the standard definitions for cybercrime is "cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity". However, the term was generally defined in the Draft of the International Convention to Enhance Protection from Cyber Crime and Terrorism, "cyber-crime refers to acts concerning cyber systems". Other publications gave a more detailed definition to the term by including the objectives and the intention behind this act; they defined it as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks". Most cybercrimes are structured to have a fatal impact on web users. However, a typical cybercrime

attack would have a remote control on specific software and engage other zombie computers to attack the targeted one. It is a very sophisticated, advanced, and controlled attack; it is no longer random (Nat'L Defense Univ Foundation 417).

Cybercrime describes a Worth mentioned category of offenses that triggered computer data and the operating system; it is pictured in computer-related forgery and fraud as phishing, content offenses such as disseminating child pornography, and copyright offenses such as the dissemination of pirated content. Cybercrime is now organized in a profit-making organization that uses the consumers' daily life reliability on the internet as fuel to their ungracious ambitions of making profits from the increasing criminal opportunities they have in Cyberspace (United Nations: Office on Drugs and Crime 203).

The new information age imposed a new rhythm of security in reaction to the new type of cyber criminality. As a result, the users of the web, software, and those who use a digital operational system should be more cautious about how to systematically use their assets. Patrick Taylor, VP of strategic marketing, Internet Security Systems, well demonstrated the previous idea:

> Every company and every computer has some responsibilities for security. If you don't have 'no trespassing signs, it's not against the law to walk on a piece of property. If the door is unlocked, and there are no signs up that say 'do not enter,' is someone breaking the law when they go in and look around? Conceptually speaking, there are a whole lot of computer doors that are unintentionally unlocked. (Curtis 8-9)

3.2.2. Cyber Attack

Nations reacted to the new threat of cybercrime by developing unique programs of protection and security within their traditional armed forces; the rise of cyber-attacks pushed these countries like the U.S., China, Russia, and North Korea to stay on hold and ahead in this domain. The United States created the 24th Air Force, which specialized exclusively in cyber operations and warfare. On the other hand, China, in 2005, incorporated, for the first time, offensive cyber warfare exercises in their cyber-operations training. Russia started using cyber operations as a multiplier force of its armed forces' more traditional, kinetic components. Additionally, North Korea launched its specialized Unit 121 for cyber warfare operations. These countries are preparing for a new era of cybercrime and cyber warfare that began with an undeniable incident in the ^{21st} century (Pool 303).

Cyber-attack was mainly misused when defining an act of cybercrime or any malicious action against the U.S. cyber infrastructure. General William M. Fraser informed the Senate Armed Services Committee that, in 2012, "US Transportation Command was" hit by almost 45,000 cyber -attacks during 2011, and quadruple that number". However, General Fraser used a comprehensive definition of cyber-attack; "not all malicious acts are classified as cyber-attack; they can be classified under different categories". Merriam-Webster defines an attack as "to act violently against (someone or something)". 'someone' in Cyberspace is a U.S. citizen or a U.S. ally, whereas 'something' is U.S. cyberinfrastructure and all its digital operational system.

The Tallinn Manual on the IL, in rule 30, defines cyber security attacks applicable to Cyber Warfare as: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."(Schmitt 91) Yannakogeorgos rose the issue that cyber-attack must fall under the category of an act of

aggression. He believed that the distributed denial-of-service DDoS interference in the U.S. financial system was an act of aggression and hacking and stealing intellectual property as an act of cyber espionage but not as a cyber-attack.

Although both acts of disruption or espionage are not armed attacks and do not exemplify any physical damage to U.S. citizens, they can be an act of cybercrime as consequently, by disturbing, hacking, and stealing intellectual property or causing a system blockade, will eventually lead to a national security response to secure the economic, military or any other domains under U.S. property. Exposing or jeopardizing these sectors by any malicious cyber activity, whether 'disruption' or 'aggressive incident', may lead, automatically, to an act of cybercrime (McKenzie 4).

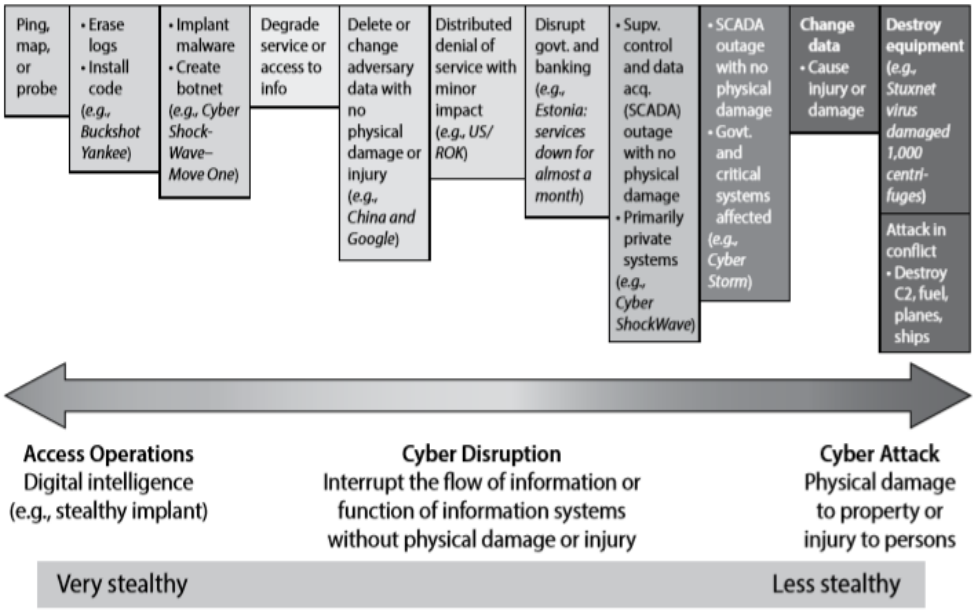


Fig. 2. Spectrum of Cyber Operations, USCYBERCOM/Judge Advocate, Briefing, Subject: Assessing Actions along the Spectrum of Cyberspace Operations, slide 18, no date.

Timothy M. McKenzie, in his report: *Is Cyber Deterrence Possible?* linked the impact of a ‘disruption’ or ‘aggressive incident’ to the reality of cybercrime. Some activities underlined by disruption or aggression could rise to the level of an act of cybercrime and even to an act of cyber warfare. He firmly believed that any theft or stealing of any military or economic U.S. property could jeopardize national security and parallelize the economy, which is the backbone of American prosperity. When any malicious act of cyber causes a financial loss to a company or the U.S. government, it should be considered an act of cybercrime as it attacks, primordially, American national security and its interests (McKenzie 4).

3.2.3. Cyber Espionage

Cyber espionage is stealing data and essential documents without being ceased by using computers or any devices related to, cyber espionage is a strategic collection of data and intelligent information to attain important military, political, technological, and economic data. The assembled data, whether by state or non-state actors, are collected and used to better known information about the competitors. Talking about espionage always leads to the complimentary section of spying, which is used to fulfill a significant part of cyber espionage’ purposes; it mainly uses spies to collect data worldwide. The act of spying is an act that is flexible and less expensive; states or non-state actors can use it. The intriguing thing about spying is that it can be used with or without computer assistance. Cyber spies have multiple objectives for information theft; they use it to intimidate, blackmail, or pre-empt any political act and maneuver it for the opponent’s benefit (Pool 308).

The act of spying was well demonstrated in the 2008 U.S. campaign when cyber attackers stealthily infiltrated both Senator Barak Obama’s and Senator McCain’s computer network systems in research for crucial information about the candidates’ plans. (308). Spying and

stealing information through cyber espionage may jeopardize the U.S.'s vulnerability. So, acquiring sensitive information about the U.S. plans and strategic programs, creates a fatal menace to American national and Cyber safety (Pool 308).

There is an amount of ceased information or attempt to steal them by an act of cyber espionage; this was exemplified in many incidents throughout history, more precisely in the 21st century; most of these attacks are attempted to blackmail or to disorient the array of any political act from its original path, destroy or cease economic chances by destroying an adversary's plan. One of the colossal cyber espionage operations was the 'Titan Rain Operation', where China used hackers to subtract ten terabytes of digital classified documents from the DoD without being perceived. This amount of information is the equivalent of data collected in the library of Congress. Eventually, China's attacks were considered attacks with international standards that directly threatened American National security (306).

In another instance of cyber espionage, A Russian hacker triggered the DoD, NASA, Department of Energy. This operation was named 'Operation Moonlight Maze'. The main objective of this operation was to steal information about the U.S. but not to destroy any operating system or software; the hackers were focused on extracting the most data and information possible about the U.S. military, economic and political system of operation and plans. This was well demonstrated by Richard Clark, a security expert in the field of cyber security, who associated this act of espionage with an innovative pre-war reconnaissance to find the 'goofs' of the system. A similar incident occurred when hackers could access Lockheed Martin's digital networks and obtained terabytes of information on the F-35 fighter aircraft developed by the United States Air Force. These acts of attack that were arranged under an act of cybercrime raised the global community's awareness of the size of cyber espionage and other

cyber assault that was occurring with large amounts in a blank of an eye but with catastrophic impact wherever it is used (Pool 306).

3.2.4. Cyber War

The act of cyber war is conducted in Cyberspace by state or non-state actors to mislead the enemy about the attack's origin. The conductors of cyber war acts use weapon information systems effectively to attain targeted political objectives. Like all wars, cyber war has its characteristics; it can be regular or irregular; it is regular when it is between the military forces of two states or more, but it is considered an irregular war if it occurs between official and non-official states and non-state actors. One reason for these cyber wars is the search for the legitimacy of recognition and manipulation of power. The specific thing about this type of war is that it can be a total cyber war that happened within the digital world, as it can be a partial cyber war and be a part of other domains' (air- marine- land) of war (Kahn et al. 18).

Though there are many definitions for cyber war, a concrete and practical definition still needs to be found as the world did not witness any cyber war yet. However, it has been easier to define cyber war in theory; it differs from the physical war in its effects; it can cause emotional devastation but not bloodshed warfare. Cyber war can destroy a system or a digital program but never kill people directly, which makes it less damaging than real warfare. According to experts in Cyberspace and cyber-attacks, to designate a cyber war, it should have devastating damages: "states should define cyber war more narrowly to encompass only acts that result in a significant level of damage. . ." (18).

3.2.5. Cyber Terrorism

Cybercrime is directly or indirectly credited to terrorists. However, it is sometimes hard to determine the attribution source. However, the link between criminality and terror groups

seemed to be very likely to be identified and, worst, to be expanded internationally because of the new means of communication and the digital world of information. Terrorist acts may enlarge their scope within countries through communication, social networks, and digital infrastructure. The terrorist network enlarged through the virtual world with highly skilled technology and computer specialists; this step forward in the world of terror made it easy for terrorists to reach much infrastructure without traveling. The car bombing attacks on the United Kingdom was an alarming sign of the spread of terrorist activities to reach the digital world; London police affirmed that the explosive used in the 2005 attacks were purchased from criminals in Eastern Europe. Terrorism is now connected unwillingly to the international digital world, which makes it a new affected zone. Regarding the potential threat in cyberspace, cyberterrorism was introduced to the digital world as one of the fatal cybercrimes (Nat'L Defense Univ Foundation431-432).

The DoD, the State Department, and the FBI agreed that terrorism is "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."(438). Regarding the linkage between both terrorism and cyber terrorism outcomes, the definition of cyber terrorism can be drawn from the same context with an enlarged scope of applicability; Cyber terrorism is viewed as:

> A computer-based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of political, religious, or ideological goals. The attack should be sufficiently destructive or disruptive to generate fear comparable to physical acts of terrorism. Attacks that lead to death or bodily injury extended power outages, plane crashes, water contamination or significant

> economic losses would be examples. . . . Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber terrorism]. (Nat'L Defense Univ Foundation 438)

The distinction between the nature of cyber terrorism as a threat conducted through the digital world has the same impact as a physical terrorist threat or may differ depending on the sector of the attack. In addition, the distinctive means of the attack makes the rigor of the threat (Nat'L Defense Univ Foundation 483). Cyber threats include cyber terrorism, hacktivism, cybercrime, cyber espionage, and state-level information warfare. All these types are well explained in the table below.

Table 1
Cyber Threats: Defining Terms

	MOTIVATION	**TARGET**	**METHOD**
Cyber terror	Political social change	Innocent victims	Computer-based violence destruction
Hacktivism	Political social change	Decisionmakers Innocent victims	Protest via Web page, defacements, or distributed denial of service (DDOS)
Block hat hacking	Ego, personal	Individuals, companies, governments	Malware, viruses, worms, and hacking scripts
Cyber crime	Economic	Individuals, companies, governments	Malware for fraud, identity theft, DDOS for blackmail
Caber espionage	Economic and political gam	Individuals, companies, governments	Range of techniques to obtain information
Informatio n war	Political or military gun	Infrastructures, information technology systems and data (private or public)	Range Of techniques for attack or influence operations

Adapted from: Nat'L Defense Univ Foundation, 439.

Hacktivism, unlike cyber-terrorism, is taking control of the information in Cyberspace to impose a political ideology. Hacking is an illegal act of infringing a computer information system. It can be malicious or benign. The benign hacking called 'white hat' is the act of hacking a system with the owner's approval to find out the faintness of the system and repair it. However, the malicious one, named "the black hat," refers to the infringement of a digital system based on its flaws. The purpose of the hackers and their motivations differs depending on the hacker's personal motive; some hackers find the act as a personal achievement, and some see it as a

challenge to their capacities and skilfulness in the digital world, so they hack the most complicated and valuable system to prove their uniqueness. However, the most common reason for hacking is financial gain, such as money laundering. Hacking for financial gain is one of the world's most common types of cybercrime (Nat'L Defense Univ Foundation 440).

Though cyber-attacks are not the only system subjected to attacks, the monetary system is susceptible too. However, the cyber system as a monitor of all domains is more exposed to cyber-attacks. It can be due to many technological imperfections, but the most noticeable attacks are viruses and DDoS attaccks. DDoS is considered one of the most scaled internet attacks; it takes control of thousands of computers and makes them an army of what is called (zombies or botnets). This army of computers (zombies) is considered a secondary victim since their owners do not know their computers are infected by malware. The DDoS attack uses them to overflow the primary target victim, a network, a website, or a computer (Demchak 39).

The incorporation of a zombie program in a secondary victim can be done months before the DDoS attack takes place. It is almost easy to infiltrate a computer and imperceptibly install a zombie program. Noticeably, the system's vulnerabilities in the software make it accessible to be installed through new programs, updated, and configured. During the DDoS attacks, the zombie sends an innocent request to the primary victim; this request sounds legitimate to this website. The serpent way of infiltrating the system will aggravate when thousands of these zombies flood the website with requests that will overwhelm it and make it unable to respond to legitimate requests. Thus, it declares a denial of service (DoS). It is called a distributed denial services attack because the inundating number of requests came from zombie computers worldwide (Lee 39).

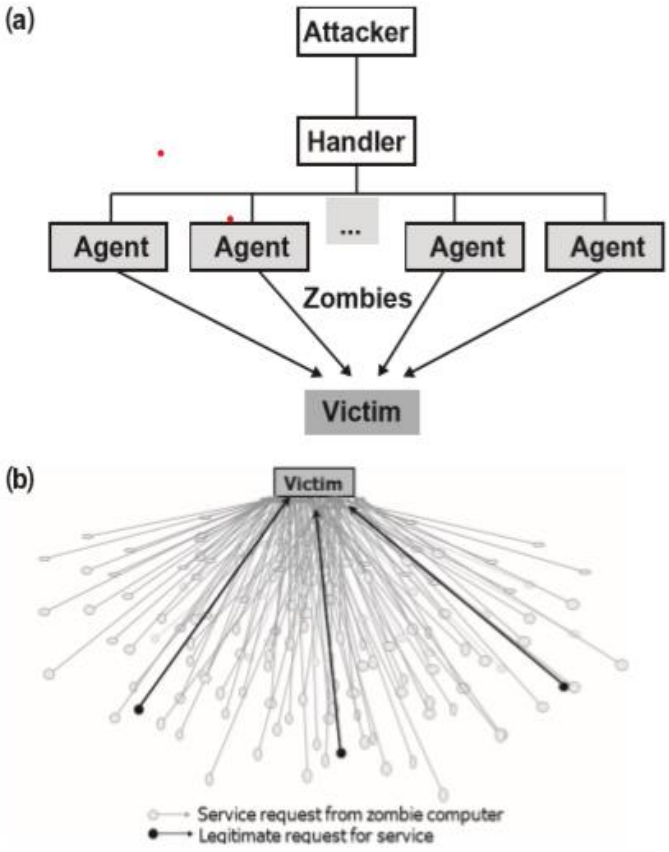


Figure 1. Distributed denial-of-service (DDoS) attack: (a) Example of a DDoS attack network; (b) DDoS attack flooding a primary victim site.

Fig. 3. Distributed Denial-of-service (DDoS) Attack

Finding the DDoS attacker is nearly impossible; the attacker will hide behind the secondary victims, tens of thousands of computers; it will be hard to trace them because they will be in countless misleading directions by using (handlers), which are themselves infected computers. Furthermore, the DDoS attack generally uses tiny storage computers with slow networking activities; this allows the attacker to 'run under the radar and will not be visible to the zombie computer's users. With this malware mechanism and with the magnitude of the number of zombies involved in the distribution of the request against the primary target victim, the DDoS can be more than an attack; its potential to parallelize the world information infrastructure makes it a new ideology of cyber war (Lee 49).

Cyberspace, or the cyber world, is a new revolutionary dimension with vital infrastructure made of interconnected operational systems, software, electromagnetic communication, people, and users. Unfortunately, this domain's physical and electronic infrastructure is vulnerable to security breakdown, attacks, infiltrations, accidents, and espionage. System vulnerability, what is known as the 'cyber-attack', has always been acrucial concern of the National Strategy to Secure Cyberspace states:

> By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten Cyberspace occur in the information assets of critical infrastructure enterprises and their external supporting structures, such as the mechanisms of the Internet. Lesser secured sites on the interconnected network also present potentially significant exposure to cyber-attacks. Vulnerabilities result from technological weaknesses and improper implementation and oversight of technological products. (Bush xi)

3.3. Major Attacks in cyber history

3.3.1. The Cyber Attack, Estonia 2007

Estonia is considered one of the western states where its government operations rely on an electronic network and a digital operational system. In 2007, 60% of Estonians used the internet in their daily activities and transactions. Further, 90% of the banks' transactions are made electronically. As estimated, this dependency on digital networks in the Estonian government system made it a model of a 'paperless government', confirmed the Estonian Ministry of Defense. However, alongside the myriad benefits of the information age, there is a nascent threat like global cyber-attacks and information warfare (Herzog 52-53).

In April 2007, a target computer was overwhelmed by messages and denied legitimate traffic services. Furthermore, the attack incapacitated several government ministries' parliamentary email servers and IT capabilities, as it paralyzed the state's capability to respond effectively to the attack. Consequently, the attack was directed to parallelize Estonian society. This DDoS attack was directed at the Estonian computer infrastructure, by which public websites suddenly received tens of thousands of order requests from all over the world, which disabled them by overloading the servers' capacity, to run these sites and resulted dramatically in a DDoS attributed the attack on the Estonian government system (Herzog 52-53; Kahn et al. 44).

The Estonian government responded to the attack using the Computer Emergency Response Team (CERT); this latter closed all the foreign servers under attack and the foreign internet transactions servers. Many security experts from various European countries, such as the European Network and Information Security Agency (ENISA) of the European Union and the NATO CERTs, have reinforced the CERT in their resilience against the attacks in an attempt to recover the cyber network proficiency (van der Meer 2). the attack's caliber was very low and luck technical sophistication in its distribution. The attack has not reached the degree of warlike (Kahn et al. 44).

3.3.2. The Cyber Attack on the U.S. in the Middle East, 2008

Another system infiltration that is considered a severe cyber-attack took place in 2008 in the Middle East, when a USB drive infected the U.S. DoD's command and control system. The code reached classified and unclassified systems and established a digital base from which data could be transferred to other sources under foreign control. This rogue program operates silently; it is not easy to detect that it is already operational in a given system; it was intended to unlock and pass the secret operational programs to the attacker or the adversary. This stealthy network

was the worst fear the DoD had ever faced; the Pentagon's operation resilience against the attack, known as Operation Buckshot Yankee, made a turning point in U.S. cyber defense strategy.

The attack by a foreign spy service was considered an unprecedented breach of the DoD system: "This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call", warning Deputy Secretary of Defense William Lynn. Though the impact of this attack on the American DoD system was not fatal, breaching a military system was to be considered a sign of an upcoming danger of cyber-attacks and malware infiltration in the U.S. DoD system (Kahn et al. 45).

3.3.3. The Cyber Attack, Saudi Arabia 2012

In August 2012, a cyber-attack targeted the oil and gas production in Saudi Arabia and the oil export companies to the rest of the world. The attack triggered the most significant oil company Aramco. The attack was attributed to a computer virus called 'Shamoon'. The unknown hackers targeted Saudi Arabia for crimes and genocides in Syria and Bahrain in response to Saudi Arabia's support for rebel groups in Syria and troops sent to Bahrain to support Sunni Muslims against Shia protesters. More than 30,000 computers were destroyed in Saudi Arabia and joint companies worldwide due to the cyber-attack. The attack aimed to prevent the company from exporting oil to the rest of the world, harming Saudi Arabia's economy and unbalancing the global economy. The hackers failed to achieve their ultimate goal of disrupting oil and gas exports, and the damage was limited to office equipment and computers, according to the Aramco company (van der Meer 3-8).

The cyber assault was a perilous advancement in international hacking as it represents the willingness and the aptitude to cause physical damage. The attack did not target data, a system,

or a network; it was oriented to crack down on the company's operations and terminate the foundation with an explosion. Investigators and intelligence analysts were very concerned with the fact that hackers could manipulate the most powerful controlling system that rules most of the operating equipment in the world; Schneider's Triconex equipment is used in about 18,000 plants, including; nuclear water treatment facilities, oil and gas refineries, and chemical plants. By making this invulnerable system a vulnerable one, James A. Lewis, a cyber security expert at the Center for Strategic and International Studies, strongly believed that: "If attackers developed a technique against Schneider equipment in Saudi Arabia, they could very well deploy the same technique here in the United States" (Perlroth and Krauss).

The August attack was supposed to be more fatal than what had happened; what saved the Saudi Arabian company was not the strength of Schneider's system but a mistake in the hacker's computer code that unexpectedly blocked the plant's production system. Amy Myers Jaffe, specialized in Middle East energy at the Council on Foreign Relations, pointed out the particularity of selecting the petrochemical sector was an attempt to sabotage Saudi Arabia's economy; "Not only is it an attack on the private sector, which is being touted to help promote growth in the Saudi economy, but it is also focused on the petrochemical sector, which is a core part of the Saudi economy".Investigators and analysts believe that the hackers overpassed the local system hacking to focus on international companies and enterprises; by fixing their mistake, they will play on a high-level attack and deploy the same technique against another industrial control system (Perlroth and Krauss).

3.3.4. The Cyber Attack, United States 2012

After Saudi Arabia, in September 2012, the United States had a cyber assault, considered the biggest cyber-attack in history. The attack was launched against the six leading banks in the

U.S.; an organized DDoS attack was directed to the banks' websites to overload them and deny responses to network legitimate network requests. Eventually, the website ran slowly and was not reachable to the banks' customers. Though the cyber-attack did not heavily affect these banks' computer networking and operational system, it still caused panic. The attack, fortunately, needed to be prepared with expertise and lack the tactic of an actual attack; otherwise, the economic damages might be devastating (van der Meer 4). In cooperation with cyber security companies, the hit banks resolved the problem within their companies.

Nevertheless, the companies lost tens of millions of dollars to fix the damages made by this cyber sabotage. Though the companies affected were in a self-recovery mode, specialists from different domains, government agencies, and departments: such as the DHS, the State Department, the NSA, and the Cyber Command of the U.S. Armed Forces, assisted in this resilient operation of recovery (4). As the government's diplomates and cyber security experts found a partial solution which sounds more diplomatic than technical. The State Department called for urgent assistance from 120 countries, demanding immediate elimination of the identified malware computer codes used as agents to accomplish the DDoS attack on all the servers worldwide. Christopher Painter, the State Department's coordinator for cyber issues, said in an interview: "The pitch was, 'We're making a request of you, and we would really like your help. You have just as much interest in taking action because these are compromised machines. Please do what you can to mitigate this threat". Though mobilization of the international cyber sphere to help stop the consequences of this attack did not end, it decreased the impact considerably as it gave more space and time to the bank technicians and cyber security specialists to lessen the impact of this assault (Van der Meer 6).

3.3.5. The 2016 Elections: The Russian Meddling in U.S. Elections.

The act of meddling in the American cyber system has a history that goes back to 2014 when the Russian hacker started to look for a vulnerable spot in the election infrastructure at the state and local levels to get through. According to the report of the *Select Committee on Intelligence of the United States Senate,* held *On Russian Active Measures Campaigns and Interference. In The 2016 U.S. Election.*

> Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections------Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities targeting the voting process---------the Committee found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes ------. (U. S. Senate 5)

The Senate report made by a sensitive Committee directed to *Russian Investigation Only* found tangible evidence that condemns the Russian government. It targeted the U.S. elections to disbalance the American democratic institution and shook their confidence in the election process (U. S. Senate 6).

Before the 2016 elections, in mid-July, the state of Illinois found suspicious net activity with an increase in outbound data in its election infrastructure cyber system, specifically on the board of voter registrations. The act resulted in data exfiltration from the voter's registration database. The FBI investigated the subject matter; on August 18, 2016, they sent a FLASH alert of a potential cyber threat to all government and private sectors to strengthen the system against

this imminent threat. The threat or the FBI FLASH was an ID “addresses identified from Illinois’s voter’s registration database” (FBI FLASH, lumber T-LD1004-TT, TLP-AMBER, August 18, 2016). The DHS and the Multi-State-Information Sharing & Analysis Center requested all the states to verify their log files if their infrastructure was affected by the FBI FLASH. Eventually, the DHS identified 20 other states affected by the August FBI FLASH alert. Their servers are connected to at least an IP listed on the alert (U. S. Senate 5).

In an interview with the Coordinator, Michael Daniel, the former Special Assistant to the President and Cyber security Coordinator reported to the National Security Council, held on August 31, emphasizing: “eventually we get enough of a picture that we become confident over the course of August of 2016 that we’re seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure regularly”. Another SSC Record of the Russian Interference Hearing, in the 2016 U.S. Dr. Samuel Liles testified that: “by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors” (Qtd. in U. S. Senate 5).

This state-directed act of breaching the 2016 U.S. presidential election voter registration process was conducted to undermine the American democratic process and influence the campaign’s credibility and fairness. The most targeted in this Russian meddling was the Democratic candidate, Hillary Clinton; they aimed to denigrate and harm her chances in the electoral process and affect her potential of winning the presidency. The Russian government’s impact and involvement not only targeted the democratic process of the election, but it also overpassed that to hack political organizations such as the Democratic National Committee and

Democratic Congressional Campaign Committee. This leaking of emails was envisioned to weaken Hillary Clinton's chances of winning the candidacy (Galante 9-10).

Hillary Clinton, in *the New York Times,* accused Russian intelligence of meddling with the American election and attempting to undermine the American democratic process. She emphasized that President Vladimir V. Putin saw Donald J. Trump's victory as an advantage to weaken American strength and upraise Russian interests in the area. Hillary surprisingly expressed herself by saying: "It's almost unthinkable", referring to recent "credible reports about Russian interference in our elections". She was more concerned with the fatal threat of this hacking; she said in a conference. "I want everyone — Democrat, Republican, Independent — to understand the real threat this represents". She asked for vigilance and readiness against other cyber threats that target the U.S. elections as it is, as she put it, "a threat from an adversarial foreign power". The adversary, the Russian government, as she pointed out several times without bringing it plainly to the public. She made it clear by using the Arkansas saying, "If you find a turtle on a fence post, it didn't get there by itself", but she never declared it directly (Chozick).

Russian government led by Vladimir Putin denied its implication in any cyber-intrusions in the United States elections or hacking the emails sent by the Democratic National Committee in July. Putin has refuted allegations made by the United States against the Russian government by officials from that country. Despite the fact that he thought about the allegations as a "distract the public's attention", he intensified the hacking act by adding, "It doesn't really matter who hacked this data from Mrs. Clinton's campaign headquarters, Putin stressed in an interview with Bloomberg News, referring to democratic presidential nominee Hillary Clinton. "The important thing is the content was given to the public" (Priest et al.).

The Attacks were proved to be malware previously used by “APT 28 and APT 29” in a statement to the Washington Post, Mandiant researcher Marshall Heilman confirmed the Mendiant’s names to be: Fancy Bear (APT) 28: and Cozy Bear (APT) 29: hacking groups. The APT 28 is a Russian hacking group sponsored by the government; these hackers have conducted highly-profile cyberattacks since 2014, including the German Bundestag and the 2016 U.S. elections. The U.S. Department of Justice and the intelligence agencies agreed that APT 28 is Russian military intelligence called GRU. Whereas APT 29, known as the “Cozy Bear/Cozy Duke”, is also considered a Russian-supported hacking group, identified as the malware that interfered in the networks of the U.S. Democratic National Committee (DNC), the U.S. Department of State, and the White House. This APT 29 was part of the Russian Federal Security Service FSB (Nakashima).

Jonathan Masters, in an article, to Council on Foreign Relations entitled “Russia, Trump, and the 2016 U.S. Election”, asked whether Trump J. Donald conspired with Russia to hack into the DNC email accounts. The act would be an abridged violation of the Computer Fraud and Abuse Act. He saw that ‘collusion’ and ‘coordination’ are a purified form of what the real terms used should be as a criminal conspiracy instead of all other terms. Donald J. Trump denied his involvement in this conspiracy. However, he admitted that he and his campaign members, including: Paul Manafort, Jared Kushner, Jeff Sessions, and Michael T. Flynn, have been in touch with Russian officials but under a lawful protocol (Masters). The investigation conducted by special prosecutor Robert Mueller found a remarkable change in spotting members from Trump campaign and later from his administration involved in the conspiracy.

In October 2017, Mueller got a guilty plea from Trump’s associates that showed the involvement of two others; George Papadopoulos, a foreign policy advisor to the Trump

campaign, confessed to being guilty of making false statements to the FBI about meetings with Russian nationals. Paul Manafort, Trump's former campaign manager, and Richard Gates, Manafort's business partner. These associates of Trump's campaign were convicted guilty and charged with conspiracy, laundering and alleged lobbyist to the Russian government of Ukraine for over a decade (Masters).

In February 2018, Mueller accused thirteen Russian people, three in business, and the Internet Research Agency, of conspiracy to betray the United States government. The circle of conspiracy was getting more significant. Mueller and his prosecutors gained a guilty plea from Alex van der Zwaan, a Dutch-born attorney and son-in-law of a Russian billionaire. This latter confessed to lying to the U.S. investigators about his coalition with Gates while lobbying the government of Ukraine. The Prosecutor gained another plea condemning. Paul Manafort and Richard Gates for filing false tax returns and committing bank fraud; Gates was convicted of lying to federal investigators and conspiring with the United States (Masters).

In the on June 21, 2017, before the Select Committee on Intelligence of the United State Senate under the testimony of Jeanette Manfra, Acting Deputy Under Secretary for Cyber security and Communications, confirmed what the report published by I&A in October 2016, that the government network went through suspicious malware targeting the election infrastructure. She clarified in her testimony that; "While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors" (Written Testimony of I&A Cyber Division 10).

Jeanette Manfra, assessing Russian interference and activities in U.S. elections, confirmed that the Russian breaching did not affect the U.S. elections' tallying:

> Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. "Additionally, "DHS assesse [d] that the types of systems Russian actors targeted or compromised were not involved in vote tallying." As we continue judging any newly available information, DHS has not altered any prior assessments. (Written Testimony of I&A Cyber Division 11)

3.4. International Initiatives to Face the Threat Challenging U.S. Cyber Security

3.4.1. The International Strategy of Cyberspace

"This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history."

—President Barack Obama, May 29, 2009

On May 16, 2011, the Obama Administration unveiled its International Strategy for Cyberspace: Prosperity, Security, and Openness in a networked world. According to President Obama, this strategy is "the first time that our nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues." In addition, the Obama Administration emphasized the need to "build the rule of law" through international norms and processes in developing an approach to maximize the advantages of Cyberspace and reduce the hazards of its increased usage. This Insight discusses the International Strategy and the role that the Obama Administration envisioned for the future of Cyberspace in international law (Fidler 5).

The Obama Administration aims to integrate economic, security, and political aspects of U.S. cyber policy into an overall, cohesive strategic framework in the International Strategy. This strategy aims to foster the social, economic, and political benefits that a networked world brings to individuals, communities, and nations while tackling dangers that weaken the Internet's

value for communications, trade, and international collaboration. This work is guided by “core commitments to fundamental freedoms, privacy, and free flow of information”. The International Strategy acknowledges the age-old contradiction between security and liberty in pressing for more cyber security and wider Internet freedoms. However, it claims its strategy “supports our national security and advances our common values” through the “rule of law” in international Policy (Fidler 5).

3.4.1.1. Purpose, Principles, and Policy Pathways

The International Strategy aims to make cyber-technologies open, interoperable, secure, dependable, and stable. Pursuing these goals on a global scale requires the U.S. to participate in coordinated efforts through diplomacy, defense, and development programs. The International Strategy served as a ‘roadmap’ for United States government departments to “better define and coordinate their role... to execute a specific path forward, and to plan for future implementation” (Fidler 25). To support such operations under the International Strategy, the United States Government prioritized seven areas of activity.

1-Economy: supporting worldwide norms and open markets that are innovative.

2-Protecting U.S. networks through improving security, dependability, and resilience.

3-Extending collaboration and the rule of law in police enforcement.

4-Military: preparing for security problems in the twenty-first century.

5-Internet governance: fostering inclusive and effective structures.

6-International Development: Capacity Building, Security, and Prosperity.

7-Internet freedom: defending essential liberties and privacy.

The United States realized that the expansion of these networks posed significant risks to. national and economic security and global security (Fidler 25).

3.5. The United States' Role in the Future of Cyberspace

To actualize this vision and contribute to the spread of constructive norms, the United States will combine diplomacy, defense, and development to boost prosperity, security, and openness so that all can benefit from networked technology. These three methods are crucial to the United States' foreign operations. The U.S. was instrumental in forging a new post-war architecture of international economic and security cooperation in the second part of the twentieth century, where they will strive in the same spirit of collaboration and collective responsibility to fulfil this goal of a peaceful and dependable internet (Fidler 8-15).

The international strategy's norms are specified as objectives to be accomplished and achieved effectively if these standards are followed and respected. The following are the objectives:

1-A Cyberspace That Empowers: The United States will work on a global scale to promote an open, interoperable, secure, and dependable information and communications infrastructure that facilitates international trade and commerce, strengthens international security and promotes free expression and innovation. To achieve this purpose, U.S. will create and maintain an environment in which responsible behavior standards guide state activities, maintain partnerships, and support the rule of law in Cyberspace.

2-Diplomatic Goal: The U.S. will work to create incentives and consensus for an international environment in which states engage and serve as responsible stakeholders, recognizing the genuine value of open, interoperable, secure, and reliable Cyberspace.

3-Defense Goal: The U.S. will support responsible behavior and oppose those who seek to disrupt networks and systems, discouraging and deterring hostile actors while retaining the right to protect these critical national assets as required and appropriate.

4-Development Goal: The United States will facilitate cyber security capacity-building in other countries, directly and via international organizations, to ensure that every nation can safeguard its own digital infrastructure, improve global networks, and forge tighter alliances in the consensus for open, interoperable, secure, and reliable networks (Fidler 8-15).

The International Strategy for Cyberspace provided the United States with a clear vision for behavioral standards that would make Cyberspace wealthy, safe, and open. The government now need a strategy for implementation. Regardless how clear the President's vision is, various agencies will interpret plans, authority, and priorities differently. Without execution and accountability, interagency coordination—a significant difficulty in cyber security—failed. Departments and agencies would be in charge of engaging overseas partners and might utilize a variety of incentives to reach an agreement with their counterparts. Although the private sector is an important partner, it cannot be expected to respond to the same incentives as government agencies or foreign partners. The importance of implementation in resolving these potential sites of disagreement and stress cannot be overstated. Furthermore, given the vast, dynamic, and uncertain technology change rate, challenges, opportunities, and progress toward the strategy's goal, it should be viewed as a real-time snapshot that should be revised frequently (8-9).

In his 2011 Union Address, President Obama wanted to meet this generation's 'Sputnik' moment with a significant investment in research, development, and innovation. In response to an external economic and political danger, the President has linked economic success, technical innovation, and national security to an implicit set of national goals. "After investing in better research and education, we did not just surpass the Soviets; we unleashed a wave of innovation that created new industries and millions of new jobs," President Obama remarked (Fidler 8-9).

Cyberspace will always be a flawed environment. Attacks will occur, and despite its pursuit of international rules, the U.S. must learn to function efficiently in Cyberspace full of corrupted networks, defective systems, and susceptible users, where risk will never be zero and people will remain a fundamental weakness. However, resources are a zero-sum game that must be led by priorities, which are founded on assumptions and produce expectations (Fidler 8-9).

However, while these programs addressed and characterized the danger to U.S. cyber systems, they still need to represent a cohesive perspective of the problem and solution sets. For example, at one end of the scale, some view cyber threats as potentially catastrophic, imagining cyber battle scenarios that might result in the extinction of U.S. civilization. On the other end of the spectrum, others argue that the issue of cyber security is overstated and simply a matter of updating virus protection and excellent police work. To those who have spent time in the security community after the 9/11 attacks, this will sound familiar: those who argue that terrorism is a criminal problem that must be addressed by law enforcement and those who argue that terrorists have declared a war that must be fought with military capabilities (Burns and Price 193-194).

In the case of terrorism, the divide between these approaches is oversimplified, and even more so when it comes to defining a plan for securing U.S. cyber assets. Forcing cyber security into a more specific unified framework limits options while underestimating the complexity of the most innovative and significant disruptive danger to national security since the nuclear age. Cyber threats will occasionally be a fundamental facet of military posturing and warfighting, and when they are essential, all aspects of national power will be required to respond. On the other hand, much harmful activity occurs at the business and individual levels, where military techniques are inappropriate, and the perpetrators are mainly from the private sector (Burns and Price 193-194).

Cyberspace emerged as a new domain in American national security; it has become a significant concern for American national and international security. Cyber-attacks that the U.S. encountered, from the cyber-attack in Estonia in 2007 to the cyber-attack in the 2016 elections, have profoundly impacted U.S. national and international security. The increasing reliance on technology has made it easier for cyber criminals to access sensitive information and disrupt vital systems, leading to significant economic, political, and security consequences. Though the government has initiated several measures to address this threat, including the development of policies, resources, and new programs in cyber security to improve this field, the immensity of the threat is aggravating and urges for new policies.

Chapter Four:

The Synergy between Federal Agencies and Higher Education in Promoting Cyber Security Programs

Cyber-attack threat continues to grow as the world becomes more interconnected through technology. This has made cyber security a serious issue for governments across the world. The United States government has taken several initiatives to address this problem, including developing partnerships between federal agencies and higher education institutions. This chapter examines the synergy between federal agencies and higher education in promoting cyber security programs and the impact of this partnership on the development of cyber security programs, including the implementation of policies and the creation of educational initiatives. Additionally, it will explore the challenges these partnerships face and the strategies used to overcome them. The chapter will comprehensively analyze the relationship between federal agencies and higher education institutions and their impact on cyber security.

The increasing dependence on technology and the growing threat of cyber-attacks have made cyber security one of the top priorities for nations across the world. The United States has taken several initiatives to build a strong cyber security personnel to protect its information data. This chapter explores the various initiatives the U.S. government took to build a national cyber security capital. The study will analyze the impact of programs such as Scholarship for Service, the Center of Academic Excellence, and the National Initiative for Cyber security Education on the development of a skilled workforce. Furthermore, the paper will examine the challenges faced by these initiatives. The chapter will provide valuable insights into the U.S. government's efforts to address the shortage of skilled professionals in the field of cyber security and the steps taken to build a strong cyber security workforce.

The emergence of cyber security challenges is traced back to the mid-1990s when the Internet became commercially available. Consequently, the entire profession has a lifespan of fewer than twenty years. Since then, cybercrime, cyberespionage, and cyber warfare have taken on real-world implications. Therefore, it is absurd to expect the modern way of life to be properly preserved until a single, widely agreed definition of the area and the profession exists. Nevertheless, despite its sudden national importance, there is a dispute regarding the correct set of activities to prevent damaging or hostile actions. Cyber security is an ill-defined field open to various interpretations by many special interest organizations. Since there has been no clear definition of the subject until now, the profession and the actual security of computers and data tend to have a lengthy record of accomplishment of failures (Kohnke 2-5).

The uncertainty on what defines the proper elements of the field or profession of cyber security stems from the principles of multiple disciplines. Some content from a range of fields may fall within acceptable boundaries, including the following different areas:

-Management of a corporation requires an understanding of many different areas, including security policy and procedure, disaster recovery and business continuity planning, human resource administration, and contract and regulatory compliance.

- Traditional computer security technical disciplines, such as computer science, provide insight into protecting information throughout its electronic processing.

- Networking expertise provides vital guidance for protecting data during transmission and storage in digital form.

-System and software assurance elements like testing, reviews, configuration management, and lifecycle process management are expanded upon in software engineering.

-Important insights into issues like protecting intellectual property and copyrights, enforcing privacy protections, litigating computer crimes, and investigating hacking incidents come from the legal and judicial systems. Discipline, motivation, training, and the validation of acquired information are only a few of the essential human qualities that behavioral scientists investigate. - The complexity of the situation is further increased by the inclusion of the ethical considerations of information usage, information protection, and standards of behavior (Kohnke 2-5).

All of these areas can contribute to the broader objective of information protection. Therefore, it seems logical to combine the principles and procedures from each domain into the overall body of cyber security best practices. However, there is still debate regarding where the line should be drawn or where the emphasis should be within those limitations (2-5).

As part of national capacity-building programs, workforce development, and education-specific research, numerous areas of cyber security education have been examined. In developed economies, the U.S. Department of Homeland Security, the U.S. National Institute of Standards and Technology (NIST), the U.S National Security Agency, the UK Government Communications Headquarters, the United Nations UN, the European Union EU, “think tanks” such as the RAND Corporation, Booz-Allen Hamilton, and the SANS Institute, among others, have exhaustively documented the scarcity of cyber security professionals and strategies for improvement (2-5).

The United States acknowledges education as a vital component of its national cyber security preparation and has enacted legislations and strategies to enhance cyber security education and the workforce. The NICE was established to improve the long-term cyber security posture of the U.S. It addresses awareness, formal education, professional training, and the

structure of the labor force. In support of this program, the NIST developed the National Cyber security Workforce Framework, which provides a uniform language (lexicon and taxonomy) for use by academia, industry, and government. This consists of seven cyber security areas of provision, job roles, and associated skills utilized by several U.S. colleges to construct academic programs. These programs are also supported by a skilled specialists (i.e., individuals with extensive experience in cyber security) that U.S. educational institutions may locate in the sector. Despite high sector compensation, educational institutions participating in RAND's 2014 poll indicate having no difficulty attracting cyber security workers. The United States needs help to build its cyber security personnel effectively. A study by the SEI reveals issues regarding the appropriateness of cyber security practices implemented by the workforce in the workplace, as well as worries regarding the workers readiness to secure IT infrastructure successfully (Catota et al. l, 2).

4.1. Nexus between Agencies and the System of Education

4.1.1. National Science Foundation NSF

The NSF funds fundamental research and education in non-medical sciences and engineering. The National Science Foundation Act of 1950 established the foundation as an autonomous federal body to "promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." The NSF is a key source of federal funding for university research in the United States, particularly in social sciences, mathematics, and computer science. It is also responsible for a sizable portion of the federal science, technology, engineering, and mathematics (STEM) education program portfolio, and government STEM student aid and support (Harris).

The NSF is a separate federal agency. Despite being subject to legislative and administration budget and monitoring processes, NSF's independence has given it greater institutional autonomy than some federal agencies. Some commentators argue that this autonomy safeguards the NSF's scientific goal. It may also be regarded as competing with other public values, such as accountability. The NSF's constant policy theme is the struggle between independence and accountability. It can be seen in previous discussions about the agency's authorization term and the role of Congress in issues like grant-making and research priority (Harris).

The National Science Foundation (NSF) has seven directorates that promote science and engineering research and education, mostly academic subjects arrange in this directorates. NSF directorates are further subdivided into divisions that handle programs (usually four to six divisions or offices per directorate). In addition to these seven directorates, the Office of International Science and Engineering (OISE) and the Office of Integrative Activities (OIA) oversee NSF-wide projects (OIA). Among various cross-directorate and agency-wide investments, two areas of particular focus at NSF and congressional interest have been artificial intelligence (AI) and the agency's "Big Ideas," which the agency defines as "bold inquiries into the frontiers of science and engineering that endeavor to break down the silos of conventional scientific research to embrace cross-disciplinary and dynamic research." (Harris).

Typically, colleges, universities, and academic associations receive approximately 80% of NSF research and education expenditures. The balance is divided among private industry (approximately 13%), nationally supported research and development centers (about 3%) and other recipients (about 4%). In addition to research awards, the NSF funds the development, operation, and repair of research facilities and equipment. In FY2020, NSF made over 12,200

new competitive awards to nearly 1,900 colleges, universities, and other institutions across all 50 states, the District of Columbia, and three U.S. territories. NSF received $8.49 billion in funding in FY2021. 81.4 % of this amount went toward the research and related activities account (RRA, $6.9 billion), 11.4 % went toward the education and human resources account (EHR, $968 million), and 2.8 % went toward major research equipment and facility construction (MREFC, $241 million), with the remainder going toward administrative and related activities (Harris).

After adjusting for inflation, NSF funding increased somewhat in FY2020 and FY2021 after being stable between FY2010 and FY2019. NSF's granting of 12,200 awards in FY2020 constituted an overall success rate of 28 % for competitively examined proposals. In the fiscal year 2019, around 29,000 people served as panelists and proposal reviewers in the merit evaluation process (Harris). The NSF primarily fulfills its mission by awarding limited-term grants – now about 12,000 new awards per year, with an average period of three years – to fund individual research projects deemed the most promising by a rigorous and impartial merit-review system. The majority of these awards are given to individuals or small groups of researchers. Others sponsor research institutes, tools, and facilities that enable scientists, engineers, and students to work at the cutting edge of knowledge.

The NSF's goals of discovery, learning, research infrastructure, and stewardship provide an integrated strategy to advance the frontiers of knowledge. Cultivate excellent, broadly inclusive science and engineering personnel, increase scientific literacy among all citizens, build the nation's research capability through investments in advanced instrumentation and facilities, and support excellence in science and engineering research and education through a capable and diverse workforce. Support for scientific and engineering education, from pre-K to graduate school and beyond, is another important component of the NSF's mission. The NSF funds

research that is deeply integrated with education to ensure that there are always a sufficient number of skilled people available to work in new and emerging scientific, engineering, and technological fields, as well as a sufficient number of capable teachers to educate the next generation. There is no one factor more crucial to society's intellectual and economic advancement, as well as the improved well-being of its individuals, than the ongoing accumulation of new knowledge (Harris).

4.1.1.1. The Role and Activities of the NSF

The following are activities of the NSF regarding the constant improvements and adaptation of new guidelines in research and education:

A. Initiate and support scientific and engineering research and programs to increase scientific and engineering research potential, as well as education programs at all levels, through grants and contracts, and assess the impact of research on industrial development and the general welfare.

B. Provide graduate fellowships in science and engineering.

C. Encourage the exchange of scientific information between scientists and engineers in the United States and other countries.

D. Encourage the development and application of computers and other scientific methods and technologies, primarily for scientific research and education.

E. Assess the status and needs of various sciences and engineering and use the results of this assessment to align the research and instructional activities with other federal and non-government programs.

F. Serves as a clearinghouse for gathering, interpreting, and analyzing data on scientific and technological resources in the United States, as well as a source of information for other federal agencies developing policy.

G. Determine the total amount of federal funds received by universities and appropriate organizations for the conduct of scientific and engineering research, including both basic and applied research, as well as the construction of facilities where such research is conducted, but excluding development, and report annually to the President and Congress on this matter.

H. Initiate and support specialized scientific and engineering efforts related to international collaboration, national security, and the societal repercussions of scientific and technological applications.

I. Initiate and support scientific and engineering research, including applied research, at university and other non-profit institutions, as well as support applied research at other organizations.

J. Recommend and encourage the development of national policies to promote fundamental research and education in sciences and engineering. Enhance research and education innovation in the sciences and engineering across the United States, including independent research by individuals.

K. Encourage activities that aim to improve the participation of women, minorities, and others who are underrepresented in science and technology (Harris).

The Internet that many of us now take for granted developed from a series of government-funded computer networking experiments. In 1986, computer and information science and engineering were given their own directorate. This would have pleased Bush, who was among the first to recognize the potential of computers to transform all aspects of life. From

funding graduate student fellowships in 1952 to presently supporting primary, secondary, and undergraduate education, as well as informal learning in science, technology, engineering, and mathematics, the education and human resources directorate's portfolio has grown (STEM).

Basic education research improves how science is taught and can create huge gains in students' learning in more quick and complex informational contexts. While conflicts about science curricula persist, particularly in primary and secondary schools, a broad range of stakeholders remain dedicated to Bush's goal of enhancing the national prominence of STEM education. Today, the education and human resources directorate collaborate with partners from academia, industry, non-profits, and other government agencies to support exciting new investigations into ways to improve STEM teaching and learning (Bush).

4.1.2. National Science Agency NSA

One of the largest and most prominent employers of cyber security professionals in the United States is the NSA. They are doing well despite the current difficulties in the market for such professionals, as only 1% of their positions still need to be fulfilled for an extended period. Supervisors who have been polled six months after hiring new employees report being extremely satisfied with the employees they receive. In addition, the NSA has a low turnover rate of employees (losing no more to voluntary quits than to retirements). As a result, senior technical development programs are prioritized to keep staff up-to-date (Libicki 39-40).

NSA must and does pay attention to labor challenges, even if it is not the major focus, it is still quite high on the list. Although just 80 employees work full-time in recruiting, another 300 have recruitment as an additional job, and another 1,500 are involved in the entire recruitment and employment process. NSA's influence extends beyond its designated Centers of Academic Excellence (CAE) to include a wide range of academic institutions; however, it does

promote the development of cyber security courses in the CAE schools, in certain situations, schoolteachers encourage pre-college students to consider a career in cyber security, particularly in Maryland (Libicki 39-40).

The NSA does hire cyber security professionals, it places a high value on identifying the traits that make people effective workers rather than simply looking for the most qualified candidates. Recruiters also pay close attention to colleges with a history of producing military-ready graduates. It is estimated that over 80% of their new hires hold bachelor's degrees or higher. Finding talented junior college graduates may be an option, but it would necessitate a significantly longer training period for them. Furthermore, they only look for a clever hacker with a college diploma. Internal training at the NSA might run up to three years for some employees. This, too, would challenge other institutions to copy (39-40).

The low turnover rate of the NSA allows it to take advantage of its size and low turnover rate. However, the latter means that NSA reaps the benefits of its investments in people rather than having the benefits accrue to other companies after the NSA has paid for the training itself. Employers with a high turnover rate may logically decide it is not worth spending so much time and money on staff education (39-40).

There are two collaborative initiatives sponsored by the NSA and the DHS: the National Centers of Academic Information Assurance (IA) Education (CEA/IAE) and CAE- Research (CAE-R) programs. The programs are designed to satisfy a rising need for IA experts in a variety of fields and promote higher education and research. Once a school has been designated as a CAE/IAE or CAE-R, it must reapply every five academic years. Whereas Scholarships and grants from the DoD and DHS are available to students who attend approved institutions. (Evans and Reeder).

4.1.3. Department of Defense and Cyber Education

No doubt that the United States has a well-developed cyber system. According to the FY2014 defense budget proposal, the United States military, currently, the world's greatest military spender, aims to strengthen its offensive and defensive capabilities in cyberspace and increase its budget for cyber operations to an estimated $4.7 billion (Spidalieri 1). Currently, the audience's understanding of cyber as an environment and a tool could be better, making it easier to present more advanced and complex issues and build comprehensive education and training programs. It must be highlighted, however, that the lack of general comprehension is a generational issue, and the problem of the current leadership lacking skill or even a basic understanding of the cyber domain should be largely remedied within the next decade (Tikk-Ringas et al. 58).

Cyber threats are becoming common as cyber espionage and cyber sabotage can expedite the development of an enemy's defense technology and have devastating effects on U.S. forces engaged in combat by disrupting communications, corrupting data, and rendering computer-based weapons inoperable. A well-executed cyberattack might shut down or damage military command, control, communications, computers, intelligence, surveillance, and reconnaissance systems, putting military missions at risk. The implications for the United States military and national security might be catastrophic (Spidalieri 1). For the United States, the danger of cyber threats is constantly imminent and ominous.

One example of a U.S. threat with the capacity to use the Internet is the Islamic State (IS). Most American soldiers are familiar with the Islamic State's (ISIS) use of social media and the dark web to recruit young people throughout the globe and propagate their message domestically and internationally in terms of the present cyber war. Since 2011, an estimated

27,000 foreign fighters have travelled to Iraq and Syria, making ISIS' effective use of cyberspace as a recruitment weapon impossible to ignore.

Similar ISIS recruitment operations have uncovered, motivated, and trained a growing number of "homegrown" terrorists who have attacked targets in Western Europe and the United States. ISIS's success is not due to robust data networks but rather to the Internet's limitless and mostly unregulated nature. Effective and frequently redundant recruiting techniques include Twitter accounts, Facebook profiles, online podcasts, YouTube, and other social media channels. While several international law enforcement authorities swiftly shut down these accounts, they are just as quickly restored as they are easily accessible and inexpensive communications platforms (Heatherly and Melendez 64).

Cyber defense and cyber security education programs for the military are still developing. Many professional military educational institutions provide tactical/technical (information assurance and security) or strategic/conceptual (policy and doctrine) training and education. At the same time, joint and operational studies remain in the background because they are difficult to compile and deliver (Tikk-Ringas et al. 58). For the DoD, once the enemy is defined, the tools used in cyber threats would be addressed accordingly, as there are multiple ways and forms regarding the enemy using them and the versatile nature of these web attacks.

The extent to which the echo of cyber security goes relies on the preparedness of the military personnel. However, it is important for service and joint-level staff officers and commanders to comprehend available cyber capabilities and assets and their potential use and threats. Officers, regardless of rank or position, must be able to evaluate their operational environments from a cyber viewpoint and be familiar with the fundamental cyber platforms and capabilities. Field commanders must actively investigate cyber possibilities within their missions

and operational region. They must comprehend how to deliver a cyber effect and be aware of the potential political and legal ramifications of their decisions and actions, such as eradicating all local communications in relation to third-party infrastructure (Tikk-Ringas et al. 58).

In order to tackle the issue, as Francesca Spidalieri and Jennifer McArdle put it, “In the future, every military leader must be a cyber-strategic leader” (142). Their study focuses on the efforts made by the U.S. Coast Guard Academy, the U.S. Air Force Academy, the U.S. Military Academy, and the U.S. Naval Academy to prepare all of their future officers for the challenges of operational– and strategic–level leadership in an era of chronic cyber danger. In addition, they stress that National security has increasingly relied on the government’s efforts to provide cyber training for civilian and military employees and develop a cyber workforce with specific skills.

As a starting point by “providing theory and doctrine, with methodology, tools, and implementation,” universities are ready to serve as a breeding ground for these non-technical cyber leaders. In addition to combining knowledge, intellectual capacity, practical skills, and in order to play a significant role in educating civilians and members of the military on the unique aspects of cyber security, universities should maximize campus-wide resources to develop comprehensive curricula that synthesize technical, policy, sociological, and legal components in the study of cyber threats. They are capable of making things happen due to their knowledge and influence. However, as highlighted by the following article, “One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat,” many of America’s non-technical graduate programs are failing to prepare their graduates—and, ultimately, the country—for leadership of crucial institutions. Professional military colleges that study national security and strategy have just lately begun include cyber security instruction in their curriculum,

despite the fact that networks and information technology are essential to operations and susceptible to attack (Spidalieri 3).

The strategy adopted by the Command and General Staff College (CGSC) for cyber education further emphasizes some of the difficulties that the Army's Training and Doctrine Command (TRADOC), which is in charge of soldier education, faces. First, only people with the right education, experience, and security clearance credentials are eligible to work as cyber instructors. For instance, most of the CGSC teaching team consists of civilian professors who left the military before cyber warfare was a common topic of discussion. The teachers undoubtedly care deeply about their work and the teaching of their kids, but in order to make cyber relevance relevant in the classroom, they will need further training. The military's teaching platform will need to quickly generate courses and instructors due to the rapid rate of change in cyber warfare. Cyber training is not a "one-and-done" kind of learning; it demands consistent study throughout a career. A third difficulty is the categorization of the substance itself. Access to and knowledge of U.S. cyber capabilities must be restricted to those with a confirmed need to know to prevent US rivals from obtaining it (Heatherly and Melendez 69).

The nature of national power, the architecture of the international system, and the more conventional facets of security and military affairs have all been altered by cyberspace. Cyber weapons and tools are employed in clandestine operations, espionage, terrorism, and criminal activity. Additionally, as was noted and still valid by Chris Inglis, Deputy Director of the NSA, "it is almost impossible to achieve a static advantage in cyberspace–whether that is a competitive advantage or a security advantage–when things change every minute of every hour of every day. Moreover, it is not just the technology that changes; it is the employment of that technology, the operations and practices" (Spidalieri 13).

To lead, manage, and oversee cyber defense and operations in this dynamic and ever-changing digital world, a new generation of cyber-strategic leaders must be developed. These people can have engineering or programming experience. However, they need a thorough understanding of the cyber environment in which they work, as well as a respect for military ethics, strategic studies, political theory, organizational theory, history, international law, and other sciences. Future cyber-strategic leaders should go beyond self-described "cyber fighters," in fact. Future military leaders must also be adept at cyber strategy (Spidalieri and McArdle 144).

It is reasonable to conclude that cyber officer in education has to confront and diverge from the main arguments made in the context of cyber defense discourse. The first is the debate over education, which contrasts a narrower focus on safeguarding and enabling one's networks and network-based services with a broader interpretation, which recognizes cyber as a resource by using those networks and services to also intentionally cause, enforce, and project hostile cyber effects on the adversary's systems and networks. Second, officer education must address the conflicting opinions of whether the cyber element is a separate task or an essential component. As was mentioned, the cognitive and educational needs of mastering other operational environments, capabilities, and consequences do not fundamentally differ from the demands of knowledge and awareness of cyber ideas, capabilities, and threats. Third, it is important to investigate and comprehend the interconnected roles and duties among people, the military, and civilian society, including the corporate sector (Tikk-Ringas et al. 60).

Rather than focusing on whether or not the United States can build the best and most powerful cyber capabilities to accomplish a particular feat, the question will be whether or not the military and the country's leaders will be prepared to face a variety of cyber threats and

establish both a competitive and security advantage on the modern battlefield. Higher education institutions for the military in the United States can no longer ignore the vital need to train the next generation of military leaders to meet these threats, with a focus on incorporating cyber into the existing Joint Professional Military Education (JPME) curriculum and accelerating the assimilation of cyber into the operational arena for every physical domain (Spidalieri 15).

The vast topic of cyber education and all its outcomes in every aspect of U.S. citizens relies on preparing the next generation for all sorts of cyber-attacks, starting from the introduction of cyber security. The U.S competitive character and the changing nature of technology will not take this kind of security for granted as the government must keep people's digital life secure, and it can be tied to the U.S instilled unalienable rights: life, liberty, and the pursuit of happiness in the digital age.

4.1.4. Department of Homeland Security DHS

New forms of governance are required because America is more vulnerable to attacks from unknown foes armed with a broad variety of weaponry. There is now no government agency whose main goal is to ensure national security. In fact, more than a hundred separate federal agencies are responsible for some aspect of homeland security. Finally, the President proposed establishing a new Department of Homeland Security, the most significant transformation of the United States government in more than a half-century, by transforming and realigning the current confusing patchwork of government activities into a single department whose primary mission is to protect the homeland (The Department of Homeland Security).

Establishing a Department of Homeland Security is another important step in the President's national homeland security policy. The President took significant action to safeguard America immediately following the 9/11 tragedy. The President exercised his full legal authority

to establish the White House Office of Homeland Security and the Homeland Security Council to guarantee that U.S. federal response and protection measures were organized and effective. The President also directed Homeland Security Advisor Tom Ridge to investigate the federal government to "Determine if the current structure allows the United States government to meet today's threats while anticipating tomorrow's unknown threats." After a thorough examination of the current structure, as well as the lessons learned since September 11 and new information about our adversaries while fighting a war, the President concluded that the United States required a more cohesive homeland security system. In the design of the new Administration, they considered many homelands security organizational suggestions that surfaced from outside studies, commissions and Members of Congress (The Department of Homeland Security).

DHS's Cyber security Workforce is responsible for a wide variety of vital operations. Nearly 240,000 people work for the DHS, and the agency has an annual budget of about $60 billion; of that, $6.4 billion was allocated to information technology in fiscal year 2017. The Department of Homeland Security is in charge of coordinating federal efforts to protect the cyber security of the United States' public and private infrastructure. In order to facilitate instantaneous responses to cyber threats, cyber security risks, and events, DHS, among other government partners, collects and distributes relevant data in real time. DHS comprises 15 components. Figure 4 depicts the 15 operational and support components, including the six mentioned above (Wilshusen 8).

Fig. 4. DHS Five Mission Areas Doug Maughan. "Re-Inventing Cybersecurity R&D: How DHS is Innovating to Deliver More Secure Systems."*Isao.org*, https://www.isao.org/wp-content/uploads/2018/09/IISC-2018-Douglas-Maughan-Re-inventing-Cyber security-R-D.pdf.

The increasing number of Internet-connected gadgets and reliance on global supply chains complicates the national and international risk picture even further. More than ever, cyber security is an issue of homeland security and one of the DHS fundamental goals. This latter is also responsible for protecting the greater government enterprise and improving the security and resilience of other vital systems. Simultaneously, it attempts to reduce cyber dangers by preventing and disrupting cybercrime and mitigate the repercussions of cyber incidents by

assuring an effective federal reaction when necessary. Finally, the DHS works to improve the environment for more effective cyber risk management by making the cyber ecosystem more secure and resilient. This plan establishes goals, objectives, and priorities for the Secretary of Homeland Security to carry out the full spectrum of cyber security responsibilities.

To develop instructional programs for the homeland security industry, it is necessary to understand how the Department of Homeland Security and the Obama administration envisions homeland security. The nation's first QHSR was the Quadrennial Homeland Security Review Report (QHSR). Its goal was to establish a unified vision of homeland security to promote the unity of purpose. The QHSR defined 'homeland security' as the "intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border patrol, and immigration". (QHSR 2010,56-58 viii). This vision of homeland security assumed that all of these responsibilities, which included both emergency management and homeland security, would be viewed through the lens of a single overarching concept of the homeland security enterprise, which recognized the need for collaborative actions and efforts across previously discrete elements of government and society. The QHSR went on to describe homeland security as a national endeavor (Kiltz 2):

> Homeland security is a widely distributed and diverse—but unmistakable—national enterprise. The term "enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. The use of the term connotes a broad-based community with a common interest in the public safety and well-being of America and American society that is composed of multiple actors and

> stakeholders whose roles and responsibilities are distributed and shared. (QHSR 2010,56-58 viii)

The QHSR clearly did not adhere to a traditional vision of homeland security that was primarily concerned with preventing and responding to terrorism but rather with an all-hazards strategy that acknowledged the usefulness of disaster preparedness structures and processes. This dual role of the homeland security enterprise was emphasized further by the QHSR's missions, which were not only the responsibility of the DHS, but also of hundreds of thousands of people from all levels of government, the private sector, and nongovernmental organizations (QHSR 2010,56-58).

4.1.4.1. Homeland Security and Education

The Homeland Security Act of 2002 required academia to actively participate in homeland security education. Despite the Act's lack of specifics, cyber security education supporting DHS's purpose and goals is a clear duty. The DHS Science and Technology (S&T) Directorate has served as the primary point of contact between academia and DHS. The S&T Directorate financed 12 Centers of Excellence (COE) through its Office of University programs after 2002. These Centers represented a comprehensive network of institutions that conduct basic and applied research in science, technology, engineering, and mathematics (STEM) programs that directly support the S&T directorates and the DHS's overall strategic plan. However, there was a very legitimate dispute about whether STEM courses were the sole way to integrate cyber security education into the larger homeland security academic endeavor.

STEM-oriented cyber security programs are largely grounded in the physical sciences and focus on programming, tool development, and security mechanism implementation rather than applied cyber security administrative, analysis, or policy components (writ large). In

contrast, most (particularly undergraduate) DHS programs are broad-area, practical social science programs that enhance middle management's analytical and critical assessment skills. Incorporating cyber security policy and management features into a high school curriculum would meet the academic demands of DHS and other homeland security agencies in the future (The Homeland Security Act 2002).

The DHS and Science and Technology Directorate (S&T) assisted in improving cyber security capabilities through strategic research and development (R&D) in the areas of mitigation, solution creation, and resilience. In accordance with the DHS Cyber security Strategy, S&T gathered leading innovators from academia, industry, and government to identify innovative tools and methods that can assist network owners and operators in combating rising cyber threats. The Under Secretary for Science and Technology (S&T) ensured the high quality of research undertaken by the DHS Centers of Excellence (COE).

Each DHS COE was made up of one principal university and several partners. This collaboration gathered colleges in the United States with specific skills to collaborate and coordinate their research and educational endeavors to produce high-quality work. COE consortia also included partners from state and local governments, the commercial sector, end users, people, and academics, as well as Minority-Serving Institutions and states participating in the Experimental Program to Stimulate Competitive Research (Science and Technology Directorate 3).

DHS posted a thorough Notice of Funding Opportunity (NOFO) on *grants.gov* for each COE topic, inviting submissions from U.S. colleges and universities to serve as lead institutions. The DHS S&T Office of University Programs (OUP) collaborated closely with DHS Component representatives to identify high-priority research issues within a chosen theme to include in the

NOFO. This collaboration ensured that the NOFO appropriately reflected DHS customers' and homeland security enterprise (HSE) stakeholders' operating demands. COE subjects must be relevant to the DHS goal, fill a knowledge vacuum, and be suitable for open-source university research (Science and Technology Directorate 3).

An obvious way for a high school program to incorporate information security education into the curriculum was to have students take these courses as offered by the computer science, computer technology, or computer engineering departments. Furthermore, focus on computer design and programming, operating systems, network architectures and protocols, and other computer science topics essential to the study of cyber security science and technology. However, this technique may only sometimes suit the demands of high school students. One issue is that these courses frequently involve requirements (or, at the very least, an expectation that students have a background) in calculus, physics, and/or programming and are not focused on "computer security for the social sciences." While a solid technological basis is required for those experts to detect, respond to, and counterattack in cyberspace, a multidisciplinary approach is also required for homeland security professionals (Science and Technology Directorate 3).

4.2. Government Initiatives to Promote and Expand Cyber Security: The Comprehensive National Cybersecurity Initiative (CNCI), (2008-2009).

President George W. Bush launched the Comprehensive National Cyber Security Initiative (CNCI) in 2008, a now-declassified twelve-point approach to combat cyber security threats across the civilian, military, government, and corporate sectors. Under the Enduring Security Framework, the DoD and DHS formed a group of government and commercial leaders to address cyber security challenges. President Obama requested a review of the CNCI shortly after entering the office and reiterated the mandate to move forward with a national cyber

program (Burns and Price 193-194). President Obama, as a result, shortly after entering office, started the preparation for a comprehensive strategy for securing America's digital infrastructure (The White House 1-5).

As a result of the Cyberspace Policy Review that followed in May 2009, the President appointed a Cyber security Coordinator in the Executive Branch who reported directly to the President. The Executive Branch was also tasked with strengthening public/private cooperation to find technological remedies to guarantee U.S. safety and wellbeing, investing in cutting-edge research and development to meet today's digital challenges, and ensuring a coordinated and unified reply to any future cyber incidents. Finally, the President commanded that these actions be carried out consistently, protecting the constitutionally granted private rights and civil liberties held dear by all Americans (1-5).

The activities underway to implement the Cyberspace Policy Review's recommendations build on President George W. Bush's Comprehensive National Cybersecurity Initiative (CNCI), launched in January 2008 with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23). President Obama determined that the CNCI and its associated operations should evolve into a components of a broader, updated national United States cyber security policy. As a result, these CNCI activities will be important in achieving

many of the essential objectives of President Obama's Cyberspace Policy Review (The White House 1-5).

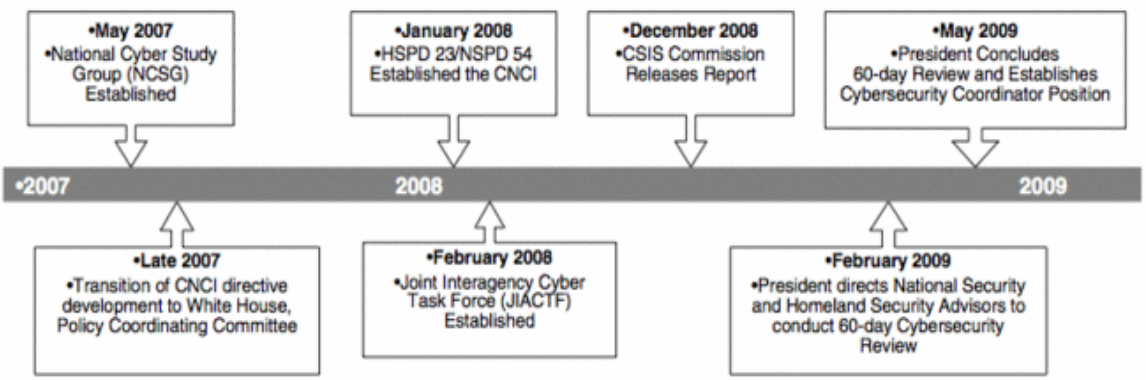


Fig. 5. The Comprehensive National Cybersecurity Initiative (CNCI) from National Security Council (May 2009).

The CNCI is a collection of mutually reinforcing activities with the following key goals to help safeguard the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats,** create or improve shared situational awareness of network vulnerabilities and threats within the Federal Government, state, local, and tribal governments and private sector partners. The ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- **To protect against the whole spectrum of threats** by strengthening U.S. counterintelligence capabilities and increasing the security of vital information technology supply chains.

To strengthen the future cyber security environment by extending cyber education, coordinating and redirecting research and development efforts across the Federal Government, and working on designing and creating tactics to dissuade hostile or malicious conduct in cyberspace.

When developing the CNCI plans, it became clear that these objectives could only be met by enhancing specific critical strategic core competencies inside the government. As a result, the

CNCI includes funding from the federal law enforcement, intelligence, and defense communities to improve key functions such as criminal investigation, intelligence collection, processing, analysis, and information assurance, all of which are significant to enabling national cyber security efforts.

In close cooperation with privacy specialists across the government, the CNCI was established with considerable care and sensitivity to privacy and civil liberties concerns. The CNCI's implementation continues to prioritize the protection of civil liberties and privacy rights. The Cyberspace Policy Review recognized more important the evidence shared as a vital factor of an operational cyber security's system, in line with President Obama's stated intention to make transparency a touchstone of his presidency. As a result, the Cyber security Coordinator has disseminated the CNCI summary description to promote public understanding of Federal initiatives (The White House 1-5).

As part of its mission to make clear the public's interest in government, military, aerospace, and defense cyber security, CNCI developed a coherent, strategic approach to cyber security. However, neither the CNCI nor any official U.S. policies clearly say that the state exercises sovereign, territorial prerogatives in cyberspace. Therefore, the following are the primary objectives of the CNCI: A compelling first line of defense against today's immediate threats is to create or enhance shared situational awareness of the federal government's network vulnerabilities, threats and events, as well as the ability to act swiftly to reduce our current vulnerabilities and prevent intrusions with state, local, tribal governments and private sector partners. Enhancing U.S. counterintelligence capabilities and securing the supply chain for information technologies would help the country combat a wide range of threats. Strengthening cyber security through increasing cyber education, coordinating federal research and

development activities, and striving to develop measures to dissuade hostile or malicious conduct in cyberspace are the goals of the National Cybersecurity and Communications Integration Center (NCCIC) (Visner 95-96).

The CNCI was included in the 54th National Security Presidential Directive on Cyber Security Policy. This directive was intended to address current security threats and anticipate them, safeguarding the confidentiality, integrity, and availability of both classified and unclassified networks. The CNCI has twelve initiatives that affect multiple federal agencies, including the DHS, OMB, and NSA (CNCI, 2009).

The CNCI's goals are primarily to help secure the United States in cyberspace: to establish a front line of defense against today's immediate threats and to defend against the full spectrum of threats by improving U.S. cyber security counterintelligence and expand cyber education. In developing plans to address cyber security in education and its weaknesses that affect the federal and private infrastructure of the United States system, the United States government directed its new policies to secure its national security by empowering education policy as it is illustrated in the CNCI content:

Initiative N◦8. 'Expand cyber education.'

> While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However, there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort.

> In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge. (The White House1-5, CNCI, 2009)

CNCI was a new plan adopted by the American government. This initiative is based on fostering the implementation of new policies to solve the arising threat of cyber security. Initiative N8 from CNCI focuses on "expanding cyber security education" and has a pathway to follow to create a new infrastructure for the sphere of Information Security. The initiative focuses on raising awareness, creating a pipeline of experts, and providing society with a qualified workforce to cover the shortage of cyber security agents. To implement this initiative, the federal government created a nexus between the agencies and higher education to invest in the new educational programs that target the taxonomy of the cyber security field of education.

4.2.1. The NICE Workforce Framework: The NIST Special Publication 800-801.

The cyber security challenges of the new era result from the rapid growth of cybertechnology and its threats. The IA is required to ensure the consistent and dependable security of cyber assets, which evolves at the same rate as the technology itself. As a result, most people regard cyber security procedures as an enigmatic collection of activities and criteria that only a few can properly comprehend or implement. As a result, many businesses' electronic infrastructures are riddled with vulnerabilities, allowing for numerous criminal and national security exploits over the last decade. According to the non-profit Privacy Rights Clearinghouse, one billion records have been lost in the last decade; However, most firms are unwilling to disclose security failures, which is likely to be underestimated (Kohnke 2-5).

Prior to the foundation of NICE in 2010, the idea for the NICE Framework was conceived out of a desire to properly identify and evaluate the cyber security workforce in both the public and private sectors. More than twenty government departments and agencies and members from the private sector and academia got together to determine how to provide a shared understanding of cyber security activity. This led to the development of two early versions of the NICE Framework before its release as NIST Special Publication 800-801 in 2017 and a second modification in 2020. The growth of the NICE Framework has resulted in a resource that is now nimble, flexible, interoperable, and modular. It continues to rely on collaboration between the government, the corporate sector, and the academic community. The NICE Workforce Framework for Cyber security offers users a consistent vocabulary that can be used to enhance processes and practices related to finding, attracting, developing, and keeping cyber security talent. It can be employed across enterprises and industries to create resources and tools that define or provide direction for specialists' development, planning, training, and education (Petersen et al.).

The NICE Framework is a crucial resource for developing and supporting a workforce capable of satisfying the cyber security requirements of a business. It provides businesses with a standard, consistent vocabulary for categorizing and describing cyber security work through Task, Knowledge, and Skill (TKS) statements that explain the work to be performed and what is required to do that task. In addition, it describes how these building pieces can be used to establish Competencies and Work Roles. Eventually, the NICE Framework interacts with numerous audiences:

Employers: To assist in defining the cyber security workforce, including those whose primary focus is on cybersecurity and those who need specific cyber security-related knowledge and

skills to manage enterprise risks; to identify hazardous gaps in cyber security staffing; and to create position descriptions consistent with the national language.

Learners: Current and future employees can utilize the NICE Framework to investigate the breadth of available cyber security-related work and opportunities, as well as Competencies that employers prize for in-demand cyber security employment and positions.

Staffing consultants and guidance counselors may also utilize the NICE Framework to assist these employees or job seekers.

Education, Training, and Credential Providers: The NICE Framework provides direct information about what a workforce must know, assisting with the creation of learning content and the development of certificates, badges, and other verification techniques that consistently describe learner capabilities (Petersen et al.).

4.2.1.1. The Development of the NICE Cybersecurity Workforce Framework

The NICE Cybersecurity Workforce Framework is an umbrella framework because its purpose is to define the entire collection of cybersecurity-related competencies. In addition, the NICE framework relates these competencies to a collection of common security jobs and a set of functions associated with those roles (NIST, 2014). This provides individual practitioners with a consistent set of suggestions regarding the activities that must be carried out to fulfill the requirements of each position (Kohnke, 4-5).

The NICE Cybersecurity Workforce Framework aims to develop a uniform taxonomy and vocabulary for describing all cyber security work and personnel, regardless of where or for whom the work is performed (NIST, 2014). The Framework consists of seven general knowledge domains and thirty-two specialization domains. These Knowledge and Specialty domains determine the scope of legitimate cyber security profession activity. In this regard,

NICE is the first fully comprehensive area definition. The NICE Framework consists of seven broad Knowledge Areas that serve as the field's overarching structure.

Table 2
The NICE Cybersecurity Workforce Framework 7 General Knowledge Areas

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/ornetwork development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Adapted from: (Petersen et al. 11).

There are thirty-two Specialty Areas that go with the seven general knowledge areas. The figure and the tables show the 32 specialty areas associated with each of their respective general knowledge areas: A description of each of the NICE Framework Specialty Areas. Each Specialty Area has a three-character abbreviation associated with it (for example, RSK), which can be used for speedy reference to the specialty area and helps identify job roles inside the NICE Framework.

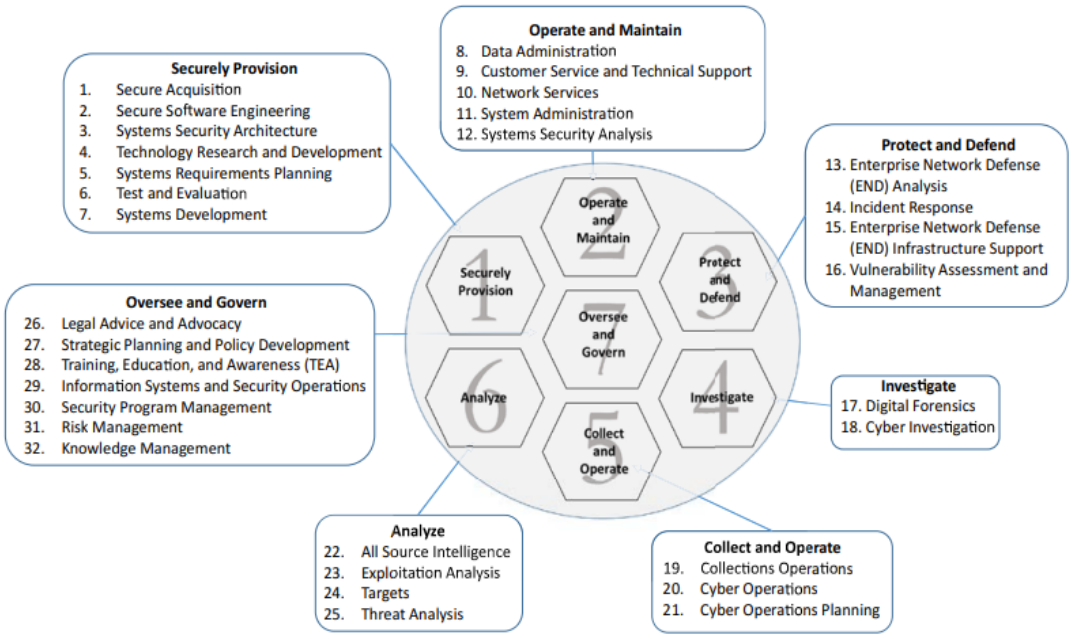


Fig. 6. The 32 Specialty Areas of the NICE Cybersecurity Workforce Framework. (Kohnke, 7). For each Specialty Area, a set of Professional Roles has been identified and associated.

The NICE Cybersecurity Workforce Framework is intended for governmental, business, and academic use. Organizations are not required to alter their organizational or vocational structures to utilize the Framework. The Framework was created because mandating such changes would be expensive, unworkable, useless, and inefficient. Consequently, the Framework can be used in various contexts and locations.

4.2.2. Cyber Security Workforce Development Programs Led by the Center of Academic Excellence (CAE)

In 1999, the NSA founded the National Centers of Academic Excellence in IA Education program. The initiative was designed to help meet the increased demand for cyber security knowledge among intelligence community employees. As it became evident that cyber defense would become an essential component of national security over time, the program's objectives grew to meet the nation's demand for cyber security workforce development (CAE in Cyber Defense Publication 4-8).

Originally, the program required schools to match their information assurance curriculum to Committee on National Security Systems (CNSS) requirements. CNSS 4011 was the first to be developed, outlining the basic knowledge required of IA professionals to execute their craft and serving as the foundation for the CAE in the IA Education Program. Institutions could map to later standards as the CNSS produced them (CNSSIs 4012-6). Institutions that successfully mapped obtained a certificate from the Information Assurance Curriculum Evaluation (IACE) program. The initial step toward CAE certification was receiving an IACE endorsement. In 2012, the program shifted from CNSS standards to developing and implementing a new Knowledge Unit (KU) structure that better reflected the status of cyber security and technology. Beginning in 2014, applicants began utilizing the new KUs for designations, and by 2017, every academic institution in the program had made the switch (CAE-CD Program Guidance 1-3).

The CAE designation has always been based on both curriculum and program standards. The criteria reflect the institution's dedication to participating in the CAE-CD program, practicing what they teach, retaining outstanding professors to assure a long-term academic program, reaching out to high schools and others needing IA knowledge, and promoting the

profession. After receiving IACE approval, an institution moves on to the second level, which involves documenting the program criteria. When the program switched to KUs, the two-stage process converged into a single application (CAE in Cyber Defense Publication 4-8).

James Madison University, George Mason University, Idaho State University, Iowa State University, Purdue University, University of California, Davis, and the University of Idaho were the first seven universities to acquire the designation. These seven schools were crucial in the early development of information assurance curricula. Because textbooks on the subject had yet to be created, the original seven schools established a bond and shared resources to begin developing a community that has since grown to 312 schools across the country (4-8).

The CAE Program Management Office has undergone numerous enhancements to stay up with the cyber landscape. The introduction of the DoD Information Assurance Scholarship Program (2001), the addition of DHS as a partner (2004), the addition of the Research designation (2008), and the Two Years Education (2010) designation are some of the most prominent modifications. Congress altered the program's name from Information Assurance to Cyber Defense in the 2017 National Defense Authorization Act (NDAA). In 2018, the CAE-CD Program Office modified the methodology for curriculum mapping and designating titles in partnership with the CAE Community. The Program Office and designated institutions convened in a series of workshops to update the program's Knowledge Unit (KU) structure and content. In the process, the institutions agreed to modify the academic standards for designation. The necessity to distinguish between Bachelor's and graduate degrees and the relationship between types and numbers of KUs at each level of recognition drove this modification (CAE-CD Program Guidance 1-3).

The curriculum mapping requirements evolved without any major changes to the KUs themselves. The new approach allowed all designating institutions to personalize their programs and represent the competence of their programs inside their designation. This also helps students, businesses, and educators understand the objective of each designated program. Also, how those programs map to the NICE Workforce Framework categories and employment responsibilities. In the 2019 application cycle, the program office implemented this new model (October 2018 to May 2019) until the automated application tool was updated (CAE-CD Program Guidance 1-3).

4.2.2.1. Center of Academic Excellence in Cyber Defense Education

The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program, co-sponsored by the U.S. NSA and the DHS, is a national quality standard for certifying and maintaining high-quality cyber security education; through rigorous and consistent program evaluation requirements and close alignment to specific cyber security knowledge units. Only roughly 200 colleges and universities in the United States have received the CAE-CDE distinction. Students will gain confidence in their ability to study if they attend a CAE school, and businesses will gain confidence in hiring if they graduate from a CAE school (Dawson et al. 12).

The national CAE-CDE program originated from the NSA's initial national CAE in Information Assurance Education (CAE-IAE) program, which began in 1998, with DHS joining as a co-sponsor in 2004, and the CAE in IA Research special designation was added in 2008 to encourage Ph.D. level research in cyber security. The CAE2Y component was established in 2010 to enable two-year universities, technical schools, and government training facilities with the option to earn the CAE credential. As a result, the present CAE-CD program comprises the following designations: CAE2Y for two-year institutions, CAE-CDE for four-year institutions,

and CAE-R for doctoral universities or DoD schools. Graduate institutions in the United States are eligible to apply for the CAE certification. The title is bestowed upon institutions that have proved compliance with stringent CAE requirements and curricula mapping to a mandated core Set of Cyber Defense knowledge Units (KUs) with Optional Focus Areas (Dawson et al. 12).

1-CAE in Cyber Defense Education (CAE-CDE):

Sponsored by the NSA and the DHS. These Bachelor's and Graduate programs have met the NSA and DHS's strict academic qualifications and institutional criteria for recognition. These programs prepare graduates to work in the cyber workforce for the nation's business and government employers (Department of Commerce). The CAE-CD designation has four levels: Associate, Bachelor, Master, and Doctoral. Suppose Institutions are interested in becoming a Center of Academic Excellence in Cyber Defense (CD) or Cyber Operations (CO). In that case, the curriculum used to map the KUs must have been taught at the school for at least three academic years. At least one graduating class must have completed the programe (CAE program in Cybersecurity Community 7-8).

Applicants for all CAE-CD designations must map their curriculum to three Foundational core KUs and five non-technical or five technical KUs.

• Cybersecurity Foundations, Cybersecurity Principles, and IT System Components.

• Foundational KUs: Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components.

• Non-technical Core KUs: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security

• Program Management; Security Risk Analysis; Cybersecurity Planning & Management

• Technical Core KUs: Basic Scripting and Programming; Basic Networking; Network Defense;

• Basic Cryptography; Operating Systems Concepts All CAE-CDE Associate applicants must be a regionally accredited, two-year community college or technical school, a U.S. government cybersecurity training center, or a state or federally-endorsed cybersecurity training center. Criteria for the CAE-CDE Associate designation include:

• Demonstration of program outreach and collaboration, student development, CD Center.

• Establishment and maintenance, CD multidisciplinary efforts, the practice of CD at the institutional level, CD faculty, and student curriculum path and recognition.

• Successful mapping of the institution's curriculum to the Foundational KUs, Technical or Non-Technical Core and three optional Knowledge Units (KUs) (CAE in Cybersecurity Community 7-8).

2-CAE in Cyber Research (CAE-R)

Supported by the NSA and DHS, CAE-R is an internationally recognized leader in cyber defense. These initiatives are the most effective and high-quality cyber security research projects at US universities (Department of Commerce). Candidates for the CAE in Research (CAE-R) must be graduates of a Department of Defense institution, a military academy with a Ph.D. program, or a four-year college with regional accrediting agencies. The Carnegie Foundation Basic Classification system (and other independent bodies measuring CD) requires them to be categorized as a Doctoral University with Highest Research Activity (R1), Doctoral University with Higher Research Activity (R2), or Doctoral University with Moderate Research Activity (R3), or they must provide a written justification outlining their significant CD research. Documentation of professor and student CD Research projects, publications, graduate-level output, and research funding are all required under the CAE-R criteria (In Cybersecurity Community 7-8, CAE).

3- CAE in Cyber Operations (CAE-CO):

Funded by the National Security Agency and the Department of Homeland Security. These are highly technical interdisciplinary higher education programs based on computer science, computer engineering, and electrical engineering disciplines. These initiatives emphasize technology and techniques relevant to specialized cyber security operations (e.g., collection, exploitation, and response) to improve the U.S. national security posture (Department of Commerce).

4.2.3. CyberCorps ® Scholarship for Service (SFS) Program: Increasing National Cyber Security Education Capacity.

New methods for building, developing, and running cyber systems, protecting existing infrastructure, and motivating people to learn about cyber security may be uncovered by approaching security and privacy as a multidisciplinary topic. The NSF, in partnership with the OPM and the DHS, is authorized by the Cybersecurity Enhancement Act of 2014, as amended by the National Defense Authorization Acts for 2018 and 2021, to establish a scholarship program to attract and train the next generation of security specialists to meet the needs of the cyber security goal for federal, state and local governments. As part of the Federal Cyber Service Training and Education Initiative, the SFS Program was created to increase the number of qualified individuals entering the Government Information Assurance (IA) workforce, the number of qualified individuals participating in research and development (R&D) in IA and the number of qualified individuals participating in the CyberCorps (CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).

The SFS program grants higher education institutions student scholarships in support of cyber security education. As a condition of receiving a scholarship under the SFS program, each scholarship recipient enters into an agreement in which the recipient agrees to work for a period

equal to the duration of the scholarship in the cyber security mission of an executive agency or, subject to prior approval, in the cyber security mission of:

1. Congress, including any agency, office, or commission established in the legislative branch;

2. an interstate agency;

3. a state, local, or tribal government; or

4. a state, local, or tribal government-affiliated non-profit organization that is considered to be critical infrastructure (CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).

The (OPM) collaborates with NSF in this program by assisting SFS scholarship students, coordinating students' transition into government employment, monitoring students' compliance with program requirements, and evaluating whether the program helps meet the federal government's personnel needs for information infrastructure protection. Grantee institutions provide scholarship support to students who compete successfully in a selection process developed by the institution, who meet the SFS eligibility criteria, and who are confirmed by OPM as qualified for employment in a cyber security-related position (CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).

The SFS program funds initiatives that are anticipated to strengthen the capacity of the U.S. higher education enterprise to generate cyber security specialists. Proposals may be submitted through the NSF-wide Secure and Trustworthy Cyberspace (SaTC-EDU) program's Education Designation. The SFS program, in collaboration with the NSA, provides funding to improve cyber security education from kindergarten to 12th grade in order to:

1. Increase student interest in cyber security careers;

2. Assist students in practicing appropriate and safe online behavior and understanding the fundamental principles of cybersecurity;

3. Enhance teaching methods for delivering cyber security content in computer science curricula from kindergarten to grade 12, and

4. Encourage teacher recruitment in the field of cyber security (CyberCorps® Scholarship for Service (SFS)(NsF21580)/NSF).

4.2.3.1. Goals of the SFS Program

The SFS program's goals are consistent with the United States' strategy to produce a great cyber security workforce. These objectives include:

> Increase the number of new entrants to the government cyber workforce, to increase the national capacity for the education of cybersecurity professionals, to increase national research and development capabilities in critical information infrastructure protection, and to strengthen partnerships between institutions of higher education and relevant employment sectors. (CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF)

The SFS Scholarship award covers up to three years of stipends, tuition, and allowances for students studying cyber security in general. The scholarships grant stipends of $25,000 per year for undergraduate students and $34,000 per year for graduate students during the academic year. Furthermore, SFS scholarships cover expenses normally incurred by full-time students at the institution; stipends, tuition, education-related costs, and professional student allowances must all be reported as Participant Support Costs in the NSF proposal budget.

The Accreditation Board for Engineering and Technology (ABET) is a non-profit organization that accredits college and university programs in applied and natural science, computer, engineering, and engineering technology. Graduates of ABET programs are prepared to enter the global workforce. ABET accredits 4,361 programs at 850 colleges and universities in

41 countries/areas worldwide as of October 1, 2021, an increase of 54 programs over 2020. In comparison, the United States has approximately 3382 programs and 653 institutions. “The United States Bureau of Labor Statistics predicts a 33% increase in job growth in this field from 2020 to 2030, and it is critical to have graduates with the skills and knowledge to meet this demand,” said ABET Executive Director and CEO Michael K. J. Milligan:

> This is an important milestone e in assuring confidence in two-year cybersecurity programs. Our criteria guide institutions in defining their programs. ABET accreditation assures the industry that a program meets quality standards that produce graduates equipped to enter the workforce (ABET Accredits 54 Additional Programs in 2021, Including First Associate Cybersecurity Programs).

After graduation, all scholarship recipients must work for a federal, state, local, or tribal government agency in a cyber security-related role for the duration of the award. A proposing university must document a strong existing academic cyber security program. ABET cyber security accreditation; National Security Agency and Department of Homeland Security designation as a Center of Academic Excellence in Cyber Defense Education (CAE-CDE), Cyber Operations (CAE-CO), or Research (CAER); or equivalent evidence documenting a strong cyber security program are examples of such evidence. The SFS program also supports efforts to improve the capacity of the US higher education enterprise to generate cyber security specialists. The Secure and Trustworthy Cyberspace - Education Designation (SaTC-EDU) and other initiatives provide funding opportunities in this field (CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).

In January 2020, 4,040 SFS scholarship recipients, 2,834, entered government service and worked at 357 federal agencies. In the academic phase, there are over 800 students. More

than 340 students will graduate in May 2020. Bachelor of Science (35%), Master of Science (62%), and Ph.D. (3%). Female (25%, 2013-2018). The tables below indicate the top fifteen universities in terms of student enrolments from 2013 to 2018, as well as the number of post-graduates. Students by agency (ABET Accredits 54 Additional Programs in 2021, Including First Associate Cybersecurity Programs).

Table 3
CyberCorps® (SFS) Top Universities

CyberCorps@ (SFS) Top Universities	
Top 15 Universities by Student Enrolments 2013-2018	
University of Tulsa OK	95
Dakota State University (SD)	67
Carnegie Mellon University (PA)	59
Florida State University (FL)	58
Naval Postgraduate School (CA)	57
University of Maryland Baltimore County (MD)	56
California State University at San Bernardino (CA)	55
Mississippi State University (MS)	52
University of Alabama Huntsville AL	46
Northeastern University (MA)	45
U of Illinois at Urbana-Champaign IL	44
University of North Carolina (NC)	42
Towson University (MD)	38
University of Texas at Dallas (TX)	38
North Carolina A&T State University (NC)	37

Adapted from: Victor Piotrowski. “CyberCorps® Scholarship for Service (SFS).” *Nationalacademies.org*, directorate for education and human resources, (nationalacademies.org).

Table 4
CyberCorps® (SFS) Top Placements

Cybercorps@ (SFS) Top Placements	
Post-Graduation Agency	**Number**
National Security Agency (NSA)	600
Department of Navy	271
MITRE managed FFRDCs	225
State/Local/Tribal Government	191

Department of the Army	153
Department of Homeland Security	125
Sandia National Laboratories	123
Department of Defense	104
Department of Justice	81
John Hopkins Applied Physics Laboratory	76
Department of Air Force	74
Central Intelligence Agency (CIA)	66

Adapted from: Victor Piotrowski. "CyberCorps® Scholarship for Service (SFS)." *Nationalacademies.org*, directorate for education and human resources, (nationalacademies.org).

The program's goal is to place all students in government cyber security roles, with at least 70% of scholarship recipients landing jobs in the federal government's executive branch. While SFS scholarship winners are responsible for job searches, the OPM/SFS program office provides numerous tools to help with the process, including annual job fairs. PIs and SFS scholarship students are encouraged to work aggressively with OPM to acquire a summer internship and permanent placement in the federal government's executive branch. A restricted number of students, but no more than 20% of scholarship holders, may be placed in a non-executive federal agency; state, municipal, or tribal government entity; National Laboratories; or Federally Funded Research and Development Centers with authorization of the OPM/SFS program office (FFRDCs) *(CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).*

The NFS program monitored and evaluated SFS to see how well it met its objectives. These SFS targeted a fragile area that the U.S. is suffering from; a pipeline of talented professionals in cyberspace to increase the number of new entrants into the government cyber workforce, increasing national capacity for cyber security professional education, increasing national research and development capabilities in information infrastructure protection, and strengthening partnerships between institutions of higher education and relevant employment sectors *(CyberCorps ® Scholarship for Service (SFS)(NsF21580)/NSF).*

Scholarship for Service (SFS) is an important program in the United States that provides financial assistance to students interested in pursuing a career in cyber security. This program helps ensure the nation has a well-trained and highly qualified personnel to protect its information infrastructure and data from cyber threats. SFS also provides students with the opportunity to gain valuable experience and knowledge in the field of cyber security, which can help them to become successful professionals in the future. This crucial initiative addresses the shortage of skilled professionals in the field of cyber security.

The partnership between federal agencies and higher education institutions has proven vital in promoting cyber security programs. This partnership impacted the development of policies, educational initiatives, and the creation of a skilled workforce. To overcome challenges, the synergy between federal agencies and higher education has proven to be contributed slightly to addressing the shortage of skilled professionals in the field of cyber security. This chapter shows the importance of collaboration between these entities and its positive impact on promoting cybersecurity programs. it provides valuable insights into the efforts to build a strong cyber security human capital.

Chapter Five:

Cyber Security Vulnerability: The Final Straw in American National Security

Cyber Security is a new threat to national security, which needs new policies or strategies to contain the threat. The new threat is overwhelming the labor force capacities of experts in the field, which necessitate the creation of a pipeline of workforce professionals and qualified cyber security agents. President Obama, in 2009, initiated the National Comprehensive Initiative N8, which focuses on "expanding cyber security education" to raise awareness, create a pipeline of experts and provide society with a qualified labor force to cover the shortage of cyber security agents. To implement this initiative, the federal government agencies create a nexus between them and education to implement the new policy; this will be accomplished only through an educational program and an increase in funding to this specific sector of Cyber security. The chapter discusses the results after the enactment of Initiative N°8 and to what extent it contributed to creating a cyber security workforce.

5.1. The Contribution of The Developed Programs in Expanding Cyber Security Education.

5.1.1. The Impact of the NICE Framework in Improving Cyber Education

The cyber security labor force shortage in the U.S. is a growing concern that seriously affects the nation's security and economic prosperity. In order to address this issue, the CAE, the NICE Framework, and SFS have been developed to help sustain and solve the problem of U.S. cyber security workforce vulnerability. The CAE program provides universities with the resources and guidance needed to develop comprehensive cyber security curricula that will equip students with the skills and knowledge needed to succeed in the field. The NICE Framework

provides a set of standards and best practices for organizations to use when developing their own cyber security programs. Finally, the SFS program offers scholarships to students who are interested in pursuing cyber security-related degrees.

The federal government's effort to support and improve cyber security education takes several forms: the NSA/DHS designation of National Centers of Academic Excellence in Information Assurance/Cyber Defense at participating colleges and universities, the NICE Framework, and the operation of the CyberCorps®: Scholarship for Service (SFS) program, which is administered by the NSF (Wennergren 5). These programs have been progressively helping to bridge the gap between the demand for cyber security professionals and the available talent pool. Providing universities with the necessary resources and guidance has enabled higher education institutions to better prepare students for the cyber security workforce. Additionally, the SFS program has motivated more students to pursue cyber security-related degrees, thus increasing the number of qualified personnel available to fill these positions(5).

In the realm of information technology and security, there are a number of campaigns aiming to raise awareness. The Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) is one of the most well-known cyber security sites, since it provides a lot of data on cyber education and training. The National Initiative for Cyber security in the Workplace (NICE Framework) is a framework developed by NICCS with the goal of establishing a standardized vocabulary for cyber job positions as well as the Knowledge, Skills, and Abilities (KSAs) necessary for each. For businesses looking to develop and educate their cyber workforce, NICCS provides a streamlined portal to a wealth of resources for k-12 cyber curriculum and related resources. The NSA and NSF have partnered to create GenCyber, an initiative that offers free cyber security camps over the summer to both kids and

educators. GenCyber sees itself as part of the answer to the cyber security problem. talent shortage by inspiring students' interest in the field earlier and advancing teaching methods in related K-12 curriculums (Cybersecurity Career Paths and Progression 4-6).

The NICE Framework and other similar initiatives provided proactive solutions to satisfy the needs of many certified and skilled cyber security experts. The framework is a structured, common model through which the industry, job candidates, students or job searchers, and academic institutions can communicate in a common language and concepts. After reviewing numerous recent cyber security job postings on various recruiting platforms, it was discovered that they have begun to include KSAs from the NICE Framework as part of the job description or qualifications. Students can then easily link to these KSAs and demonstrate that they have finished courses and training or have credentials that cover such KSAs with their degrees and certificates (Alsmadi 1-6).

One of the NICE Framework's primary goals is to assist the U.S. market in meeting its demand for cyber security specialists by providing a consistent language through which enterprises, job recruiters, and educational institutions may communicate. There is no debate about the truth and importance of these concerns, nor the NICE Framework's ability to address them aggressively (1-6). The NICE Framework successfully guided the design of cyber security courses and programs,

Educators, business leaders, and policymakers all have a stake in developing cyber security courses and programs geared toward the needs of the workforce. With the use of a database powered by the NICE Framework, KSA's and Work Roles may be easily searched by site visitors. Additionally, AI may aid in the creation of curricula, ensuring that the most relevant KSAs are included. Teachers may also look for information by Job function to help them train

their pupils for positions and skills that are in demand. – Morgan State University's Chair and Professor of Computer Science Paul Wang emphasized that: "Use of the NICE Framework prepares students with the KSAs that shorten the transition from study to work" (Nice Framework Success Story).

5.1.2. The Impact of The CAE Programs on Improving Cyber Education

The NSA established and managed the NCAE in Cyber security. This program designed and tested cohesive teaching curricula in cyber security and related subjects at community colleges and universities. The framework, among other things, establishes standards for cyber defense instruction curriculum across academic institutions, creates development events for students and faculty, raise awareness amongst student by encouraging competitions and conferences, and promotes community engagement through workshops with industry stakeholders or field days for K-12 students (Local Academic and Economic Impacts of the CAE-CD Designation 5-6).

Institutions are designated based on the strength of their curriculum, faculty qualifications, program expansion, and projected community involvement. The designation ensures these programs provide state-of-the-art training to the nation's future cyber security and IT support workforce. However, these CAE-designated programs have a large local impact; establishing a local program produced a robust talent pipeline, greatly decreasing hiring costs and time. Second, the local skill pool increase made it cheaper and easier for local businesses to build resilient computer systems and anti-attack defenses. Local consumers, businesses, and government agencies benefit from programs; safer data management avoids the need to pay more expensive ransoms for assaults (Local Academic and Economic Impacts of the CAE-CD Designation 5-6).

Institutions that provide cyber security degrees are eligible for the following designations: a. CAE-CD given to regionally authorized colleges and offer cyber security degrees (certificate, associate, bachelor, or graduate degrees). b. CAE-R (Cyber Research) given to the DoD schools, military academies, and regionally approved four-year universities that grant Ph.D. degrees. c. CAE-CO (Cyber Operations) is a multidisciplinary higher education curriculum combining computer sciences, computer engineering, and electrical engineering. The CAE-CO provides students with hands-on experience through labs and exercises. This diversity in designations contributed to the rapid expansion of CAE-accredited programs from seven designated institutions in 1999 to 338 in 2021 (Local Academic and Economic Impacts of the CAE-CD Designation 5-6).

The final significant aspect of the CAE-CD certification is how well-prepared local firms are for cyber-attacks. Aside from enhanced output and productivity, enterprises benefit from the designation by being better protected against threats. The CAE-CD credential enables establishment of local networks of educated specialists to assist these smaller enterprises in becoming less vulnerable to cyber threats. With a global cost of $20 billion in 2020 ($157 million for American healthcare organizations since 2016), stopping these assaults and minimizing exposure has become a top goal for many enterprises. Workers trained in cyber security programs at community colleges secured the availability of a qualified local pool of labor to assist enterprises in these efforts. The availability of specialized cyber security helped these enterprises to focus on their main economic activity rather than paying for extremely expensive ransomware (Local Academic and Economic Impacts of the CAE-CD Designation 60-61).

The CAE-CD program has yet to receive funding to provide grants every fiscal year. It has received financing from Congress regularly to help expedite the program's growth and stimulate research. Congress appropriated $6 million for research in FY2015, distributed to CAE-CD authorized institutions. Congress appropriated one million dollars for grants to CAE-2Y-authorized universities in FY2016. The program got $25 million from the President's budget in FY17, which aided in establishing the CNRCs and the other three CRRCs. It allowed the program office to issue 45 grants for projects at approved institutions (Academic Excellence in Cyber Defense Center 2019).

Cyber security-focused CAE programs have been studied, discussed, and verbally supported for three successive presidential administrations. The 2016 Cyber security National Action Plan (CNAP) proposed that $62 million be invested in cyber security personnel, including strengthening the National CAE in Cyber security program (Office of the Press Secretary, 2016). Putting the CNAP into action on November 1, 2019, there were 312 designated institutions across 48 states and the District of Columbia. 108 Community Colleges were offering Associate programs and degrees. However, the CAE program endured a remarkable change and growth through the years for what it epitomizes for American national security. (Centers of Academic Excellence in Cyber Defense Publication 4-8).

5.1.3. The Development of the Centers of Academic Excellence (CAE)

5.1.3.1.CAE in Cyber Defense (CAE-CD)

From the table and graphs above, which analyze the development of the CAE, it can be noted that from the year 2016 to 2022, the growth percentage of institutions adopting the CAE-R program was 23% going from 64 to 79 institutions, while for the program CAE-CDE, the growth percentage was 162% from the year 2016 to 2022, jumping from 128 to 335 institutions. It is

positively noticeable how the program has developed over the years, with a primary goal that remained the same and persist to foster higher education and research in the field of cyber defense, as well as the production of specialists with competencies in cyber defense. This is done to enhance the size of the cyber security workforce and lower the number of vulnerabilities in the national infrastructure of the United States (Centers of Academic Excellence in Cyber Defense Publication 4-8).

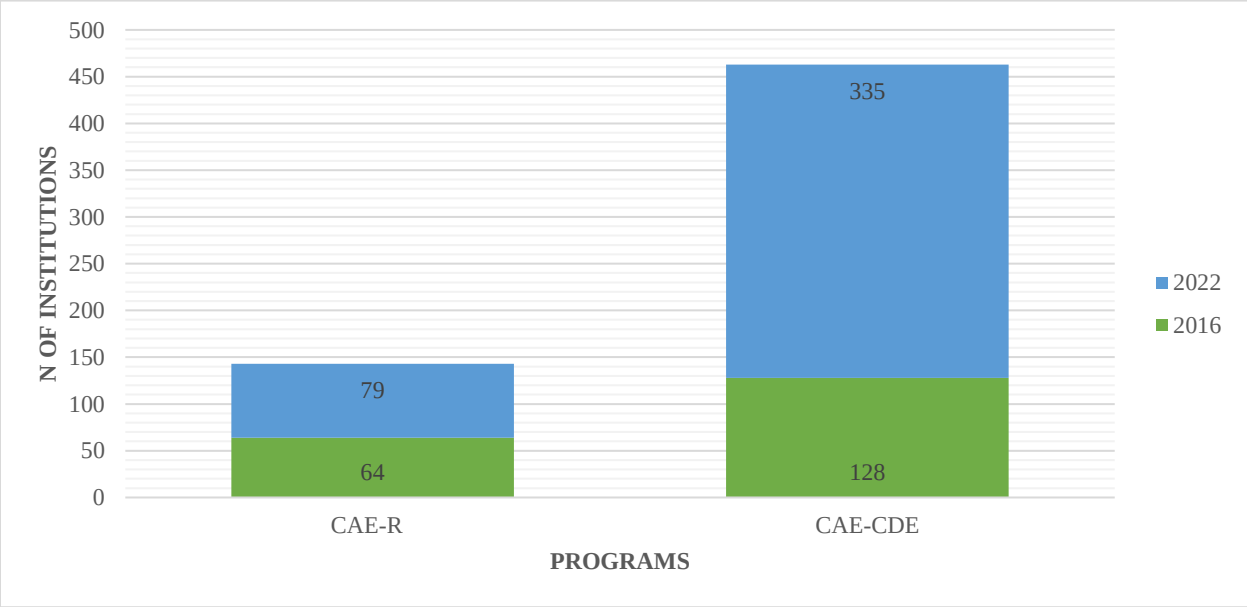


Fig. 7. Number of Institutions Adopting CAE-R & CAE-CDE Programs (2016, 2022)

Table 5
Number and Percentage of Institutions Adopting CAE-R & CAE-CDE Programs (2016, 2022)

Program	2016	2022	Percentage
CAE-R	64	79	23%
CAE-CDE	128	335	162%

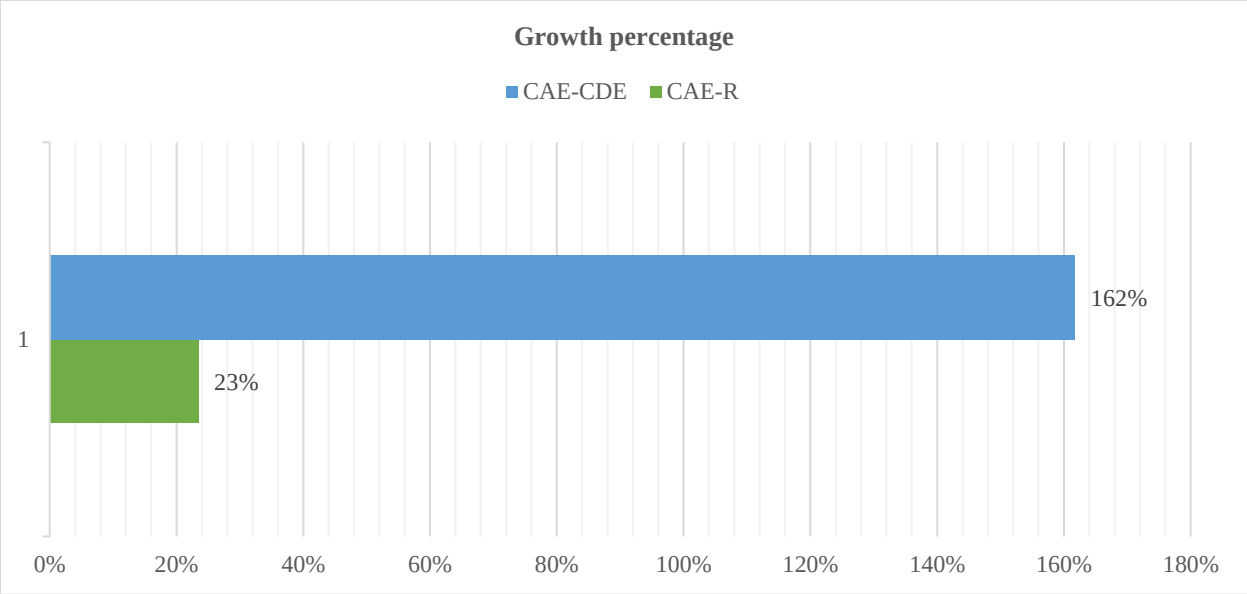


Fig. 8. Growth Percentage of Institutions Adopting CAE-R & CAE-CDE Programs (2016-2022)

6.1.3.2.CAE in Cyber Operation CO

The importance of the CAE in general and the CAE-CO can be interpreted from this data, which studied the growth of the CAE-CDE from (2016-2022) and the CAE-CO from (2015-2022). From the graphs and table above, from 2015 to 2022, the growth of the percentage of the CAE-CO program was 57% going from 14 to 22. The National Center for Education in Cyber Operations (NCE-CO) is an important initiative that promotes and supports high-quality academic programs that train the nation's cyber workforce. The NCE-CO focuses on technologies and techniques relevant to specialized cyber operations (such as collection, exploitation, and response) to improve the nation's national security posture (National Centers of Academic Excellence in Cybersecurity NCAE-C 2022).

Table 6
CAE in Cyber Operations (CAE-CO)

	2015	2022	Growth percentage (2015-2022)
CAE-CO	14	22	57%

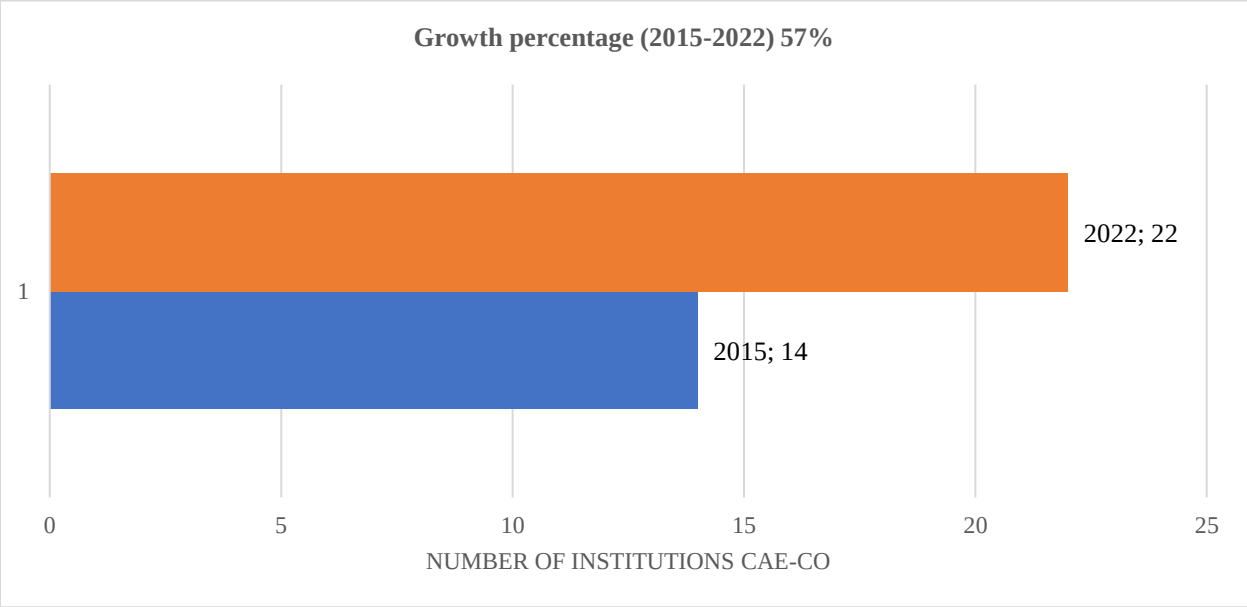


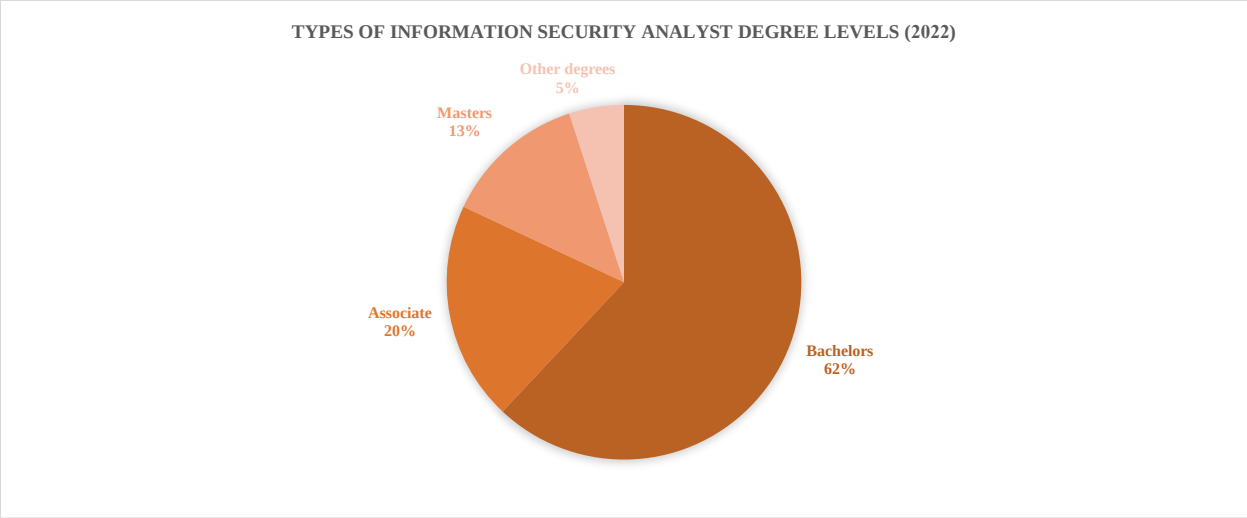
Fig. 9. Growth Percentage of Institutions Adopting CAE-CO Program

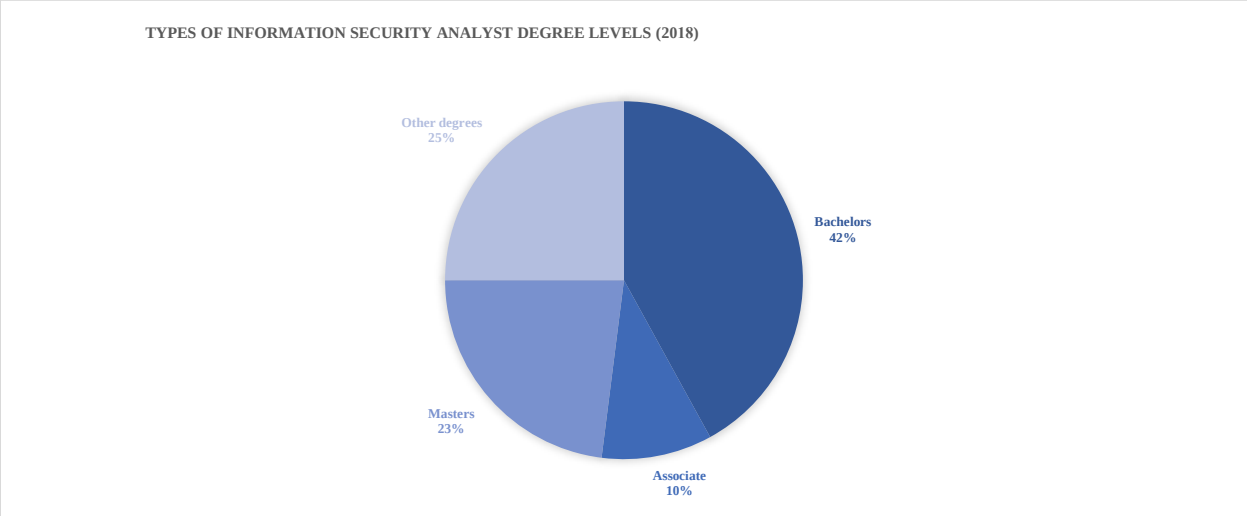
Today, over 230 colleges have been certified as CAEs and designated as Centers of Academic Excellence in Cyber Defense (CAE-CD); this project focuses on minimizing vulnerabilities in the United States national information infrastructure. An additional 20 programs have met the more intensive requirements to be recognized as CAE-CO, concentrating on specialized offensive cyber operations to enhance U.S. national security. The CAE-CO program has been greatly recognized for emphasizing foundational knowledge and practical training. The Homeland Security Advisory Council (HSAC) Task Force on CyberSkills, highlighted in 2012 that the CAE-CO schools were the only universities in the country offering cyber security courses that could “assure employers that hands-on skills are a major criterion for graduation” (Williams et al., 6-7).

Aside from its emphasis on core knowledge, the CAE-CO program is remarkable for requiring institutions to include hands-on lab opportunities for various courses, including software reverse engineering, networking, and cyber protection. The CAE-CO curriculum also allows students to obtain hands-on experience working with the NSA through summer internships, ensuring that every student has the opportunity to be exposed to real-world, on-the-job training throughout their study. The CAE-CO program succeeded in improving cyber security education; it has helped spur the development of many of the country's leading cyber security programs. The CAE-CO pointed the way toward a superior model for university-level cyber security education by requiring schools to cover basic technical skills and incorporate hands-on labs into their curriculum (Williams et al., 6-7).

5.2. The Progress of Information Security Analysts Graduates

The core issue of this data analysis of Information security analysts' graduates is that more people need to graduate with the necessary expertise to satisfy the expanding demand. According to Simpson (2019), there are less than 65,000 computer science undergraduates per year, with cyber security constituting only a small portion of that total (Beveridge 54). From the graphs and table above, it can be noted that the percentage of bachelor's degrees increased from 2018 to 2022 by 20%, as well as the percentage of associate degrees from 2018 to 2022 by 10%. However, it is also noticeable that the master's degree decreased by 10% in the master's in the same timeframe.





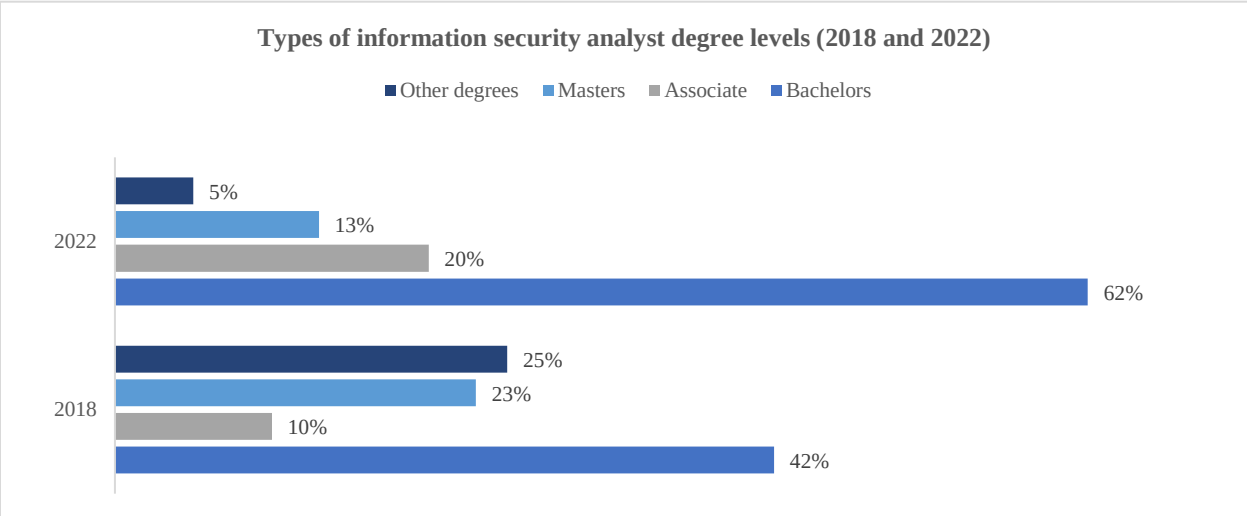


Fig. 10. Types of Information Security Analyst Degree Levels (2018), (2022)

Table 7
Percentage of Increase of each Degree Type (2018-2022)

Type of Degree	Percentage of increase (from 2018 – 2022)
Bachelors	20%
Associate	10%
Masters	-10%

There could be several underlying causes behind this decrease in master's degree holders specializing in information security. One possible explanation could be the need for adequate financial resources available for students interested in pursuing higher education related to information security or cyber-security studies at the postgraduate level since these courses tend to involve expensive lab equipment and software licenses and high tuition fees with such programs. It also reflects inadequate career prospects after graduation due to a shortage of job opportunities or low salaries compared to other more lucrative IT fields like software engineering, cloud computing... etc. Moreover, some students may opt out of these specialized programs because they feel overwhelmed by their complexity, thus leading them to pursue different options which they find easier on their wallet & time commitments.

5.3. Cyber Security Workforce: Demand Surpasses Supply

5.3.1. Data Analysis of the Labor Force in Cyber Security

The demand for cyber security jobs is on the rise. With the government and more businesses relying on digital systems to store, process and protect their data, the need for qualified professionals in this field has never been greater. Eventually, the total employed cyber security workforce continues increasing each year due, largely in part because of how essential these professionals are becoming across all types of industries around the globe. The data analyzed below shows the statistics of the total cyber security job opening and the total cyber

security labor force and how they immensely increased because of the urgent demand for this pipeline of professionals.

Table 8
Total Cyber security Job Openings and Employed Workforce (2016-2022)

Year	Total cybersecurity job openings	The total employed cybersecurity workforce	SUPPLY/DEMAND RATIO
2016	11153	17182	65%
2018	313735	715715	44%
2020	507924	922720	55%
2021	597767	1053468	57%
2022	769736	1108725	69%
Increase rate (2016-2022)	**6802%**	**6353%**	

Increase Rate = (final value - initial value) / initial value %

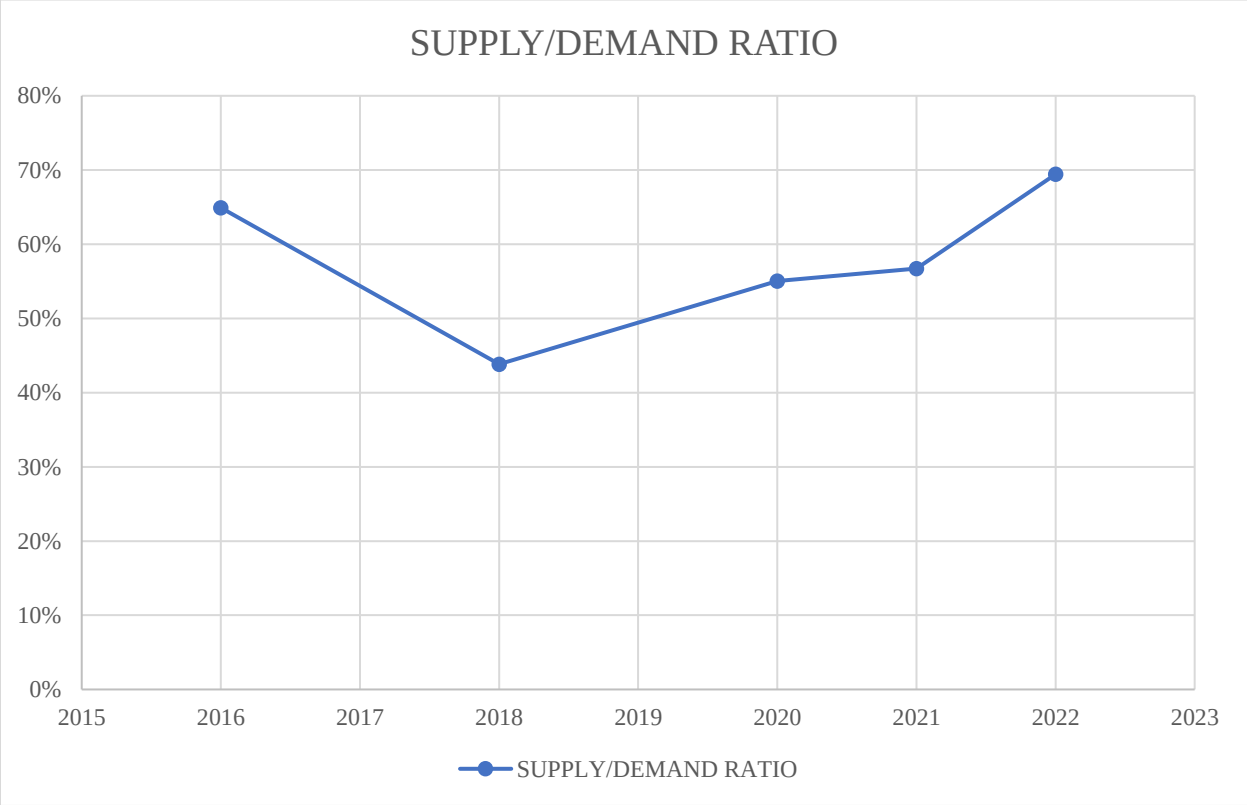


Fig. 11. U. S. National Supply/Demand Ratio between Total Cybersecurity Job Openings & The Total Employed Cybersecurity Workforce (2022)

The data presented in the table and graph above clearly show the recent status of cyber security job openings and the employed workforce in the United States. From 2016 to 2022, there has been an impressive 6802% increase rate for total cyber security job openings, going from 11153 to 769736. Similarly, there has been a 6353% increase rate for the total employed cyber security labor force over this period, increasing from 17182 to 1108725 individuals. This shows that the increasing demand for cyber security professionals is being met with a healthy rise in the workforce.

This rapid growth is indicative of both increased demands for skilled cyber security professionals and a lack of adequate supply, given that employers can only fill 44-68% of these positions with existing personnel at any given time during these six years, according to the Supply/Demand Ratio graph. This suggests that although more people are entering into cyber security-related jobs each year than ever, there may not be enough qualified applicants available yet to meet employer demands fully or even close by 2022 if trends continue on their current trajectory.

Based on the table and graph above, it is clear that the number of job openings and employed cyber security workers have seen a significant increase from 2016 to 2022. The total number of job openings has increased from 11,153 in 2016 to 769,736 in 2022, representing an increased rate of 6802%. Similarly, the total employed cyber security labor force has increased from 17,182 in 2016 to 1,108,725 in 2022, representing an increased rate of 6353%. This shows that the increasing demand for cyber security professionals is being met with a healthy rise in the workforce.

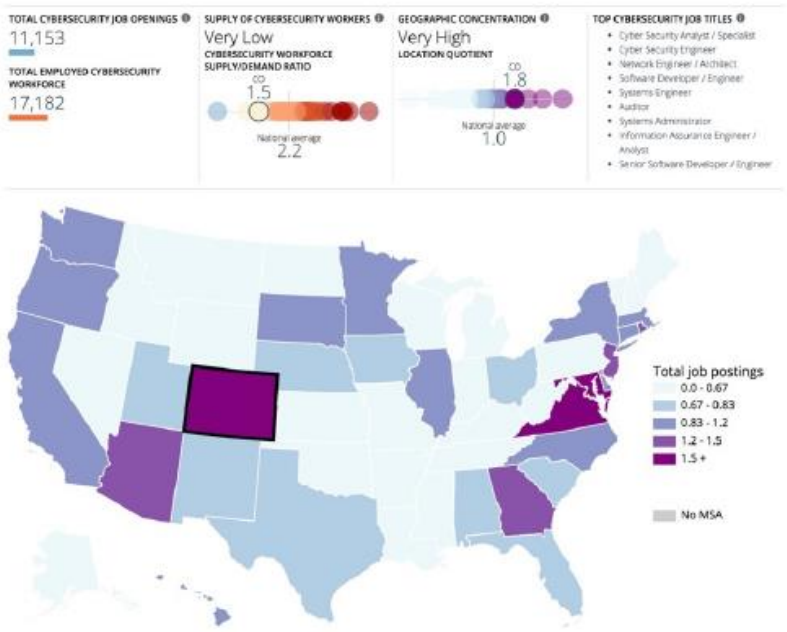


Fig. 12. Total Cybersecurity Job Openings and Employed Workforce2016 Michelle Lange. "CyberSeek Tracks Explosion in Cybersecurity Demand." *Default*, 1 Nov. 2016, https://www.comptia.org/blog/cyberseek-tracks-explosion-in-cybersecurity-demand.

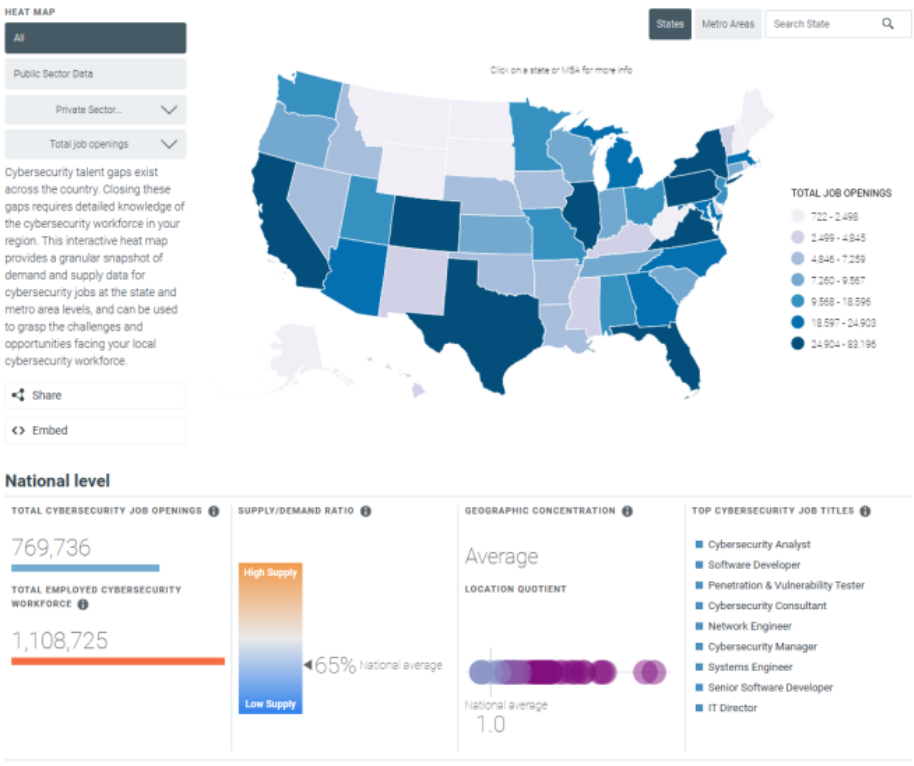


Fig. 13. Total Cybersecurity Job Openings and Employed Workforce2022 *Cyberseek.org*, https://www.cyberseek.org/heatmap.html.

5.4. The Reasons Behind the U.S. Shortage

> There are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. in order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. (The White House 1-5, CNCI May 2009).

The main challenge in aligning cyber security capabilities and needs is a more cyber security workers. The United States' best protection against new cyber dangers is to "create a robust, nimble, and highly trained cyber security employees. To grow this workforce, firms must first assess their present supply as well as strategies for identifying and meeting future demand". It is easy to understand the vital role cyber security employees play in national defense and capabilities planning; nevertheless, there is a cyber security labor force shortage compared to the number of positions that need to be filled. Furthermore, beyond the current demand for cyber security professionals, many more will be required in the future (Coulson 4-7).

The Global Information Security Workforce Study from (ISC)2 in February 2017 identified a labor force gap between the cyber security workers needed and those able to perform those roles. The group predicts a 1.8 million employment deficit in the world by 2022. Furthermore, CyberSeek estimates that there are 285,681 overall cyber security job opportunities, with a very low supply of cyber security workers. The federal government needs more qualified cyber security personnel. Tony Scott, the former Federal CIO (the United States Government's Chief Information Officer), projected in 2015 that there were more than 10,000 unfilled positions for cyber employees, but more people needed to fill them. Policymakers must

address this shortage by establishing a pipeline through which persons can be trained in cyber security before being employed and retained in the federal cyber security workforce (Coulson 4-7).

The shortage of cyber security professionals has been studied before. Studies showed that the cyber security workforce is more than a simple problem of the lack of specialists; it is more related to the quality than to the quantity, especially in the beginning of the widespread of this phenomenon:

> The problem is both of quantity and quality, especially when it comes to highly skilled…professionals. [The United States] not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts. (Wennergren 10-11)

In recent years, it has become evident that the cyber security personnel requirements are multifaceted and diverse. Many different types of talents are required. While some job categories have long been established, and there is a high demand for technological skills, not all desired job categories are entirely or even largely technical. Furthermore, even in technical professions, every graduate must be capable of problem-solving and critical thinking (10-11).

The problem of the cyber security workforce shortage reached a critical level in 2009. Former President Barack Obama described the U.S. lack of qualified cyber security personnel as "one of the most serious economic and national challenges we face as a nation" (Office of the Press Secretary, 2009). Effectively minimizing and reacting to cyber threats requires a

knowledgeable and well-trained cyber security team. Information security professionals are in high demand, yet there is a scarcity of them throughout the world. Cyber security Ventures, a research firm, believes that there are over a million unfilled vacancies in the cybersecurity industry throughout the globe. The present rate of employment growth in cyber security is expected to result in 3.5 million vacant positions by 2021(King). Companies have reported many challenges in recruiting and hiring for available jobs. Talented professionals are being nurtured in classrooms around the country, but many of these schools' programs are still in their infancy (Beveridge 55).

Dr. Gregory White, a professor of computer science and the director of UTSA's Center for Infrastructure Assurance and Security, claims that there is a shortage of qualified workers in the cyber security industry because the United States is unable to produce enough graduates to meet the market's rising demand. "We could double the number of people in school now and still not fill all open positions," White says. Working Around the Labor Shortage, it is clear that "Organizations need to truly ask themselves if their positions require a [four-year IT] degree," he said: "I would guess that a number of vacant positions can be filled by people without a degree." In fact, many cyber security professionals learned the necessary skills through certificate programs and on-the-job training rather than a degree program.He believed that: "There are students in the San Antonio area that are obtaining two or three certifications in high school and getting job offers after graduation" (Projected Job Growth in the Five Most Populous States).

Rigorous assessments are required to certify colleges and universities. The NSA, in collaboration with NICE and the NICE Workforce Framework, has defined standards that all CAE-CD institutions must satisfy (National Institute of Standards and Technology, 2017). Therefore, there is already a system in place to certify colleges that may develop scholarship

programs to educate students for government cyber security employment. For the initiative to be effective, however, sufficient money is essential.

5.4.1. The Shortcomings in Cyber Security Programs

According to a recent CSIS poll of IT decision-makers from eight countries, 82% of businesses reported a scarcity of cyber security capabilities, and 71 percent say that this talent gap causes direct and measurable harm to their organizations. According to CyberSeek, a National Initiative for Cybersecurity Education (NICE)-funded initiative, the United States had a cyber security professional shortage of almost 314,000 as of January 2019. To put this in context, the country's overall cyber security workforce is only 716,000 people. According to job posting data, the number of unfilled cyber security jobs has increased by more than 50% since 2015. The global cyber security manpower gap is expected to reach 1.8 million unfilled positions by 2022(Crumpler and Lewis 1).

There are workforce shortages in practically every area within cyber security, but the most pressing demands are for highly qualified technical personnel. According to the CSIS report A Human Capital Crisis in Cyber security, the United States:

> Not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts. (2)

According to the interviewees, the United States only possessed around 1,000 security specialists with the necessary skills and competencies to fill these tasks, despite a demand for 10,000 to 30,000 employees (2)

Since 2010, these challenges have prevailed. CSIS discovered in 2016 that IT professionals still deemed technical skills such as intrusion detection, secure software development, and attack mitigation to be the hardest to find. A 2018 poll of California firms indicated that one of the organizations' biggest issues when hiring cyber security candidates was a lack of essential technology capabilities. These difficulties were especially apparent for mission-critical employment roles, with more than a third of firms reporting a shortage of technical skills in candidates. Employers currently require more cyber security professionals; what organizations genuinely require are graduates who can design safe systems, develop new defense tools, and identify hidden flaws in software and networks. (Lewis and Crumpler 2)

5.4.1.1. U.S. Graduates Lack of Cyber Security Skills.

Cyber security education and training programs in the United States should be evaluated to see whether they are educating students for the sorts of high-skilled technical professions that have the greatest need for workers. It seems unlikely that the answer is yes. According to the recently released Report to the President on *Supporting the Growth and Sustainment of the Nation's Cybersecurity Professionals*, written by the U.S. Departments of Commerce and Homeland Security, businesses are growing increasingly concerned about the importance of cyber security-related educational programs in addressing the requirements of their organizations. Only 23% of IT firms in a 2016 CSIS poll said that current education programs effectively equip students for careers in cyber security. ISACA, a professional group, found in 2018 that 61 percent of businesses feel that less than 50 percent of candidates for available cyber security roles are suitable for the job (Prebil).

According to cyber security practitioners, employers are disappointed because graduates of these schools need more practical experience and knowledge of the principles of computers

and information security. As a result, many graduates need substantial on-the-job training before they can start working. Furthermore, companies frequently find that cyber security graduates need to improve in soft skills such as teamwork, problem-solving, and communication. Organizations are also dissatisfied with the present cyber security education environment, which lacks consistent criteria or rankings to assist companies in determining which programs, certifications, and degrees are most successful. Addressing these concerns would assist the U.S. in strengthening its cyber security talent pipeline (Crumpler and Lewis 2).

5.4.1.2. Graduates Lack the Fundamentals.

Cyber security spans a wide range of specialty areas and job positions, and only some education programs can be expected to provide all the particular skills and industry knowledge required by each company. However, certain knowledge sets and abilities are required for any new employee in a crucial technical work role, regardless of their chosen field or specialty. Understanding computer architecture, data, cryptography, networking, secure coding principles, operating system internals, proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques are required. Employers are discovering that graduates lack this basis; one of the corporations indicated: “the current [education] environment does not provide a common baseline set of skills from which to build the role-specific knowledge necessary to meet employer workforce requirements.” (3).

Cyber security programs emphasize policy planning, compliance audits, and other skills that, in the end, have less impact on an organization’s security posture than duties enabled by a strong technical foundation. According to studies, these tasks—which include penetration testing, secure system design, incident response, and tool development—represent the highest

requirement for enterprises (Libicki and Senty 28). However, these positions can only be filled by employees who understand computing foundations and how an organization's information systems work. Traditional computer science programs do not teach students the fundamentals of information security. A 2016 survey found that only one of the country's top 36 computer science programs required a cyber security course for completion, while three of the top ten programs offered no cyber security classes at all. Without prior experience in cyber security, computer science graduates face significant barriers to entry in the area (Crumpler and Lewis 2).

5.4.1.3. Graduates Lack Practical Skills (Hands-on Experience)

One of the most common criticisms directed at cyber security education programs is that an overemphasis on theory and book learning precludes students from developing the necessary practical skills. Theory alone will not equip graduates for the tasks they confront on the job. Practical training and hands-on experience are required to provide students with the practical skills that companies demand (Crumpler and Lewis 4).

According to surveys, organizations prioritize hands-on experience over all other factors when evaluating new hires. The incorporation of a hands-on learning environment, in which students work on realistic cyber security challenges, has been identified as one of the key factors distinguishing leading education programs in the eyes of cyber security practitioners. According to the non-profit cyber security training group U.S. Cyber Challenge, "hands-on, applied learning methods are the common thread across the most effective public, private, domestic, or international cyber workforce training programs." (Cybersecurity Career Opportunities).

Organizations continue to discover that graduates of cyber security programs lack hands-on experience; "Their training is also most often theoretical," according to the professional body ISACA; "Their training is also most often based in theory. They receive very little hands-on

training; thus, the skill sets need to be developed on the job." As a result, the value of a cyber security degree has begun to decrease in the eyes of employers, with surveys indicating that up to 80% of hiring managers believe a four-year degree no longer effectively equips students for cyber security positions (Crumpler and Lewis 4).

5.4.1.4. Graduate Lack of Soft Skills

All cyber security education and training programs must prioritize developing technical competency in their trainees as their top objective. However, schools still need to emphasize the need for students to develop soft skills that may translate technical knowledge into value for their employers. Organizations have continuously identified soft skills like communication, teamwork, and problem-solving as significant for new recruits. According to a poll conducted by the security business Tripwire, 100% of respondents said soft skills were vital when hiring for a security team, and 21% thought they were more important than hard skills (Crumpler and Lewis 5).

Many cyber security education program graduates need to gain these soft skills. According to the CSIS poll, 70% of cyber security graduates believe communication to be a scarce skill set, and more than half struggle to identify individuals that are good at teamwork and team leadership. Failure to develop these abilities significantly influences graduates' effectiveness once they enter the workforce. Because a single individual rarely handles cyber security, the ability to work as part of a team is crucial. Problem-solving is at the heart of effective cyber security employment, and many graduates face substantial challenges regarding real-world troubleshooting systems. Finally, communication and writing skills are required for translating technical knowledge into business value, whether by communicating threats and

trends to business management or by writing and implementing effective, user-friendly cyber security policies to protect an organization's information systems (Crumpler and Lewis 5).

5.4.2. Women Cyber Workforce Shortage

By 2021, it is anticipated that cybercrime will cost the global economy more than $6 trillion. As a result of their efforts to protect the information that is most important to them, businesses are devoting a significant number of resources to safeguard themselves against incidents like this. Businesses are shelling out more than one hundred billion dollars annually for cyber security personnel, resources, insurance, and technology. Unfortunately, only 12,000 of the 56,000 graduates are women or minorities. It became extremely difficult to fill positions worldwide since there was a shortage of skilled workers, especially with a low representation of women and other underrepresented groups in the technological workforce (Beveridge 54).

The statistics for 2019 of senior cyber security women in cyber security show how men and women predominate in the senior cyber security analyst position over time. The statistics on the graphs and the table below indicate a low representation of women in the cyber security analyst profession, 18,8% compared to males, which are the dominant category in this profession with 81,2%. The man containment of the cyber security position is remarkable in the statistics of cyber security analysts by year. The percentage of male representation in cyber security analyst positions continues to grow progressively from72,86% in 2010 to 81,94% in 2019, whereas the female percentage in this position keeps getting lower; it fell from 27,14% in 2010 to 18.06 % in 2019.

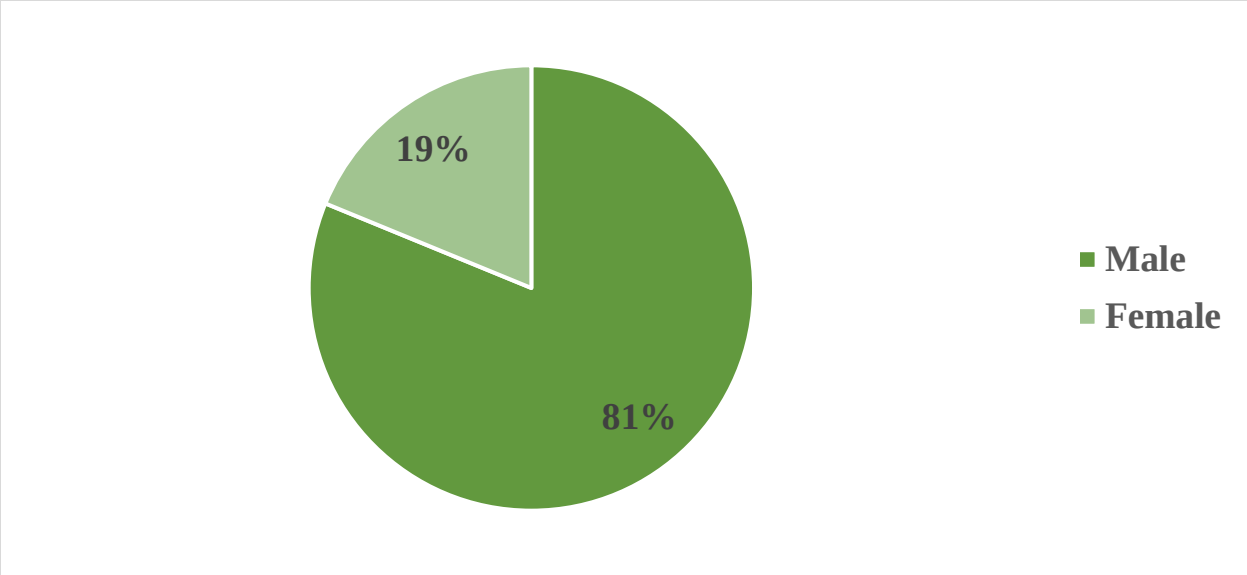


Fig. 14. Senior Cyber Security Analyst Gender Representation 2019. ("Cyber Security Analyst Demographics and Statistics [2023]: Number of Cyber Security Analysts in the US").

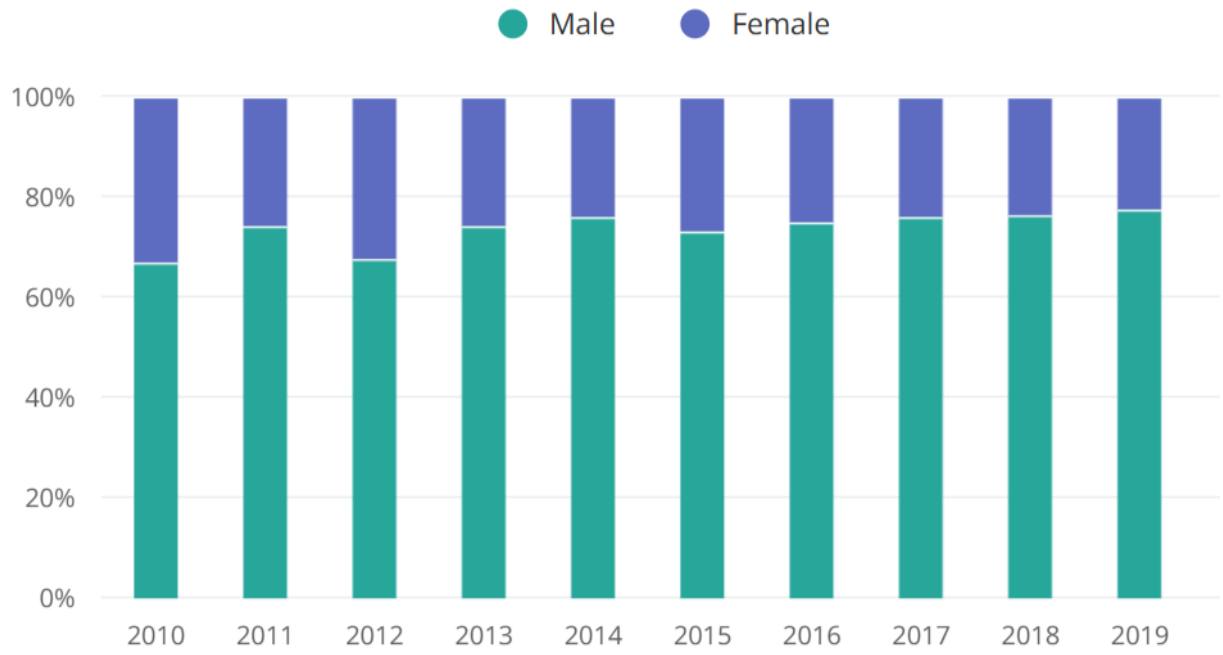


Fig. 15. Senior Cybersecurity Analysts by Year (2010-2019) ("Cyber Security Analyst Demographics and Statistics [2023]: Number of Cyber Security Analysts in the US").

Table 9
Senior Cybersecurity Analysts by Year

Year	Male	Female
2010	72.86%	27.14%
2012	73.32%	2668%
2015	78.36%	21.64%
2013	79.04%	20,96%
2011	79.22%	20.78%
2016	79.85%	20.15%
2017	80.72%	19.28%
2014	80.73%	19.27%
2018	81.12%	18.88%
2019	81.94%	18.06%

Adapted from: ("Cyber Security Analyst Demographics and Statistics [2023]: Number of Cyber Security Analysts in the US") "Cyber Security Analyst Demographics and Statistics [2023]: Number of Cyber Security Analysts in the US." *Zippia.com*, 9 Sept. 2022, https://www.zippia.com/cyber-security-analyst-jobs/demographics/.

Women's shows to be more interested in other fields than cyber security, and their contribution is considerable regarding this field. Women make up 15% of the military workforce, of which 25% are in information technology fields, which cyber security is a subdivision of (Poster, 2018). In the civilian sector, women make up 25% of information technology jobs; however, in cyber security jobs, women make up only 14%. The real challenge facing the women's job market is that 56% of all those in information technology depart after five years to pursue other jobs, resulting in a decrease rate of women's contribution that doubles that of men in the same field (Annabi & Lebovitz, 1046).

According to Annabi and Lebovitz, women are abandoning sectors related to technology for various reasons, some of which include but not limited to "stereotypes, questions of legitimacy, isolation, access, masculine organizational climate, and work-life balance" (p. 1050). Employers need to take advantage of highly trained women and promote to recruit this underrepresented group into the information technology industries, including but not limited to

cyber security, in order to close the labor shortfall gap. This will allow the workforce gap to be closed (Beveridge 55).

The under-representation and under-utilization of female talent is a key business issue and a barrier to developing more secure and resilient economies and communities, as well as the overall safety and protection of countries. This disparity exacerbates gender inequality in other industries while also increasing the scarcity of cyber security workers at a time when they are in great demand. Furthermore, female internet users face a higher rate of cybercrime, online harassment, and security breaches. These considerations highlight the pertinence of developing a safer and more gender-inclusive cyberspace, as well as promoting initiatives to reduce the labor force and gender gap (Women Cybersecurity: Creating a More Inclusive Cyberspace).

There is a need to have more diversity in the U.S. national workforce. Women's low representation in cyber security job positions is causing an evident threat to the U.S. labor force equilibrium. It is an obsolete fact in Science, Technology, Engineering, and Math (STEM) fields, but it is more damaging in cyber security. Lower participation percentages can mean that organizations miss out on extra applicants with promise and the valuable contributions of diverse teams. As one industry executive put it, "mature cyber security teams require a mix of skills and diversity of thought—you must foster inclusive teamwork that integrates multidisciplinary and diverse perspectives" (Ross and E. Duke 4).

Women's underrepresentation in internet security is linked to a greater issue of underrepresentation in science, technology, engineering, and mathematics. Women make up only 30% of scientists and engineers in the United States. Although there is nothing inherent in gender that predisposes men to be more interested in or proficient at cyber security, this is the prevalent perception. Furthermore, the business misleads potential employees into believing that only

technical abilities are important in cyber security, which might give women the impression that the area could be more complex or an area of their interest (Kshetri).

This disparity exists despite the fact that women make up more than half of the global labor force and can be attributed to a wide range of causes, including stereotypes and biases in the workplace, societal and family pressures, a lack of digital and cyber literacy, wage gaps, lower earning potential at every level, missed or delayed promotions, and a more difficult path to the top of the corporate ladder. Despite the fact that women often have more education and credentials than males, this is still the case (Women Cybersecurity: Creating a More Inclusive Cyberspace).

5.5. The Alarming Cyber Security Threats: Assessment and Implications

5.5.1. Cybercrime Financial Losses

The data presented in the graphs and table above is alarming, as it reveals a sharp increase in cybercrime financial losses across the United States. From 2017 to 2021, these losses increased by 429%, with New York experiencing the largest rise of 532%. California experienced an even more drastic jump over this period: 214U.S. million dollars lost in 2017 compared to 1227.99 million U.S. dollars lost four years later, an overwhelming 473% increase! Washington state saw comparatively less growth at 266%, but still enough to cause concern among citizens and business owners; they are vulnerable to cyber-attacks or other forms of malicious activity online. This loss due to cybercrimes is a high financial menace to American financial security, particularly in states like New York and California.

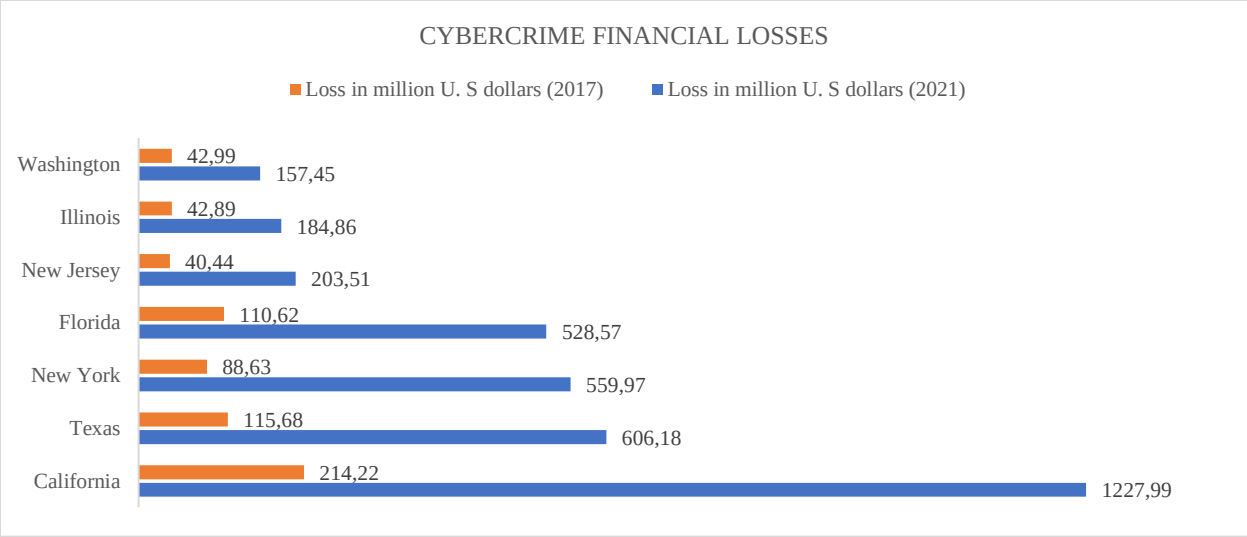


Fig. 16. Cybercrime Financial Losses between 2017-2021

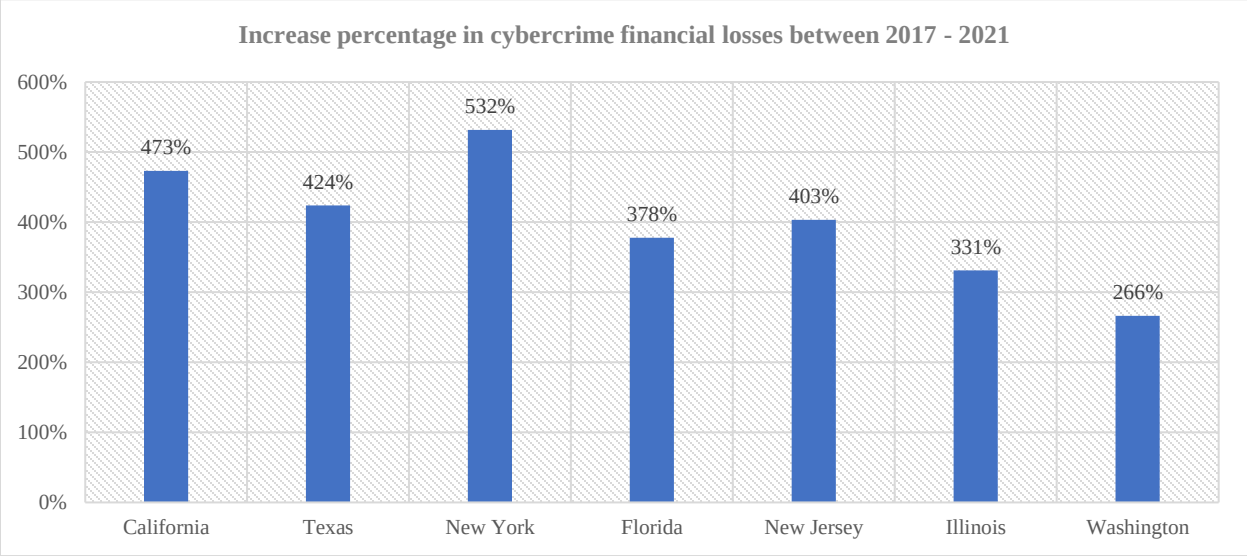


Fig. 17. The Increase Percentage of Cyber Security Financial Losses between 2017-2021

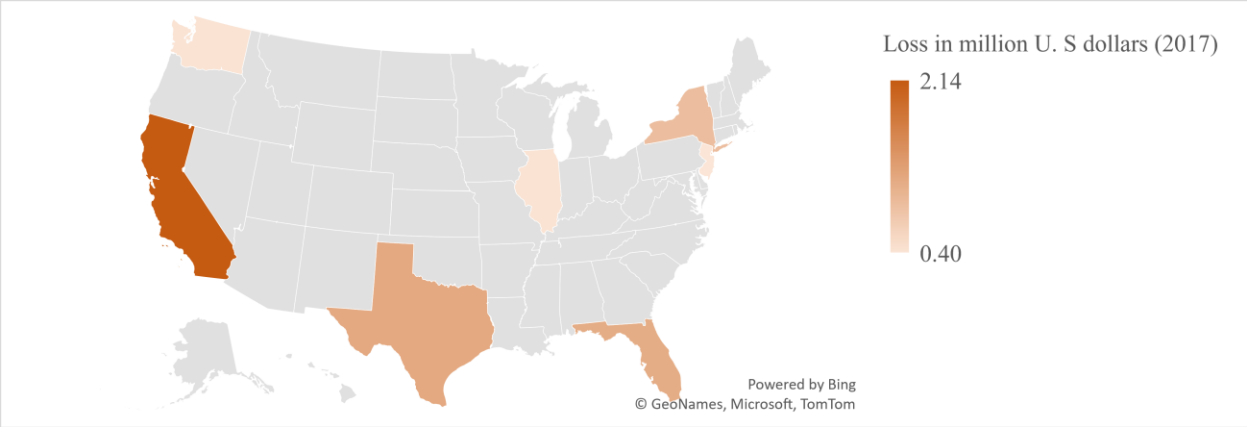


Fig. 18. The Main States Affected by Cybercrime Losses in 2017

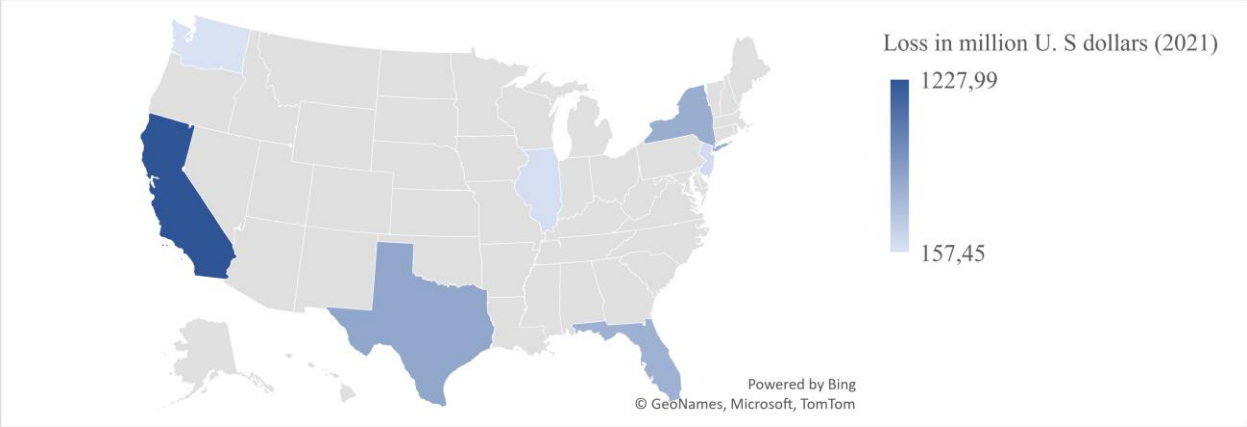


Fig. 19. The Main States Affected by the Cybercrime Losses in 2021

Table 10
The Increase Percentage in Cyber Security Financial Losses between 2017-2021

	Loss in a million U. S dollars (2017)	Loss in a million U. S dollars (2021)	Increase percentage
New York	88.63	559.97	532%
California	214.22	1227.99	473%
Texas	115.68	606.18	424%
New Jersey	40.44	203.51	403%
Florida	110.62	528.57	378%
Illinois	42.89	184.86	331%
Washington	42.99	157.45	266%
Total	**655.48**	**3468.53**	**429%**

5.5.2. Cyber Complaints and Cyber Losses

The table and the graphs below illustrate the number of complaints (in billions) in the U.S. banking sector from 2016 to 2020. It can be noted that there has been a significant increase in both categories over this period. In terms of complaints, it is evident that they have risen steadily since 2016, from 298,728 to 791,790 by 2020, an increase of almost 400%. When examining total losses (in billions), we see that while there was a slight decrease from 2016-2017, this figure has increased continuously to reach $3 billion by 2020. The reasons behind this could range from internal to external threats such as cyberattacks and data breaches, which put sensitive information at risk and cost companies dearly in terms of payment protection insurance claims. The fatal external factor that contributed to this immense rise in losses is the Pandemic (Covid 19) that hit the world in general and the U.S. particularly. Its impact had abrupt results on the American economy because of the new policies adopted, such as healthcare and work protocols (will be discussed above in details).

Table 11
The Number of Cyber–Breaches Complaints and the Total Losses

Years	Total Complaints	Total Losses (In Billion)
2016	298.728	$1.50
2017	301.58	$1.40
2018	351.937	$2.70
2019	467.361	$3.50
2020	791.79	$4.20
Total	**2211.396**	**$13.30**

Adapted from: Paul Abbate. "2020 Internet Crime Report." *Ic3.gov*, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Page 5.

5.5.3. Top Crime Type Comparison 2016-2020

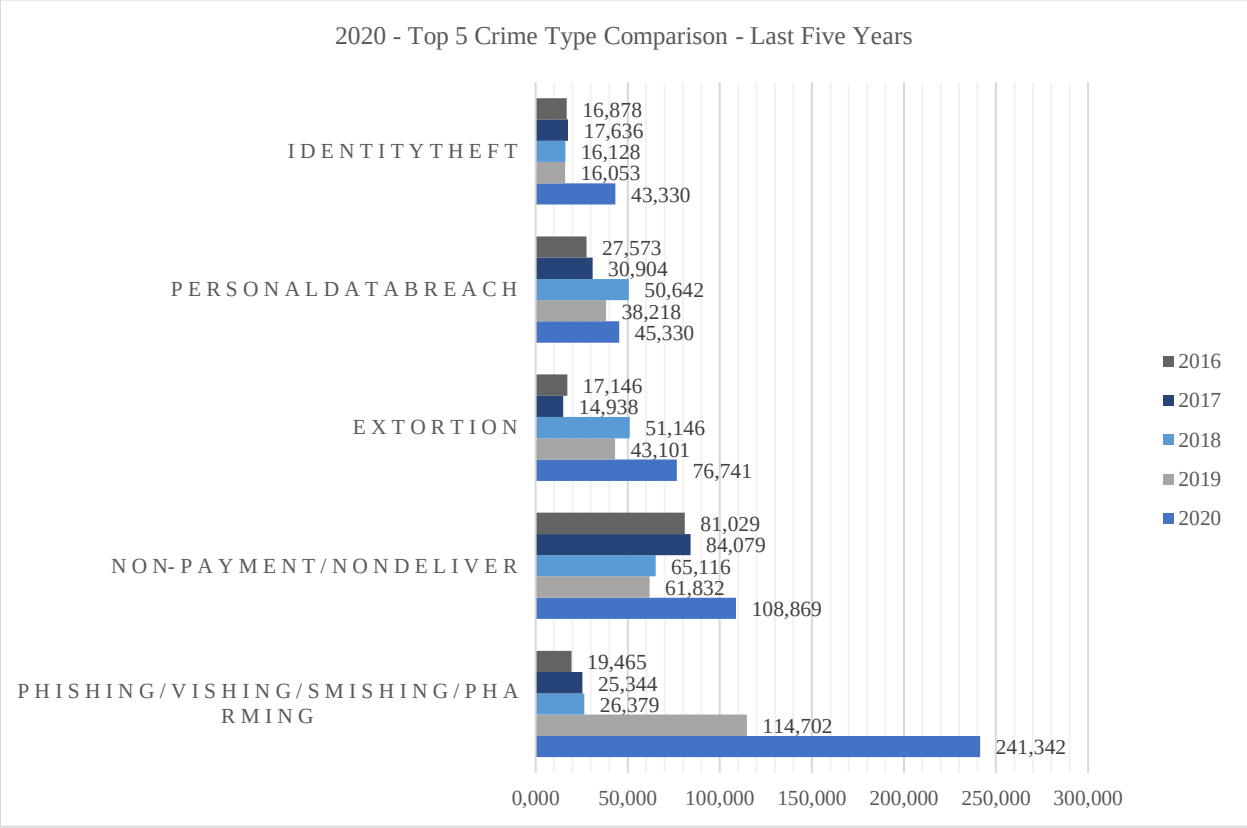


Fig. 20. Top Crime Type Comparison 2016-2020. (Abbate 6).

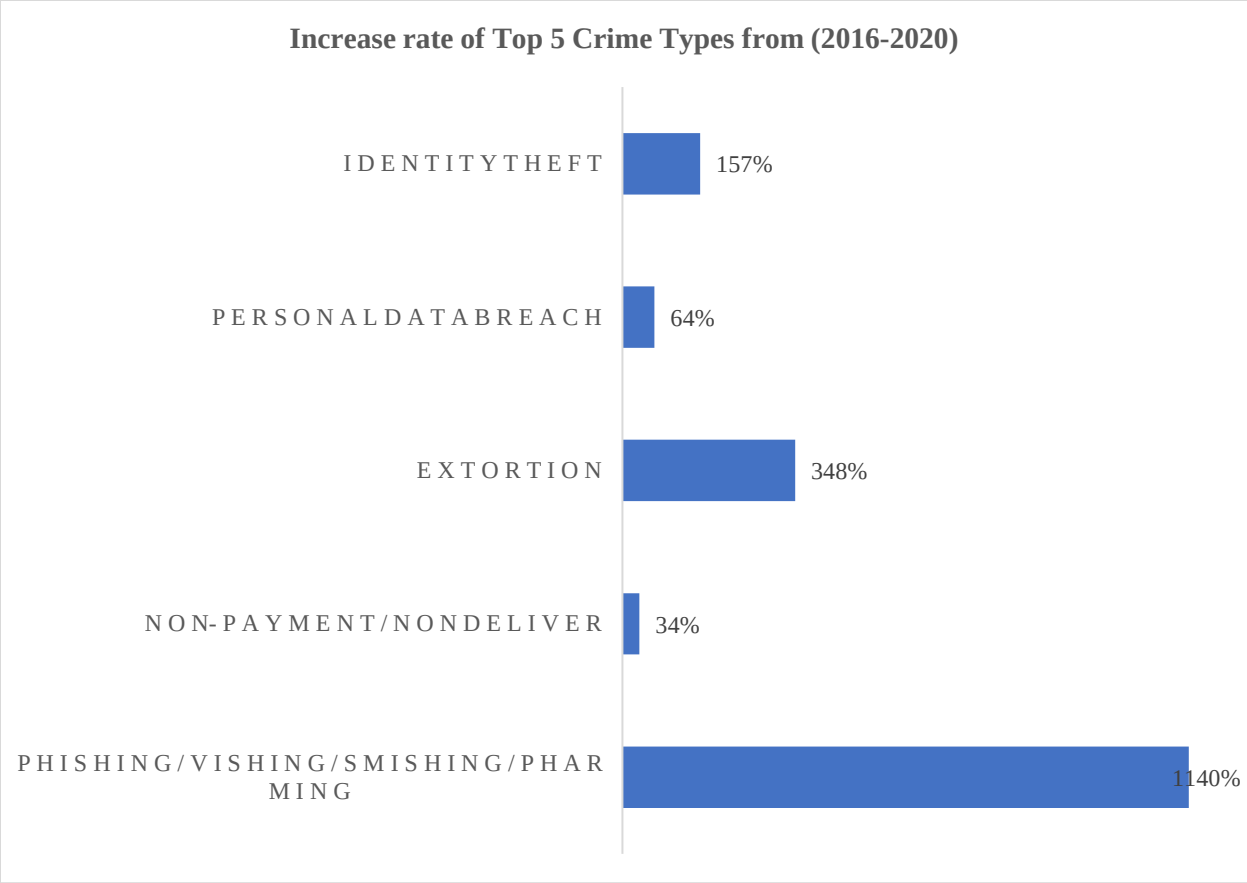


Fig. 21. Increase Rate of top 5 Crime Type From (2016-2020).

Cybercrime has become increasingly prevalent in our digital world, with an alarming rise in the number of complaints reported over the past five years. From 2016 to 2020, all five cybercrimes (phishing/vishing/smishing/pharming) dramatically increased. They had the highest rate of increase at 1140%, going from 19.465 cases in 2016 to 241.342 cases in 2020. A high record for these types of crimes indicates how severe this issue is becoming across nations as technology evolves each year exponentially.

5.5.4. The Correlation between Cyber Complaints Reported and Losses.

Understanding the correlation between these two variables is very important here. The correlation between the total complaints (cyber-complaint reported) and total losses is a significant one proven by statistical analysis. It can be noted from the correlation table between

these two variables that there is a strong positive relationship with an 88.6% value for their association, which also happens to be significant at the 0.05 level (0.045 < 0.05). This implies that any increase in total complaints will contribute directly to an 88.6% increase in overall losses.

Table 12
The Correlation

		Total Complaints	Total Losses (In Billion)
Total Complaints	Pearson Correlation	1	.886*
	Sig. (2-tailed)		.045
	N	5	5
Total Losses (In Billion)	Pearson Correlation	.886*	1
	Sig. (2-tailed)	.045	
	N	5	5

*. Correlation is significant at the 0.05 level (2-tailed).

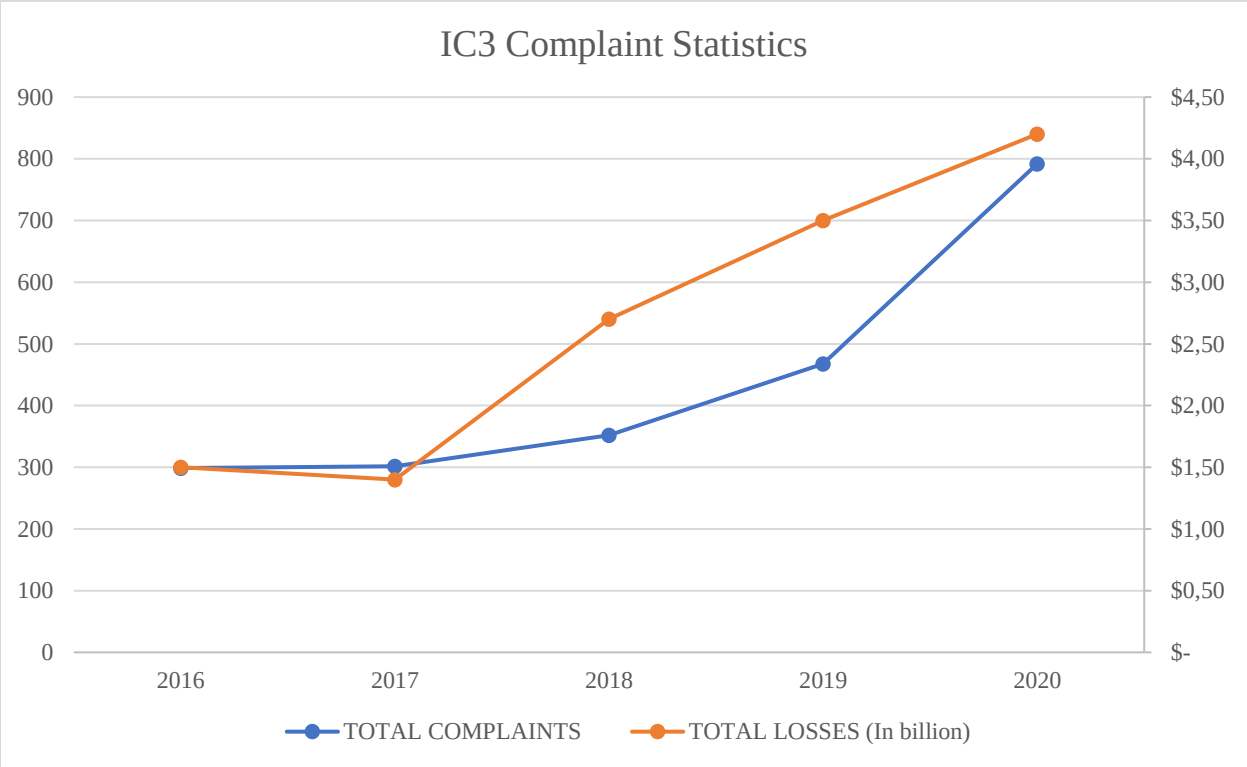


Fig. 22. Complaints and Losses Statistics (2016-2020)

Table 13
Top 5 Cybercrime Type Comparison – (2016-2020)

	Phishing / vishing / smishing / pharming	Non-payment / non deliver	Extorsion	Personal data breach	Identity theft	Total
2020	241.342	108.869	76.741	45.330	43.330	**515.612**
2019	114.702	61.832	43.101	38.218	16.053	**273.906**
2018	26.379	65.116	51.146	50.642	16.128	**209.411**
2017	25.344	84.079	14.938	30.904	17.636	**172.901**
2016	19.465	81.029	17.146	27.573	16.878	**162.091**
Total	**427.232**	**400.925**	**203.072**	**192.667**	**110.025**	**1333.921**
Increase rate	1140%	34%	348%	64%	157%	

Adapted from: (Abbate 6).

The COVID-19 pandemic has profoundly impacted the cyber security of the United States. The most recent statistics from 2016 to 2020 demonstrate a significant increase in all five major cybercrimes, with Phishing/vishing/smishing/pharming having the highest increase rate by 1140%. This alarming trend can be linked to increased vulnerability due to people working remotely and using less secure networks during this time.

The disruption caused by COVID-19 has made it easier for criminals to target vulnerable individuals and businesses and exploit weaknesses in technology infrastructure. With more people relying on digital tools for communication, collaboration, and commerce than ever, organizations have rapidly adopted digital technologies without adequate planning or safeguards against potential threats. This lack of preparedness has created opportunities for malicious actors who can take advantage of lax security measures or even create new ones through social engineering attacks such as phishing emails or fake websites designed specifically with malicious intent.

5.5.5. COVID-19 as an Escalating Threat to Cyber Security

Even before the outbreak of the COVID-19 pandemic in 2020, it was anticipated that a large number of IT positions would be in high demand throughout the following decade. Because

of the epidemic, those who work in information technology will be even more vital to the economy in the future. The COVID-19 conference contributed to the anticipated expansion of computer jobs, which are forecast to have a significant level of growth between the years 2020 and 2030.

Since the beginning of the pandemic, there has been an increase in remote and hybrid work arrangements in places of employment. There was a boom in online commerce, and the availability of telemedicine and telehealth services has substantially expanded. Because of these shifts, there is a greater need for highly developed and complex cyber Security solutions and an increase in the number of computer experts. Over the decade spanning 2020–2030, employment in computer-related fields is expected to increase by 13.4 %, which is 5.7 percentage points greater than the average growth rate of 7.7 % for all occupations. Notably, the occupation group that deals with computers did not witness a drop in employment throughout the epidemic (Sara).

One of the most significant changes brought about by the COVID-19 pandemic is the rise of distant and hybrid work, which is also one of the shifts likely to persist over the long run. At the beginning of the epidemic, there was a noticeable rise in the number of people working from home. In the early months of the COVID-19 pandemic, Global Workplace Analytics performed a poll, and the results showed that 77% of office-based workers were working remotely full-time, compared with only 9% at the start of the epidemic. Even if some employees have returned to their jobs since the pandemic's peak, the percentage of employees working remotely, full-time or part-time, is still significantly higher than the trend before the pandemic. According to a poll of full-time workers in the United States that Gallup carried out in September 2021, 45 % of employees worked either entirely or partially from their homes (Sara).

The unexpected transition of a sizeable section of the workforce to remote or hybrid work environments produced substantial disruptions and slowdowns in network performance for many businesses in the United States. Working remotely raises concerns about network safety because it expands the number of entries points that hackers can use to compromise computer systems. During the pandemic, hackers and other online criminals took advantage of the fact that many people were working remotely to find and exploit weaknesses in IT infrastructure and mobile device networks. It is anticipated that there will be a 33.3% increase in the number of jobs available for information security analysts between 2020 and 2030. This is due to the significant movement of the workforce toward remote work as well as the requirement for increased security measures (Sara).

Since the pandemic's beginning, workplaces have increased the use of remote and hybrid work arrangements, the volume of online commerce has increased significantly, and the number of telemedicine and telehealth services available has significantly increased. A growing number of medical facilities started providing patients with more telehealth options, such as video conferences between doctors and patients and medication delivery without personal interaction. In the year 2020, the United States had a 50% increase in the number of telehealth visits as compared to the previous decade's levels. In 2020, healthcare systems invested millions of dollars in virtual health platforms for virtual care, particularly for patients with chronic diseases, routine appointments, and ongoing care. (Sara). This new, rapidly growing trend of hybrid work necessitates the development of more complex and advanced cyber security solutions.

During the COVID-19 crisis, the usage of telemedicine has proven to be quite helpful in assisting a large number of patients. This is especially true given that traditional in-person appointments are becoming increasingly difficult. For instance, after the COVID-19 epidemic at

New York University, there was a 4330 % rise in nonurgent virtual visits. The risk posed by hackers who target Zoom meetings is high. Even though the Office for Civil Rights of the Department of Health and Human Services has relaxed enforcement of HIPAA's privacy rule during the COVID-19 pandemic, services such as Zoom do not currently offer end-to-end encryption, making it not truly Health Insurance Portability and Accountability Act (HIPAA)-compliant. This is the case even though end-to-end encryption is required for HIPAA compliance (Williams et al. 2).

More cyber security assaults have been launched against the healthcare industry than have been launched against the financial industry. The World Health Organization (WHO) reports that the number of cyberattacks that have been carried out has increased by a factor of five since the beginning of the COVID-19 epidemic. A similar phenomenon occurred in 2005 following Hurricane Katrina when thousands of phony websites sprouted up and solicited fake donations while also claiming to deliver false government aid. Cybercriminals frequently assume the identity of reputable and reliable institutions, such as the WHO, to prey on individuals' feelings of vulnerability during uncertain times, such as during a pandemic. Moreover, organizations that provide medical care become major targets when there is a public health emergency (Williams et al. 2).

The risk that the pandemic poses to the integrity of our digital systems is a significant one that must not be underestimated. Hackers are taking advantage of remote working and insecure networks to attack organizations and individuals alike due to the pandemic, which has led to a spike in the number of cases of cybercrime. The epidemic caused by the Covid-19 virus has presented information security professionals worldwide with an entirely new set of challenges. The danger of being targeted by a cyberattack multiplies rapidly as more people and companies

adopt the practice of working remotely. Because hackers are taking advantage of the heightened online activity that is occurring during this time to target vulnerable systems and networks, cyber security is currently more vital than ever.

The findings of this chapter shed light on the crucial part that higher education plays in bridging the skills gap in the cyber security sector in the United States. Despite the efforts that programs in higher education have made, the study's findings show that the United States is still susceptible and vulnerable to cybercrime. Higher education has helped offset the problem of labor shortage, but it has not been enough to eradicate or diminish the country's cyber risks. As the results of the data gathering and statistical analysis presented in this chapter illustrate, higher education played and still plays a crucial role in bridging the skills gap in the cyber security sector, but they could not address the country's cyber risks and diminish the country's vulnerability to cyberattacks.

In conclusion, the data provided talks about where the U.S. currently stands when meeting employer needs within the Cyber security industry today. It emphasizes how much further the country needs to go to ensure sufficient numbers of trained professionals ready and able to take up these roles. The government should highlight potential areas that could benefit from additional focus, such as education or training initiatives designed to help bridge the gap between what employers want to hire and what workers have to offer them moving forward into future years.

Conclusion

The concept of security has evolved from the traditional view of security as a matter of foreign policy to a more comprehensive view of national security that encompasses international and domestic issues. The traditional view of security-focused primarily on the defense of a nation's external borders and its relations with other nations. However, the current view of national security looks at the security of a nation from a more holistic perspective, taking into account its economic, social, political, and environmental well-being. This new view of security recognizes that a nation cannot be secure unless its citizens are secure and that internal threats, such as terrorism, poverty, and organized crime, can be just as devastating as external threats.

The new view of security has led to a shift in the focus of foreign policy and the development of new policy tools, such as cyber security, to address internal and external threats. The evolution of national security between 1940 and 1989, from a policy focused on isolationism to one that emphasized the need for international alliances, strong defense capabilities, and active engagement in global affairs. During this period, the U.S. government recognized the growing threat posed by the Soviet Union. It moved to expand its military capabilities and develop new strategies for countering the Soviet threat. The U.S. also began to build a network of alliances and international organizations to deter Soviet aggression and maintain peace and security in Europe and Asia. The U.S. also increased its involvement in international economic and political affairs, launching initiatives to provide economic and military aid to developing countries and to promote democracy and human rights.

National security is the concept of protecting the United States and its citizens from foreign and domestic threats. It encompasses various military, diplomatic, economic, and financial measures. The main goal of national security is to protect the United States national

interests, including its citizens, its allies, and its interests abroad. The American NSS is a document outlining the United States' strategic goals, objectives, and the means it will use to achieve them. The U.S. NSS seeks to ensure the safety and security of the American people, its homeland, and its interests around the world.

President Truman created the NSC in 1947 as part of the National Security Act of 1947. The NSC was created to assist and advise the president on national security matters. The CIA was also created as part of the National Security Act of 1947 and is charged with gathering and analyzing intelligence from around the world. In 1950, the NSC issued a document known as NSC-68, which outlined the U.S. objectives and programs for national security. It was an important document in the history of U.S. foreign policy, as it marked a shift away from the previous policy of neutrality towards a more proactive approach to containing the spread of communism.

President Eisenhower, John F. Kennedy, and Richard Nixon introduced various policies and reforms to the NSC. Eisenhower used the NSC meetings to make key foreign policy decisions. At the same time, Kennedy and Nixon both worked to strengthen the NSC's role in formulating and managing foreign policy. Additionally, Kennedy implemented the first formal set of NSC procedures, which set out the rules and procedures for the NSC's work. Nixon expanded the NSC's responsibilities to include intelligence, arms control, and crisis management.

President Reagan passed the Goldwater-Nichols Department of Defense Reorganization Act of 1986, which gave the Chairman of the Joint Chiefs of Staff more authority and expanded the role of the unified and specified combatant commanders. It also promoted the concept of jointness, which emphasized inter-service cooperation and teamwork. The Act also established

the position of the Joint Chiefs of Staff Vice Chairman. In addition, it established the Office of the Secretary of Defense and the Deputy Secretary of Defense. It expanded the role of the National Security Council. These measures were intended to improve the coordination of national security policy while preserving individual services' independence.

President George H. W. Bush and Bill Clinton both strongly focused on national security. Bush's policy focused on the Cold War, while Clinton's focused on global security, human rights, and economic stability. George W. Bush and Barack Obama significantly changed U.S. grand strategy in the 21st century. Under Bush, the U.S. shifted its focus away from traditional allies towards a policy of pre-emption, focusing on the "global war on terror" and the invasion of Iraq. Under Obama, the U.S. shifted its focus from pre-emption towards a multilateral engagement strategy, focusing on international cooperation and integration.

Cyber security poses a new and serious threat to American national security. Cyber-attacks can have consequences ranging from the theft of sensitive information to disruption of data to economic damage due to disrupted services or networks. Thus, the United States made steps to ensure that its networks, systems, and data remain secure. It can include developing robust cyber defense measures, enacting legislation to protect critical infrastructure, and investing in research and development to stay ahead of emerging threats. Additionally, the U.S. continued cooperating with other countries to identify and combat cyber-attacks and ensure the effectiveness of cyber defense measures.

The amalgamation between federal agencies and higher education institutions in promoting cyber security programs is a powerful tool for protecting the nation's digital infrastructure. Through collaborative efforts, these agencies can provide resources to universities that will enable them to develop innovative approaches and best practices for safeguarding data

networks. The NSF has been particularly active in this regard, providing grants to universities across the country so they can create specialized curriculums focused on cyber security topics. Additionally, theDHS, through its CAE Program, provides funds and technical assistance to support academic research into various aspects of computer science-related fields, such as network engineering or software development, with an emphasis on cyber security applications. Finally, by collaborating through initiatives like these, federal organizations can leverage their collective expertise towards creating a more secure cyberspace environment overall.

The NICE, the NIST, and CAE are three key programs that promote and expand American cyber security. NICE focuses on developing a cyber security workforce, while NIST provides technical guidance to help organizations implement effective cyber security practices. The CAE program recognizes academic institutions that meet rigorous standards for producing highly qualified graduates with expertise in information assurance or related disciplines. These three programs work together to create a strong foundation for protecting the nation's digital infrastructure from malicious attacks by providing knowledge, resources, training opportunities, recognition awards, and scholarships to those who pursue careers in this field.

The U.S. government is taking a proactive approach to building a strong national cyber security workforce by investing in resources and initiatives that will help develop the skills of current and future employees. Through its NICE, the federal government provides training, scholarships, internships, and other opportunities to students interested in entering this field as well as established professionals who want to upgrade their existing cyber security expertise. Additionally, organizations such as the DHS's and the SFS program provide financial support for qualified individuals seeking advanced degrees related to information assurance or cyber security topics, while also providing funding for research projects aimed at improving public sector cyber

security capabilities across multiple areas including energy infrastructure protection and resilience. These investments are essential not only so that U.S. can remain secure from malicious actors. Also, can continue developing cutting-edge technology solutions designed with safety in mind from inception through deployment into production environments.

It is clear that relying on the analysis of statistical data has helped enhance the importance of this research. Cyber threats and the training of a professional workforce can significantly impact the security of organizations. By utilizing statistical data, organizations can gain insight into the current state of their security systems and identify areas of weakness or potential threats. Additionally, training a professional personnel in cyber security can help to ensure that all employees understand the importance of security protocols, and are aware of the potential risks associated with cyber threats. This can help reduce the chances of an attack or data breach. Finally, the rapid rise of cyber threats led to an emergency application of specialized educational programs to ensure that organizations stay abreast of the latest developments in the security field, allowing them to stay one step ahead of malicious actors.

The findings of the study indicate that higher education has played a significant role in mitigating the shortage of skilled workers in the field of cyber security. The research revealed that higher education programs helped to minimize the threat of workforce shortage. However, despite these efforts, the U.S. remains vulnerable to cybercrimes. The results of the analysis show that while higher education programs have made a significant contribution to addressing the workforce shortage issue, they have not been able to fully eliminate or reduce the country’s vulnerabilities to cybercrimes.

Based on the findings of the research, several areas for further study can be suggested to further explore the relationship between higher education and the U.S. cyber security workforce and vulnerabilities to cybercrimes:

- Assessment of the effectiveness of specific higher education programs in preparing students for careers in cybersecurity. This could include an analysis of curriculum design, student outcomes, and the job market demand for graduates of these programs.
- Examination of the relationship between the shortage of skilled workers in cybersecurity and the increasing frequency and sophistication of cybercrimes. This could include an analysis of the factors that contribute to the shortage of skilled workers and the ways in which this shortage contributes to the increasing risk of cyber-attacks.
- Investigation of alternative approaches to addressing the shortage of skilled workers and reducing vulnerabilities to cybercrimes. This could involve exploring new and innovative solutions, such as online learning platforms, certification programs, and public-private partnerships.

These areas for further research have the potential to provide a more comprehensive understanding of the role of higher education in addressing the challenges faced by the U.S. in cyber security and could lead to the development of more effective solutions to change it.

Work Cited

"ABET Accredits 54 Additional Programs in 2021, Including First Associate Cybersecurity Programs."*Abet.org*, https://www.abet.org/abet-accredits-54-new-programs-in-2021-including-first-associate-cybersecurity-programs/. Accessed 13 Oct. 2021.

"Career Opportunities in Cybersecurity." *Penn State Greater Allegheny*, https://greaterallegheny.psu.edu/academics/cybersecurity/career. Accessed 11 Oct. 2022.

"CyberCorps(R) Scholarship for Service (SFS) (Nsf21580)."*Nsf.gov*, http://www.nsf.gov/pubs/2021/nsf21580/nsf21580.htm.

"H.R. 5005 (107th): Homeland Security Act of 2002."*GovTrack.Us*, 2002, https://www.govtrack.us/congress/bills/107/hr5005.

"National Security Act of 1947." *Pub. L. No. 235, 61 Stat. 495*, 26 July 1947, https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.

"The Comprehensive National Cybersecurity Initiative."*The White House*, 2008, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

"Written Testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Intelligence Hearing Titled "Russian Interference in the 2016 U.S. Elections."*Dhs.gov*, 21 June 2017, https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting.

Albright, Madeleine K. *Interview on NBC-TV "The Today Show" with Matt Lauer*. Office of the Spokesman, 19 Feb. 1998, https://1997-2001.state.gov/statements/1998/980219a.html.

Alsmadi, Izzat. "Cybersecurity Education Based on the NICE Framework: Issues and Challenges."*ISACA Journal*, vol. 3, 2018, pp. 1–6, https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/cybersecurity-education-based-on-the-nice-framework-issues-and-challenges.

Annabi, Hala, and Sarah Lebovitz. "Improving the Retention of Women in the IT Workforce: An Investigation of Gender Diversity Interventions in the USA."*Information Systems Journal*, vol. 28, no. 6, 2018, pp. 1049–1081, https://doi.org10.1111/isj.12182.

Bartolotto, John K. *The Origin and Development Process of the National Security Strategy*. 3 May 2004, https://apps.dtic.mil/sti/pdfs/ADA423358.pdf.

Best, Richard A., Jr. *The National Security Council: An Organizational Assessment*. Congressional Research Service, 2009, https://apps.dtic.mil/sti/pdfs/ADA501333.pdf.

Beveridge, Robert. "Addressing the Gender Gap in the Cybersecurity Workforce."*International Journal of Cyber Research and Education*, vol. 3, no. 2, 2021, pp. 54–61, https://doi.org10.4018/ijcre.2021070105.

Bostdorff, Denise M. "The Evolution of a Diplomatic Surprise: Richard M. Nixon's Rhetoric on China, 1952-July 15, 1971."*Rhetoric and Public Affairs*, vol. 5, no. 1, 2002, pp. 31–56, https://doi.org10.1353/rap.2002.0005. Accessed 11 Oct. 2022.

Brailey, Malcolm. "Pre-Emption and Prevention : An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force in Defence of the State."*Institute of Strategic Studies Singapore*, 2003.

Brown, H. "The Proceedings against Richard M. Nixon."*High Crimes and Misdemeanors in Presidential Impeachment*, 1st ed., Palgrave Macmillan, 2010, https://doi.org10.1057/9780230102255.

Brown, Harold. *Thinking about National Security: Defense and Foreign Policy in A Dangerous World*. Westview Press, 1983.

Burns, Nicholas, and Jonathon Price, editors. *Securing Cyberspace: A New Domain for National Security*. Aspen Institute for Humanistic Studies, 2012.

Bush, George W. "Remarks on the Future of Iraq."*Selected Speeches of President George W. Bush*, 2001 – 2008, https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.

---. "The National Strategy to Secure Cyberspace, February 2003."*General Security*, no. 73, 2003.

---. "The Second Inaugural Address."*Selected Speeches of President George W. Bush*, 2001 – 2008, https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.

---. "West Point Commencement."*Selected Speeches of President George W. Bush*, 2001 – 2008, https://georgewbush-

whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.

---. *Selected Speeches of President George W. Bush*. 2001 – 2008, https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.

---. *The National Security Strategy of the United States of America*. The White House, Sept. 2002.

Bush, Vannevar. *Science: The Endless Frontier*. National Science Foundation, 1945.

Butler, Timothy A., and Air War College Maxwell AFB United States. *Prevention, Preemption, and the Bush Doctrine*. 2012, https://apps.dtic.mil/sti/citations/AD1018121.

Catota, Frankie E., et al. "Cybersecurity Education in a Developing Nation: The Ecuadorian Environment."*Journal of Cybersecurity*, vol. 5, no. 1, 2019, https://doi.org10.1093/cybsec/tyz001.

Centers of Academic Excellence in Cyber Defense Publication. *Celebrating 20 Years with the Centers of Academic Excellence in Cyber Defense*. Department of Homeland Security and National Security Agency, 2019, https://www.caecommunity.org/sites/default/files/CAE_Book_Version_1.6-2.pdf.

Chozick, Amy. "Hillary Clinton Accuses Russia of Interfering with U.S. Election."*The New York Times*, The New York Times, 6 Sept. 2016, https://www.nytimes.com/2016/09/06/us/politics/hillary-clinton-russia.html.

Clinton, Hillary Rodham. "Foreign Policy Address at the Council on Foreign Relations."*U.S. Department of State*, July 2009, https://2009-2017.state.gov/secretary/20092013clinton/rm/2009a/july/126071.htm. Accessed 28 Apr. 2020.

---. "Transcript of Hillary Clinton's Confirmation Hearing."

Crumpler, William, and James A. Lewis. *The Cybersecurity Workforce Gap*. Jan. 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

CSIS Commission on Smart Power, et al. *CSIS Commission on Smart Power: A Smarter, More Secure America*. CSIS, 2007.

Curtis, Paul A., and Lee Colwell. *Cyber Crime: The next Challenge an Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond*. School Of Law Enforcement Supervision, 12 Nov. 2000.

Cuvelier, Gilles, editor. *Department of Homeland Security Science & Technology Directorate: Mission & Issues*. Nova Science, 2013.

Dalby, Simon. "American Security Discourse: The Persistence of Geopolitics."*Political Geography Quarterly*, vol. 9, no. 2, 1990, pp. 171–188, https://doi.org10.1016/0260-9827(90)90017-5.

---. *Geopolitics, Grand Strategy and the Bush Doctrine*. Institute of Defence and Strategic Studies, Jan. 2005, pp. 1–20.

Davis, Darren W., and Brian D. Silver. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America."*American Journal of Political Science*, vol. 48, no. 1, 2004, p. 28, https://doi.org10.2307/1519895.

Dawson, Maurice, et al. "The Role of CAE-CDE in Cybersecurity Education for Workforce Development."*Information Technology - New Generations*, Springer International Publishing, 2018, pp. 127–132.

Defeng, Yang. "Power Supply Safety Management of High-Risk Customers of Regional Grid."*IOP Conference Series. Earth and Environmental Science*, vol. 827, no. 1, 2021, p. 012025, https://doi.org10.1088/1755-1315/827/1/012025.

Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press, 2011, https://muse.jhu.edu/book/2643.

Department of Homeland Security. *Quadrennial Homeland Security Review Report. A Strategic Framework for a Secure Homeland*. Feb. 2010, https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf.

Dimitrova, Anna. "Obama's Foreign Policy: Between Pragmatic Realism and Smart Diplomacy."*Institute for Cultural Diplomacy: Cultural Diplomacy Research*, 2011.

Dodaro, G. L. *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*. United States Accountability Office, 2018.

Donnelly, Thomas, and Colin Monaghan. *Legacy Agenda, Part II: The Bush Doctrine and the Long War*. American Enterprise Institute, 2007, http://www.jstor.org/stable/resrep02990. Accessed 27 Apr. 2020.

Drew, Dennis M. *Making Twenty-First-Century Strategy: An Introduction to Modern National Security Processes and Problems*. Air University Press, 2007.

Dueck, Colin. "Ideas and Alternatives in American Grand Strategy, 2000–2004."*Review of International Studies*, vol. 30, no. 4, 2004, pp. 511–535, https://doi.org10.1017/s0260210504006205. Accessed 3 Apr. 2020.

Evans, Karen, and Franklin Reeder. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. CSIS, 2010.

Executive Office of the President of The U.S. *The Comprehensive National Cybersecurity Initiative*. 2010, https://apps.dtic.mil/sti/pdfs/ADA517364.pdf.

Falk, Stanley L. "The National Security Council under Truman, Eisenhower, and Kennedy."*Political Science Quarterly*, vol. 79, no. 3, 1964, p. 403, https://doi.org10.2307/2145907. Accessed 3 Apr. 2020.

Fichtenkamm, Maik, et al. "Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made." *ISACA JOURNAL*, vol. 2, no. 2022, Apr. 2022, pp. 1–10, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world.

Fidler, David P. "International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace."*ASIL Insights*, vol. 15, no. 15, June 2011.

Furnell, Steven, et al. "Pandemic Parallels: What Can Cybersecurity Learn from COVID-19?"*Computer*, vol. 54, no. 3, 2021, pp. 68–72, https://doi.org10.1109/mc.2020.3046888.

Gaddis, John Lewis. "Containment: Its Past and Future."*International Security*, vol. 5, no. 4, 1981, p. 74, https://doi.org10.2307/2538714.

---. *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War*. Oxford University Press, 2005.

Galante, Laura. "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents."*Atlantic Council*, 2018.

Gelb, Leslie H. "The Elusive Obama Doctrine."*The National Interest*, no. 121, 2012, pp. 18–28, http://www.jstor.org/stable/42896546.

Gerges, Fawaz A. "The Obama Approach to the Middle East: The End of America's Moment?"*International Affairs*, vol. 89, no. 2, 2013, pp. 299–323, https://doi.org10.1111/1468-2346.12019.

Glaser, John, and A. Trevor Thrall. “Obama’s Foreign Policy Legacy and the Myth of Retrenchment.”*SSRN Electronic Journal*, Cato Institute, 2017, https://doi.org10.2139/ssrn.2979450. Accessed 27 Apr. 2020.

Goh, Evelyn. “Nixon, Kissinger, and the ‘Soviet Card’ in the U.s. Opening to China, 1971-1974.”*Diplomatic History*, vol. 29, no. 3, 2005, pp. 475–502, https://doi.org10.1111/j.1467-7709.2005.00500.x.

Goldberg, Jeffrey. “The Obama Doctrine.”*The Best American Magazine Writing 2017*, edited by Sid Holt and The American Society of Magazine Editors, Columbia University Press, 2017, pp. 243–302.

Gompert, David C., et al. *Blinders, Blunders, and Wars: What America and China Can Learn*. RAND, 2014.

Gormley, Ken. *The Presidents and the Constitution: A Living History*. New York University Press, 2016, 2016, http://www.jstor.org/stable/j.ctt1803zfw. Accessed 11 Oct. 2022.

Greenstein, Fred I. *The Presidential Difference: Leadership Style from FDR to Barack Obama - Third Edition*. Princeton University Press, 2012, https://doi.org10.2307/j.ctvcm4h5n. Accessed 11 Oct. 2022.

Harris, Laurie A. *The National Science Foundation: An Overview*. Congressional Research Service, 9 Apr. 2021, https://crsreports.congress.gov/product/pdf/R/R46753.

Hastedt, Glenn. “Reconnaissance Satellites, Intelligence, and National Security.”*Societal Impact of Spaceflight*, edited by Roger D. Launius Steven. J Dick, NASA History Series Publications, 2007, pp. 369–383.

Heaps, Jennifer Davis. “Tracking Intelligence Information: The Office of Strategic Services.”*The American Archivist*, vol. 61, no. 2, 1998, pp. 287–308, https://doi.org10.17723/aarc.61.2.fj0j77432841j855.

Heatherly, Christopher J., and Ian Melendez. “Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army.”*The Cyber Defense Review*, vol. 4, no. 1, 2019, pp. 63–74, https://www.jstor.org/stable/26623067.

Hemmer, Christopher. *American Pendulum: Recurring Debates in U.s. Grand Strategy*. 1st ed., Cornell University Press, 2015.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.”*Journal of Strategic Security*, vol. 4, no. 2, 2011, pp. 49–60, https://doi.org10.5038/1944-0472.4.2.3. Accessed Oct 12, 2022.

Huntington, Samuel P. *The Third Wave: Democratization in the Late Twentieth Century*. University of Oklahoma Press, 1993.

Hylton, Sara, et al. “What the Long-Term Impacts of the COVID-19 Pandemic Could Mean for the Future of IT Jobs.” *Beyond the Numbers: Employment & Unemployment*, vol. 11, no. 3, Feb. 2022, https://www.bls.gov/opub/btn/volume-11/what-the-long-term-impacts-of-the-covid-19-pandemic-could-mean-for-the-future-of-it-jobs.htm.

Jablonsky, David. “The State of the National Security State.”*Parameters: Journal of the US Army War College*, vol. 32, no. 4, 2002, https://doi.org10.55540/0031-1723.2122.

Jervis, Robert. “Understanding the Bush Doctrine.”*Political Science Quarterly*, vol. 118, no. 3, 2003, pp. 365–388, https://doi.org10.1002/j.1538-165x.2003.tb00398.x. Accessed 27 Apr. 2020.

John, Anthony Wanis-St. “The National Security Council: Tool of Presidential Crisis Management.”*Journal of Public and International Affairs*, vol. 9, no. 1, 1998, pp. 102–127.

Jordan, Amos A., et al. *American National Security*. 6th ed., Johns Hopkins University Press, 2009, https://doi.org10.1353/book.26472.

Kahina, Goudjil. “The Conceptualization of Freedom in U.S. Politics: A Normative Strategy to Preserve Global Liberal Values.”*Fiat Iustitia*, vol. 12, no. 2, 2018, pp. 96–112, http://fiatiustitia.ro/wp-content/uploads/2021/03/380-Article-Text-738-1-10-20190404.pdf.

Kahn, Robert E., et al. “America’s Cyber Future: Security and Prosperity in the Information Age.”*Center for a New American Security*, edited by Kristin Lord and Travis Sharp, vol. 11, June 2011.

Katulis, Brian. *Democracy Promotion in the Middle East and the Obama Administration*. Century Foundation, 2009.

Kiltz, Linda. “The Challenges of Developing a Homeland Security Discipline to Meet Future Threats to the Homeland.”*Journal of Homeland Security and Emergency Management*, vol. 8, no. 2, 2011, https://doi.org10.2202/1547-7355.1899.

Kimball, Jeffrey. “The Nixon Doctrine: A Saga of Misunderstanding.”*Presidential Studies Quarterly*, vol. 36, no. 1, 2006, pp. 59–74, https://doi.org10.1111/j.1741-5705.2006.00287.x. Accessed 11 Oct. 2022.

Kohnke, Anne. “A Holistic Approach to Cybersecurity: Mapping the NICE Workforce Framework to the Critical Infrastructure Cybersecurity Framework.”*Journal of The Colloquium for Information Systems Security Education*, vol. 4, no. 1, 2016, https://cisse.info/journal/index.php/cisse/article/view/44.

Korb, Larry. *US Strategies for National Security: Winning the Peace in the 21st Century, A Task Force Report of the Strategies for US National Security Program*. Edited by Michael Kraig, Stanley Foundation, Oct. 2003.

Kshetri, Nir. “The Lack of Women in Cybersecurity Leaves the Online World at Greater Risk.”*The Conversation*, May 2020, http://theconversation.com/the-lack-of-women-in-cybersecurity-leaves-the-online-world-at-greater-risk-136654.

Leffler, Melvyn p. “9/11 and American Foreign Policy.”*Diplomatic History*, vol. 29, no. 3, 2005, pp. 395–413, https://doi.org10.1111/j.1467-7709.2005.00491.x.

---.“9/11 in Retrospect: George W. Bush’s Grand Strategy, Reconsidered.”*Foreign Affairs (Council on Foreign Relations)*, vol. 90, no. 5, 2011, pp. 33–44, http://www.jstor.org/stable/23041774. Accessed 27 Apr. 2020.

Levy, Jack S. “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis.”*International Studies Quarterly: A Publication of the International Studies Association*, vol. 28, no. 2, 1984, p. 219, https://doi.org10.2307/2600696. Accessed 6 Oct. 2022.

Libicki, Martin C., et al. “Findings from Interviews and Statistics.”*Hackers Wanted: An Examination of the Cybersecurity Labor Market*, RAND Corporation, 2014, pp. 29–40, http://www.jstor.org/stable/10.7249/j.ctt7zvzmj.11.

Little, Douglas. *Us versus Them, Second Edition: The United States, Radical Islam, and the Rise of the Green Threat*. UNC Press Books, 2022.

Marshall, George C. “THE MARSHALL PLAN SPEECH.”*The George C. Marshall Foundation*, 2 Dec. 2021, https://www.marshallfoundation.org/the-marshall-plan/speech/. Accessed 14 Mar. 2019.

Masters, Jonathan. “Russia, Trump, and the 2016 U.S. Election.”*Council on Foreign Relations*, 26 Feb. 2018, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election. Accessed Oct 12, 2022.

McKenzie, Timothy M. “What Is a Cyber Attack?”*Is Cyber Deterrence Possible?*, Air University Press, 2017, pp. 3–5, http://www.jstor.org/stable/resrep13817.7. Accessed Oct 12, 2022.

Mueller, Karl P., et al. *Striking First: Preemptive and Preventive Attack in U.s. National Security Policy*. RAND Corporation, 2006.

Nakashima, Ellen. “Cyber Researchers Confirm Russian Government Hack of Democratic National Committee.”*Washington Post (Washington, D.C.: 1974)*, The Washington Post, 20 June 2016, https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html. Accessed Oct 12, 2022.

Nanto, Dick K. *Economics and National Security*: Issues and Implications for U.S. Policy*. Library of Congress. Congressional Research Service, 4 Jan. 2011, https://sgp.fas.org/crs/natsec/R41589.pdf.

Nat’L Defense Univ Foundation. *Cyberpower and National Security*. Edited by Franklin D. Kramer and Stuart H. Starr, University of Nebraska Press, 2011, muse.jhu.edu/book/47431.

Nelson, Anna Kasten. “THE EVOLUTION OF THE NATIONAL SECURITY STATE: UBIQUITOUS AND ENDLESS.”*The Long War: A New History of U.S. National Security Policy Since World War II*, edited by Andrew J. Bacevich, Columbia University Press, 2007, pp. 265–301.

Ninkovich, Frank. “Ideology, the Open Door, and Foreign Policy.”*Diplomatic History*, vol. 6, no. 2, 1982, pp. 185–208, https://doi.org10.1111/j.1467-7709.1982.tb00371.x.

---. “Ideology, the Open Door, and Foreign Policy.”*Diplomatic History*, vol. 6, no. 4, 1982, pp. 185–208, https://doi.org10.1111/j.1467-7709.1982.tb00798.x.

Nixon, Richard. “Address to the Nation Announcing Decision to Resign the Office of President of the United States.”*Ucsb.edu*, 8 Aug. 1974, https://www.presidency.ucsb.edu/documents/address-the-nation-announcing-decision-resign-the-office-president-the-united-states.

---. “Address to the Nation on the Situation in Southeast Asia.”*Ucsb.edu*, 30 Apr. 1970, https://www.presidency.ucsb.edu/documents/address-the-nation-the-situation-southeast-asia-1.

Nye, Joseph S., Jr. “Public Diplomacy and Soft Power.”*The Annals of the American Academy of Political and Social Science*, vol. 616, no. 1, 2008, pp. 94–109, https://doi.org10.1177/0002716207311699.

---.*The Future of Power.* Public Affairs, 2011.

Obama, Barack. “A New Beginning: Speech at Cairo University.” 4 June 2009, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Cairo%20University.pdf.

---. “Address to the Nation on Libya.” National Defense University, 28 Mar. 2011, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Libya%20Nation%20Speech.pdf.

---. “Address to the People of Cuba.” Gran Teatro de la Habana, 22 Mar. 2016, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Cuba%20People%20Speech.pdf.

---. “Nobel Prize for Peace.” 10 Dec. 2009, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Nobel%20Lecture.pdf.

---. “On American Diplomacy in the Middle East and North Africa.” State Department, 19 May 2011, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Middle%20East%20Diplomacy.pdf.

---. “Speech at West Point on Troop Increase in Afghanistan.” Eisenhower Hall, West Point Military Academy, 1 Dec. 2009, americanrhetoric.com/speeches/PDFFiles/Barack%20Obama%20-%20Afghanistan%20War%20Troop%20Surge.pdf.

Offner, Arnold A. “LIBERATION OR DOMINANCE? THE IDEOLOGY OF U.S. NATIONAL SECURITY POLICY.”*The Long War: A New History of U.S. National Security Policy Since World War II*, edited by Andrew J. Bacevich, Columbia University Press, 2007, pp. 1–52.

Patman, Robert G. “Globalization, The End of The Cold War, and The Doctrine of National Security.”*Globalization and Conflict National Security in a “New” Strategic Era*, edited by Robert G. Patman, Routledge, 2006, p. 27, https://doi.org10.4324/9780203007938.

Payne, Angela R., et al. “The Marshall Plan - Global Strategy and Foreign Humanitarian Aid.”*Globalization - Approaches to Diversity*, InTech, 2012.

Perlroth, Nicole, and Clifford Krauss. “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.”*The New York Times*, The New York Times, 15 Mar. 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

Petersen, Rodney, et al. *Workforce Framework for Cybersecurity (NICE Framework)*. National Institute of Standards and Technology, 2020, https://doi.org10.6028/nist.sp.800-181r1.

Platt, Tony, and Cecilia O’Leary. “Patriot Acts.”*Social Justice (San Francisco, Calif.)*, vol. 30, no. 1 (91), 2003, pp. 5–21, http://www.jstor.org/stable/29768164. Accessed 27 Apr. 2020.

Pool, Phillip. “War of the Cyber World: The Law of Cyber Warfare.”*The International Lawyer*, vol. 47, no. 2, 2013, p. 299, https://scholar.smu.edu/til/vol47/iss2/9?utm_source=scholar.smu.edu%2Ftil%2Fvol47%2Fiss2%2F9&utm_medium=PDF&utm_campaign=PDFCoverPages.

Poster, Winifred R. “Cybersecurity Needs Women.”*Nature*, vol. 555, no. 7698, 2018, pp. 577–580, https://doi.org10.1038/d41586-018-03327-w.

Prebil, Michael. “Teach Cybersecurity with Apprenticeship Instead.” *New America*, 14 Apr. 2017, https://www.newamerica.org/education-policy/edcentral/teach-cyber-apprenticeship-instead/.

Priest, Dana, et al. “U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections.”*The Washington Post*, 5 Sept. 2016.

Quinn, Adam. *US Foreign Policy in Context: National Ideology from the Founders to the Bush Doctrine*. Routledge, 2009.

Quinn, Malcolm, editor. *Goldwater-Nichols Department of Defense Reorganization Act: Reforms & Considerations*. Nova Science, 2016.

R., Angela, and Bharat S. “The Marshall Plan - Global Strategy and Foreign Humanitarian Aid.”*Globalization - Approaches to Diversity*, edited by Hector Cuadra-Montiel, InTech, 2012.

Reichard, Gary W. “The Domestic Politics of National Security.”*The National Security Its Theory and Practice, 1945-1960*, edited by Norman A. Graebner, Oxford University Press, 1986, pp. 243–273.

Reilly, Thomas P. *The National Security Strategy of the United States: Development of Grand Strategy*. 3 May 2004, https://apps.dtic.mil/sti/pdfs/ADA424247.pdf.

Rice, Condoleezza. “Dr. Condoleezza Rice Discusses President’s National Security Strategy.”*Georgewbush-whitehouse.archives.gov,* Office of the Press Secretary, 1 Oct. 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/10/20021001-6.html.

---. “The Road Map to Peace.”*Georgewbush-whitehouse.archives.gov,* Office of the Press Secretary, 12 June 2003, https://georgewbush-whitehouse.archives.gov/news/releases/2003/06/20030612-12.html. Accessed Apr 28,2020.

S. Nelson Drew, Paul H. Nitze. *NSC-68: FORGING THE STRATEGY OF CONTAINMENT*. Diane Publishing, 1994.

Sarkesian, Sam C., et al. *US National Security: Policymakers, Processes and Politics*. 5th ed, Lynne Rienner, 2013.

Satterthwaite, Joseph C. “The Truman Doctrine: Turkey.”*The Annals of the American Academy of Political and Social Science*, vol. 401, Sage Publications, Inc., May 1972, pp. 74–84, https://doi.org10.1177/000271627240100109.

Schmitt, Michael N., editor. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013, https://doi.org10.1017/cbo9781139169288.

Science and Technology Directorate. *Metrics Used to Make DHS Center of Excellence Awards*. Department of Homeland Security, 2015, https://www.hsdl.org/c/view?docid=817757.

Spidalieri, Francesca, and Jennifer McArdle. “Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in US Service Academies.”*The Cyber Defense Review*, vol. 1, no. 1, 2016, pp. 141–164, http://www.jstor.org/stable/26267304.

Spidalieri, Francesca. *Joint Professional Military Education Institutions in an Age of Cyber Threat*. Pell Center for International Relations and Public Policy at Salve Regina

University, 7 Aug. 2013, https://www.pellcenter.org/wp-content/uploads/2015/05/Joint-Professional-Military-Education-Institutions-in-an-Age-of-Cyber-Threat.pdf.

Suri, Jeremi. "Liberal Internationalism, Law, and the First African American President."*The Presidency of Barack Obama: A First Historical Assessment*, edited by Julian E. Zelizer, Princeton University Press, 2018, pp. 195–211. Accessed 27 Apr. 2020.

Tarzi, Shah M. "The Folly of a Grand Strategy of Coercive Global Primacy: A Fresh Perspective on the Post-9/11 Bush Doctrine."*International Journal on World Peace*, vol. 31, no. 3, 2014, pp. 27–52, http://www.jstor.org/stable/24543747.

The White House. "The Comprehensive National Cybersecurity Initiative."*The White House*, 2008, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

---. *A National Security Strategy of Engagement and Enlargement*. 1994, https://history.defense.gov/Portals/70/Documents/nss/nss1994.pdf?ver=YPdbuschbfpPz3tyQQxaLg%3d%3d.

---. *A National Security Strategy of Engagement and Enlargement*. 1995, https://history.defense.gov/Portals/70/Documents/nss/nss1995.pdf?ver=pzgo9pkDsWmIQqTYTC6O-Q%3d%3d.

---. *A National Security Strategy of Engagement and Enlargement*. 1996, https://history.defense.gov/Portals/70/Documents/nss/nss1996.pdf?ver=4f8riCrLnHIA-H0itYUp6A%3d%3d.

---. *A National Security Strategy of Engagement and Enlargement*. 1987, https://history.defense.gov/Portals/70/Documents/nss/nss1987.pdf?ver=FUZbPLy3ZDfa4UTDpMkNzw%3d%3d.

---. *A National Security Strategy of Engagement and Enlargement*. 1988, https://history.defense.gov/Portals/70/Documents/nss/nss1988.pdf?ver=uXpmo-mT0TKzq2Ut6PmfjA%3d%3d.

---. *A National Security Strategy of Engagement and Enlargement*. 2002, https://history.defense.gov/Portals/70/Documents/nss/nss2002.pdf?ver=oyVN99aEnrAWijAc_O5eiQ%3d%3d.

Tikk-Ringas, Eneken, et al. "Cyber Security as a Field of Military Education and Study."*Joint Force Quarterly 75*, vol. 4, Sept. 2014, pp. 57–60.

Truman, Harry S. “President Harry S. Truman’s Address Before A Joint Session Of Congress, March 12, 1947.”*Yale.edu*, 1947, https://avalon.law.yale.edu/20th_century/trudoc.asp. Accessed 2 Apr. 2020.

U. S Government Publishing Office GPO. “The Central Intelligence Agency.”*Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, Executive Agency Publications, 1996, pp. 61–70, https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-10.pdf.

U. S. Senate. *Report of the Select Committee of Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election*. 2020.

U.S. Department of Commerce, U.S. Department of Homeland Security. *Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. 10 May 2019.

United Nations: Office on Drugs and Crime. “Cybercrime.”*The Globalisation of Crime: A Transnational Organized Crime Threat Assessment*, United Nations, 2010, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf. Accessed Oct 12, 2022.

United States Objectives and Programs for NS. *A Report to the National Security Council - NSC 68*. 14 Apr. 1950, https://www.trumanlibrary.gov/library/research-files/report-national-security-council-nsc-68?documentid=NA&pagenumber=1. Accessed Sep. 2021.

van der Meer, Sico. *Foreign Policy Responses to International Cyber-Attacks: Some Lessons Learned*. Clingendael Institute, 2015, http://www.jstor.org/stable/resrep05303. Accessed Oct 12, 2022.

Visner, Samuel. “Cyber Security’s Next Agenda.”*Georgetown Journal of International Affairs*, 2013, pp. 89–99, http://www.jstor.org/stable/43134325.

Watson, Cynthia A. *U.S. National Security: A Reference Handbook, 2nd Edition*. 2nd ed., ABC-CLIO, 2008.

Weiner, Tim. *Legacy of Ashes: The History of the CIA*. Anchor Books, 2008.

Williams, Christina Meilee, et al. “Cybersecurity Risks in a Pandemic.” *Journal of Medical Internet Research*, vol. 22, no. 9, 2020, p. e23692, https://doi.org10.2196/23692.

Wilshusen, Gregory C. *Cybersecurity Workforce: DHS Needs to Take Urgent Action to Identify Its Position and Critical Skill Requirements*. United States Government Accountability Office, 7 Mar. 2018.

Xydis, Stephen G. "The Truman Doctrine in Perspective."*Balkan Studies*, vol. 8, no. 2, 1967, pp. 239–262, https://ojs.lib.uom.gr/index.php/BalkanStudies/article/view/1066. Accessed 30 Jul. 2018.

Yannakogeorgos, Panayotis A. "Cyberspace, the New Frontier — and the Same Old Multilateralism."*Global Norms, American Sponsorship and the Emerging Patterns of World Politics*, Palgrave Macmillan UK, 2010, pp. 147–177, https://doi.org10.1057/9780230289611_5.

Yergin, Daniel. *Shattered Peace: The Origins of the Cold War and the National Security State*. Boston: Houghton Mifflin, 1977.

Zaharna, R. S. "Obama, U.s. Public Diplomacy and the Islamic World."*World Politics Review*, 16 Mar. 2009, https://www.worldpoliticsreview.com/obama-u-s-public-diplomacy-and-the-islamic-world/.

Zimmerman, Roberta, editor. *Department of Homeland Security: Assessment, Recommendations & Appropriations*. Nova Science, 2015.