People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Larbi Tebessi University-Tebessa-

Faculty of Letters and Languages

Department of Letters and English Language

The title

Manifestations of Cybersecurity in the American Foreign Policy -Biden's Administration

A Dissertation Submitted to the Department of Letters and English Language in Partial Fulfilment of the Requirements for the Degree of Master in Literature and Civilisation

Candidate:	**Supervisor:**
SAIDANE Younes	**Mrs.Goudjil Kahina**

Board of Examiners:

President: Ms.BOUAZIZ Amina	**MAA ,Larbi Tebessi University-Tebessa**
Supervisor: Mrs.Goudjil Kahina	**MAA ,Larbi Tebessi University-Tebessa**
Examiner: Mrs.BRAHMI Halima	**MAA ,Larbi Tebessi University-Tebessa**

2021 /2022

Dedication

First and foremost, the highest gratitude goes to Allah.

This dissertation is dedicated to my father, my mother and my wife. Without my mother's supplications and the constant support of my wife, this dissertation would not have been accomplished.

Acknowledgement

Many thanks go to the jury members for having led the supervision of this master's dissertation. A great deal of gratitude goes particularly to Mrs Kahina Goudjil for guiding the researcher for what best fits this study. I also would like to express my deepest gratitude to the head of the department and my teachers for their sustained encouragement.

Abstract

The United States, in its quest for world supremacy, went through military challenges as part of its foreign policy. Thus, in many worldwide conflicts, the US had a hand in them as the objective was to protect its national security. This explains why all sorts of interventions were military. With the introduction of the internet, the world has become digitally interconnected. Therefore, physical world relations have their equivalent in cyberspace with a certain complexity where geographical borders are replaced with virtual ones and can be easily crossed. Thus, the US officials sought the need to use the cyberspace as an extension to their foreign policy as part of what is known as the soft power. They argued that the cyberspace is absorbing the world 's culture. Consequently, the US political weight should be thoroughly exercised as many rivalling powers continue to threaten the US national security. For the US, cyberspace security is never a safe channel; thus, securing this digital gate means maintaining world supremacy.

Keywords:

Cyberspace, Soft Power, United States of America. Foreign Policy, International Relations, National security

Résumé

Les États-Unis, en quête de la suprématie mondiale, ont dû relever des défis militaires dans le cadre de leur politique étrangère. Ainsi, de nombreux conflits dans le monde entier, les États-Unis avaient une main dans eux comme l'objectif est de protéger la sécurité nationale. Cela explique pourquoi toutes sortes d'interventions étaient militaires. Avec l'introduction d'Internet, le monde est devenu uni numériquement, ou connecté. Par conséquent, les relations physiques du monde ont leur équivalent dans le cyberespace qui sont complexes. Une telle complexité réside dans le fait que les frontières sont virtuelles et peuvent être facilement franchies. Ainsi, les responsables américains ont cherché à utiliser le cyberespace comme une extension de leur politique étrangère dans le cadre de ce qu'on appelle le soft power. Ils ont fait valoir que le cyberespace absorbe la culture mondiale. Par conséquent, le poids politique des États-Unis devrait être exercé avec rigueur, car de nombreuses puissances rivales continuent de menacer la sécurité nationale des États-Unis. Pour les États-Unis, la sécurité du cyberespace n'est jamais un canal sûr ; sécuriser cette porte numérique signifie maintenir la suprématie mondiale.

Mots Clés :

Espace Electronique, La force Souple, Politique Etrangère et Relations Internationales, Sécurité Nationale.

الملخص

إنَّ السَّعي وراء السّيادة العالمية جعل الولايات المتّحدة الأمريكية تدخل في صراعات و تحدّيات عسكرية لحماية أمنها القومي، ذلك ما يفسّر أشكال تدخلاتها العسكرية، التّي لم تقف عند حدود الواقع بل تعدّته إلى الفضاءات الرّقمية لتصبح بذلك العلاقات العالمية المادّية لها نظيرها الرّقمي في الفضاء الإلكتروني المعقّد.

الأمر الذي جعل المسؤولين الامريكيين في حاجة إلى تطوير و استخدام الفضاء الإلكتروني بصورة أكبر، باعتباره امتدادا لسياستهم الخارجية، و بوصفه قوّة ناعمة عابرة للحدود و مخترقة للثقافات، وبالتالي كان لابد من ضرورة تأمين هذه البوابة الرّقمية حفاظا على السّيادة و حماية للوزن السّياسي للولايات المتّحدة في ظل المنافسة المهدّدة لسياستها الوطنية، و من هنا كان الأمن السبراني القوّة النّاعمة التّي اعتمدها النّظام الأمريكي.

الكلمات المفتاحية: الفضاء الإلكتروني، القوة الناعمة، الولايات المتحدة الأمريكية، السّياسة الخارجية، الأمن القومي.

List of Acronyms

AIDS: Acquired Immunodeficiency Syndrome

APT: Advanced Persistent Threat

ARPANET: Advanced Research Projects Agency Network

CERN: the European Organization for Nuclear Research

CIA: Central Intelligence Agency

CPU: Central Processing Unit

DDOS: Distributed Denial of Service

DoS: Denial of Services

FBI: Federal Bureau of Investigation

FTP: Files Transmission Protocol

HTTP: Hyper Text Transfer Protocol

IAB: Internet Activities Board

IAB: the Internet Activities Board

IANA: the Internet Assigned Number Authority

IANA:Internet Assigned Number Authority

IBM: International Business Machine

ICCB Internet Configuration Control Board

ICCB: the Internet Configuration Control Board

ICT: Information and Computer Technologies

ICT: Information Communication and Technologies

ID: Identification

IETF : Internet Engineering Task Force

IETF: the Internet Engineering Task Force

IFA: Internet Freedom Agenda

IoT: Internet of Things

ISOC: Internet Society

IT: Information Technology

ITU: International Telecommunication Union

KGB: Russian Secret Service

MITM: Man in the Middle Attack

NIAG: National Information Assurance Glossary

NPL: National Physical Laboratory

NSA: National Security Agency

PLA: People's Liberation Army

QWERTY: Keyboard layout

RAND: a Research Organization that develops solutions for public policy challenges

RAT: Remote Access Trojan

SQL: Structured Query Language

SRI: Sandford Research Institute

TCP/IP: Transmission Control Protocol and Internet Protocol

UCLA: University of California, Los Angeles

US: United States

VPN: Virtual Private Networks

WHO: World Health Organisation

WWW: World Wide Web

Table of Content

Introduction

The last decade is considered, by excellence, the era of Information and Computer Technologies (ICTs). One of the significant features of this development is that states have become significantly interconnected via physical networks. Interestingly, the fact that states' physical demonstrations have dispersed in cyberspace has provoked a new mindset to security and power dichotomy.

The notions of security and power are key elements in national security strategies. Nation-states' technological capabilities are subsidised by the political will to encounter the evolving nature of cyberthreats, the involving actors and assert their dominance over the digital space. In contrast to military dominance, exercised through hard power coercion, cybersecurity emerges as a soft power tool aiming at gaining interests and wielding influence on other world actors.

As the pioneer of technological advancement, the United States has experienced several cyberattacks. These cyberthreats originated from states, mainly Russia, Iran and China, and non-state actors like cyberterrorists. In addition, US international interests also were thwarted. As a response, US officials accentuate the need for a cyber strategy to defend the country's national interests against a potential cyberwar.

This research discusses how the United States utilise cyber security as a soft power tool to exert political influence during Biden's administration.

This research was conducted to answer the following questions :(a) What is soft power? (b)What are cyber security and cyberspace? (c)Why has cyberspace become essential to US foreign policy? (d) What are the cyber security threats facing U.S. National security? (e)How is the soft power manifested in cyberspace?

The impact of the cyberthreats has urged US scholars and politicians to set practical solutions to secure national security and the country's supremacy. This research used the descriptive and analytical approach to explain the notion of cyberspace and the challenges it poses to national security. The analytical approach helps in finding the link between the idea of soft power and how it is linked to the practice of digital diplomacy.

As a consequence, this research is divided into three chapters. The first chapter tackles definitions of cybersecurity concepts and their relation to politics and soft power. The second chapter elucidates cyber issues, major cyber-attacks and their link to national security. The third chapter clarified how digital-diplomacy acts as soft power, emphasising Biden's perspective on cybersecurity issues.

This dissertation might contribute to raising the reader's awareness about the challenges of cyberspace to US national security. Moreover, this work might elucidate the importance of digital diplomacy and how it emerged as a soft tool in foreign policy.

Conducting this research faced several limitations related to sources, time and methodology. Cyberspace is purely technical, and the challenge is to limit the scope of the study and find the link between technology and how it is incorporated into politics. Another difficulty is deciding which methodology to adopt because the topic intersects with other fields of study. Moreover, finding sources of how digital diplomacy is conducted remains vague in politics. However, legislative and military approaches continue to rise .

Chapter 1: The Historical Background of Cyber Security

Introduction

Like any nation, the US national security is of high priority. This concept arose to meet the need to encounter emerging powers that had started to threaten its interests. Thomas Hobbes, the 17th-century philosopher, points out that “when there is a war of all against all there is no room for commerce, for the generation of knowledge, or for culture”. This condition of war generates a continual sense of danger and fear that urges individuals to “surrender some independence to their state”, as Hobbes states. In this context, the state is fully responsible for protecting its citizens and the territory(Samuels xxxviii).

The protection of national security encompasses engaging in wars and diplomatic means to achieve strategic goals. Adopting an over-force approach to secure the sphere of domination would endanger the nation’s integrity. Thus, the hard power could be substituted by a soft intervention.

In addition to commercial interests, digital technology has become a matter of interest. Securing cyberspace has received much attention from US stakeholders. Introducing information technology to American society has turned the virtual space into a replica of real-world aspects. This explains why US authorities have considered cyberspace another area of interest where the state could intervene.

1. The US National Security and the Mobility of Threats

National security is defined by Caudle as “a matter of protection against traditional, external military threats”(2). Nevertheless, this definition has been revised in regard to the national security necessities. For instance, Globalization forced the notion of the mobility of factors towards the US space, like goods, ideas, and the emerging of information technology. As a result, the traditional view of security had to be developed to cope with contemporary threats.

The concept of national security depends on numerous “drivers of change” (Caudle 2). Biskop et al. point out that power distribution among nation-states is defined by the growth of the power of non-state actors such as terrorist groups to be the contemporary change (4).

1.1. The Views on Security

The Post-Cold era had shaped how politicians viewed security. Thus, the definition of national security is consistent with specific change drivers. For instance, the traditional threats that endanger the state’s existence, such as military conflicts, have expanded to include non-traditional threats like cybercrimes and cyber terrorism**.**

1.1.1. The Traditional View

The Traditional studies on security consider all kinds of military threats as a matter of security. For example, the US declaration of war against Spain in 1898 was part of protecting its sphere of domination over the western Pacific and Latin America. The Spanish existence near its borders periled its economic interests in the area. In the same course of the war, the assassination of the crew of the US ship near Cuba prevails the issue of the security of individuals as a continuation of national security. Indeed, including individuals in the security equation challenges the traditional view about the field and prepares for a more grounded theory (Hoogensen and Rottem qtd. in Caudle 4.)

1.1.2. The Non-Traditional View

As the world changes, a need to cope with contemporary issues appears. Unlike the traditional view, which utterly focused on military threats, the non-traditional perspective on security went far beyond armed conflicts. Nation-states’ sovereignty is likely to experience other kinds of threats which compromise its physical existence and socio-economic and political welfare (Caudle 4). Moreover, it is noticed that the notion of security can be expanded to “include matters of individual identity, such as gender, ethnicity, and race”

(Hoogensen and Rottem. qtd. in Caudle 4). The concept of security might be broadened to involve mobility threats such as migration, transnational crimes, cyber terrorism, and other related issues outside the borders. This view, therefore, approaches security matters with individuals and international threats (5).

2. Types of Threats

The status of instability of a nation-state falls in the area of insecurity. As threats continue to rise, their impact on the existence of the state and its components relatively disturbs its security. Thus, recent studies presented in the non-traditional view of national security suggest other sources of threats which Sundelius categorises as structural and one-actor-focused threats (Sundelius qtd. in Caudle 5).

Such division alters the emphasis on the territory's physical security to include protecting critical functions within the state like societal issues, defending cultural values and the government's institutions (5).

2.1. Structural Threats

According to Sundelius, this type of perils refers to unintentional domestic or foreign accidents. For example, a nuclear explosion in a neighbouring country or a pandemic are foreign accidents. In contrast, the accidents that require crisis management, such as the collapse of infrastructure or a natural disaster, are domestic perils(5)..

2.2. One-Actor-Focused Threats

These kinds of threats are somewhat intentional. They are defined as assaults by armed individuals or groups, such as a cyberattack against the state's national or international interests.

For governments to withstand such threats, thresholds are applied (6). Consequently, threat-assessment plans to account for threats' severity and priority would enhance the security landscape. This explains the difference in states' reactions and risk identification.

The US considers transnational terrorism a central issue; recently, other threats have been identified to endanger US domestic functions of the state, like cyberattacks.

Unlike the traditional view of threats, it is believed that threats are evolving and relatively complex. Military actions are not solely about the obliteration of an opponent or seizure of territories; it is about the implicit political and economic objectives. Thus, it is important to be aware of the objectives which range from specific to complex, evolving to respond to forthcoming events. To illustrate, the Cold War era witnessed multiple threats that were complex in nature. Defending the national security of both opponents took political, economic and ideological dimensions. “The Americans cultivation of anti-communism as for the Soviet with anti-imperialism” lead to political threats to both countries. In the US, for instance, McCarthy’s episode threatened societal and political integrity. Anarchy in international relations stems from the battles of ideas, economies, and technologies; therefore, national security policies are set due to many varieties and system styles that emerge or be built (Buzan 95).

3. Cyberspace and Transformation in The Concept of Power

3.1. The Notion of Soft Power

The conventional definition of the concept of power has been restricted to military, economic and political contexts. As those contexts persist to dominate the world’s international setting, cyberspace also has emerged as an influential actor in ‘world politics’ (Jr 6).

According to Jr, cyber power, which is the adjunct of cyberspace, is more accessible due to reliance on the information. Consequently, the world’s major actors are facing difficulties in controlling this loose manmade environment. As a result, this digital domain has become the new arena of conflict in which world major powers exercise their capabilities or ‘soft power’ (6).

Cyber power is a transparent field of struggle amongst the world's major political entities to assert national security (Choucri 8). Nazli argues that this transparent field can appear on the surface of international relations since it is subject to "dynamics of interaction"; this explains the use of the concept "low politics" to account for "cyber politics" (8).

Either low politics or soft power, the two concepts recognise cybersecurity as means to achieve "power and welfare". This explains the warnings to urge governments to consider Information Technology a part of sustainable development. For example, an insightful observer declares, "no longer ignore the political salience of cyberspace…cyberspace is becoming "heavily contested, colonised and reshaped by governments, militaries, and private corporate and civic networks" (13).

This explains the perpetual domination of the US over world resources by the implementation of hard power.

As for the US, its future as hegemonic power is maintained through its hard control over world resources and an inevitable shift to soft procedures, as Jr. theorises. He argues that this shift of power revolves not only around controlling resources, or having them but also about changing states' behaviour, and accordingly, influencing their political environment; it is a part of confronting future complex challenges (155).

The US's efforts to place itself well in a world of mutilators was one main objective of its foreign policymakers. For instance, the president Henry Kissinger who was in favour of classical balance-of-power politics, delivered a speech asserting that "we are entering a new era. Old international patterns are crumbling. ... The world has become interdependent in economics, in communications, in human aspirations" (Nye 156). According to Kissinger, the world of politics would be more complex and challenging. Its complexity resides in its relation to the human desire to influence and control, which encompasses all domains of human interaction, mainly through information as a crucial means of communication.

Similarly, the US Secretary of State Hillary Clinton proclaims the necessity to consider Information and cyberspace as a means of soft influence. This idea was made clear in a 2010 speech at the stage of the Washington Newseum. Because of her deeply rooted beliefs in spreading Democracy all over the world. Hillary sought the need to implement Information Technology abilities to influence rather than other forms of hard power. Her declaration was in response to the exclusive dependence on the economic, military power and “lower-tech” to dominate, which furnished the Bush administration era (Morzov 34).

The cyberspace has attracted the US politicians during Obama’s presidency as an effective tool to advance the US model of democracy known as the Internet Freedom Agenda (IFA). Unlike the Freedom Agenda, which escalated public debate over its efficiency and methods, the IFA was seemingly regarded as a soft means to achieve democratic change. As a result, the Department of State pumped huge amounts of money to digital companies and organisations to carry out the project of Internet Diplomats. In this context, the anti-government outbreaks in “Iran, Moldova and China’s Xinjiang” were further cherished by the US freedom advocates.

Paradoxically, the ID, whose role was to promote democracy, have been associated by foreign states as “a Trojan Horse …and part of the American Imperialism” as Morozov states (34). The latter fact reveals how can cyberspace be utilized to serve an implicit agenda, in addition to the risk of power alienation; i.e, to act as a part of the Freedom Agenda both domestically and internationally, for which Bush was criticised.

3.2. What is Cybersecurity?

It is assumed that the term cybersecurity is widely incorporated to refer to information security and online activity. Thus, scholars have tried to provide proper definitions for the term which reflect their vision of the level of relationships between its variables.

Firstly, Merriam-Webster defines cybersecurity as the “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”. This definition rather emphasises the technical aspect and implicitly defines the user as a passive variable. Indeed, the protection of systems is paramount and measures should be set accordingly, yet it does not address other interdisciplinary variables that explain the complexity of securing the grid.

Secondly, cybersecurity, as defined by the Oxford dictionary, refers to the usage of different technical measures to encounter all sorts of criminal or illegitimate exploitation of electronic data through cyberspace. Furthermore, the word ‘cyber-’ is derived from cybernetics which means ‘the science of communications and automatic control systems in both machines and living things’ (‘Cyber- Combining Form’). Hence, ‘cyber-’ is combined with other ‘reality’ concepts such as terrorism, wars and security to denote the shift from reality to the virtual world.

Thirdly, the term cybersecurity has received much attention as the real world intersects with the virtual one; accordingly, academic views vary as the challenges accumulate. For example, Craigen et al. provide a literary review of the most convenient definitions. Cybersecurity is about the defensive procedures adopted to confront the ‘would-be intruders’ (Kemmerer qtd. in Craigen 14). In addition, the definition that the International Telecommunication Union (ITU) provides a broader scope to the term cybersecurity. For ITU experts emphasize the importance of protecting the users as well as the digital environment. In order to achieve this, many security variables are utilized like ‘technical tools, policies, security concepts, security safeguards, guidelines, risk management approaches concepts’(Cybersecurity)

3.3. Basics of Cybersecurity

Cybersecurity revolves around the safety of any internet-connected systems, networks, software and different types of data from cyberattacks. The cyberattack's objectives are consistently intended for destabilizing the system, to access, change and destroy sensitive information.

Cybersecurity has rapidly evolved during the last two decades imposing difficulties for both experts and academics as they seek to define its limits. Described as a vast digital space, many actors are involved in this environment, making it unsafe and to some extent hostile.

In order to understand this system of overlapped variables that interacts and drastically develop. It is necessary to tackle the basics that form the pillars of its security. To secure is what governments and high-tech companies try to work on to avoid any forms of system defiance and information exploitation. Thus, system designers incorporate authentication, authorization and nonrepudiation as security tools to address the "CIA triad";i.e, confidentiality, integrity, and availability.

3.3.1. Authentication

Information protection requires authentication procedures. According to Cuhen and others, authentication is a "security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorisation to receive specific categories of information». This definition clarifies the role of the source of information, the receiver and the message in itself. If one element does not conform to security standards, security is then jeopardised.

To achieve maximum protection of the three elements, numerous methods are adopted. Firstly, individuals' security is set through single or multifactor authentication. For instance, a system links an account with a simple security method like a question to be answered or simply a passcode. Whereas multifactor protection is rather a complexity is a combination of single methods such as the use of specific mobile applications provided by Microsoft. Secondly, protecting the message is also part of security. Generally, any transmitted data like emails are verified through an electronic signature. A signature or cryptography is like a passport that allows the message to pass security barriers. If the signature is outdated, it would be stopped, to some extent, considered a threat. Simultaneously, that signature defines the source of the message whether it is trustworthy or not.

3.3.2. Authorisation

Many users face difficulties in accessing certain data. This is because they lack permission; in other words, they do not attain authorisation. It is the privileges given to a user to access data, a program, or a process. Microsoft windows authenticate the user's credentials but limits the process of modifying or uninstalling programs. This is determined by a level of security set by the system's administrator to achieve maximum security and prevent data loss or exploitation (Contributor).

3.3.3. Non-repudiation

The amount of the exchanged data between different parties in cyberspace necessitates clear security standards. This is actually to trace the route of data and decide about the digital responsibility which is known as nonrepudiation.

According to Cuhen et al., nonrepudiation is defined as "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.". Therefore, the issue of digital responsibility can also provide physical proof to be relied on, in the real world during verification processes.

Secure systems thoroughly assign single or pair keys to each processed information known as symmetric and asymmetric systems. Firstly, the process of encrypting and decrypting data using one private key is called symmetric cryptography. Secondly, asymmetric systems maintain the use of pair keys; one is public to sign data whereas the second is private to verify data. This is known as nonrepudiation.

The asymmetric and symmetric systems are different in terms of the level of protection both afford. Symmetric systems' use of single keys to encrypt and decrypt data poses potential risks. If the key is reached by an information exploiter, the identity is thus easily exposed, as well as its data. Asymmetric cryptography is rather complicated and secured due to reliance on different keys to signature data. If the public key is exposed, the private key remains secure. Hence, any claims of identity forging are less likely to take place. This is known as nonrepudiation property.

3.3.4. Confidentiality

The term confidentiality is another key to assuring security. It is defined as the "assurance that information is not disclosed to unauthorized individuals, processes, or devices" ('SI110: Information Assurance').

To assert confidentiality is to protect information from being exposed to unauthorized parties. To achieve this objective, three steps are required. Firstly, the information has to be equipped with self-security protection abilities to keep it inaccessible to unauthorized users. Secondly, the level of restrictions should be set so that only the allowed personnel can view them. Thirdly, the presence of an authenticating system to check users' identities against information violators. Apparently, authentication overlaps with authorization for the sake of concealing and protecting information. Therefore, maximum confidentiality is attained.

To conceal data from its abusers, the storage appears to be another layer of confidentiality. This layer involves storing information in private locations or on networks.

Hence, solely legitimate users are allowed to access information. But, when the data needs to be transferred via a public network, it has to be secured by private keys which are used by authorized parties to decrypt the digital items. Another possibility of confidential data travelling is carried out through virtual private networks (VPN). A VPN secures the traffic routes as well as offers strong encryptions between endpoints. Additionally, the confidentiality of information should also be realized by encrypting data on the physical backups; this procedure prevents data misuse.

Confidentiality of digital information encompasses controlling the physical environment of potential users. It is noticed that most of the threats come from the world of the user. For instance, some digital crimes happen due to shoulder surfing. It is a nontechnical method that requires looking over someone's shoulder to steal sensitive information from the computer screen. Acquiring such confidential data jeopardises confidentiality. Yet, new techniques are developed by hackers such as the direct embedding of malwares in the victim's computer to steal data. The outside world imposes threats that one should consider.

3.3.5. Integrity

The concept of integrity is one of the pillars of information security. It signifies the trustworthiness and reliability of a system where data is stored and that it is not subject to unauthorized modifications. Herrmann defines integrity as follows:

> "Quality of an IS (Information System) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information." (Herrmann 561)

According to the definition, information systems integrity implicitly mean data integrity. This means that data safety requires system integrity; authorization, authentication and nonrepudiation are the keys to sustaining such integrity. To illustrate, if a system is invulnerable, the stored data is thus safe and far away from manipulation.

An information system, which involves software that is vulnerable, threatens data integrity. The exploitation of the system's deficiency results in the modification of data; therefore, the host system is described as untrustworthy. For instance, the exploitation of the Structured Query Language (SQL) of a server by injecting vulnerabilities allows the hacker to modify the stored database. Hence, confidentiality, authorization and authentication are violated. A hacker infiltrates the bank's database as a result of vulnerabilities in the system. The possibility to intercept a message of a bank transfer from a potential client to another. As a result, the target account number is modified and the route of transfer is altered to another destination. This example illustrates the risks behind the lack of data integrity.

3.3.6. Availability

The last feature of the CIA triad is availability. It is about the system accessibility in real-time to provide services. Therefore, any delay to respond to online service or denial of requests of the authorized users questions its value. The NIAG defines availability as "timely, reliable access to data and information services for authorized users". To clarify how system abusers exploit availability, hackers tend to overload the system with packets that mainly target the CPU, network or any other system component that can be influenced. These attacks are known as Denial of Service (DoS). It is aimed at saturating the system until it stops responding to legitimate users' requests.

3.4. The History of Cybersecurity

The history of cybersecurity goes in parallel with the introduction of the notions 'Cyberspace and the Internet. Such digital dimensions were actually the result of a heating competition between the US and the Soviet Union during the Cold War as part of their supremacy practices, mainly in the field of telecommunication.

The telegram, and then the wired telephones as means of communication seemed traditional and vulnerable which the West continued to dominate especially during WW2 and later. The Russians were a step ahead to reach outer space by launching their first space satellite, Sputnik on the 4th of October 1957. As a reaction, the US rushed the world to face a new era after it had announced its Advanced Research Projects Agency Network (ARPANET) in the 1960s.

The idea of the ARPANET project is based on connecting two computers via a wired network. The aim of this 'simple' network is to send messages between two terminals; their objective is to anticipate a time of nuclear war where all traditional sorts of connections could be shut down. In order to ensure the flow of connection, experts' novelty resides in breaking data into packets that are transmitted through wires. Consequently, the first experiment was held at Leonard Kleinrock's laboratory at the University of California, Los Angeles (UCLA).

Scientists' design of the network took a linear form;i.e, "two nodes". Each node is connected to a computer. In addition, the computers were located in different places; the first was at UCLA whereas the second was at Stanford Research Institute (SRI). The next step was crucial; The experts managed to send the message 'Login' from the first computer to the second one. Unexpectedly, on the target computer, only the first two letters from the word 'Login' appeared on the screen, and the network faced a complete shutdown. Afterwards, the lab technicians repaired the network, and communication was restored without defects. The ARPANET first prototype coined a huge technological advancement in the US and notably cyberspace.

The US expanded the usage of the ARPANET to link many universities. This could only be possible by developing sets of 'rules of communication or protocols' via the internetwork which was referred to as Transmission Control Protocol and Internet Protocol

(TCP/IP). Such development ensured the transmission of data between different computers by organising the assigned address of each university on the network.

As a consequence, the National Science Foundation which was created in 1986 gathered many US universities on the same network forming the NSFNet. By the 1990s, the NSFNet replaced the ARPANet in the US. Subsequently, many other networks were created alongside with ARPANet. For example, the National Physical Laboratory (NPL) in 1965 and the Michigan Educational Research Information Triad formed the MERIT in 1966. Remarkably, this technology was also utilized by other countries mainly the United Kingdom and France (Andrews).

The spread of such significant technology across continents paved the way to more sophisticated plans to link not only universities but also societies in a digital space, cyberspace; paradoxically, security issues are imposed as a part of the dichotomy.

3.4.1. The Internet Structure

In order for a network to work effectively, it has to be identified and well-structured besides other sub-networks; this also applies to the components of each network. For a network to work efficiently it should be assigned a numerical address or TCP/IP. Such an organisation is based on mathematical algorithms that prevent any technical problem. The Internet system is thus protected via sets of protocols and regulations, though millions of networks are interconnected. Therefore, The Internet Society, which was established in 1992, monitors the issues related to the enormous networks such as setting ‘rules, regulations and protocols that allow access to the global network.

3.4.2.The Internet

The term Internet refers to the medium where networks overlap and connect through protocols. It is defined as the inevitable common space that provides digital services and utilities like the World Wide Web (WWW), messaging, e-commerce and video telephony.

From the 1980s to the 1990s, the internet was exclusively operated by the US military through the ARPANet. Afterwards, Experts sought the need to separate the two systems so that civilians could access the service as commerce flourished. Notably, both layers of the military or civilian internet were kept interrelated. This fact demonstrates how 'the control over technology' practised by the pioneering firms in the US like IBM was part of the US political domination over the world. For example, IBM introduced its own technological standards like QWERTY type-writer keyboards. The same company had its own TCP/IP which was different from other firms like Xerox.

The race of interests between the US government and other governments made the Internet a battlefield. For example, the early adoption of English intimidated other ethnic groups like the French. To solve this issue, computer companies designed graphical system interfaces that support different languages. Furthermore, the US applications that afforded file transmission (FTP), the internet provided were not satisfactory to world users in terms of data location. Thus, a world arrangement was set by adopting the World Wide Web application. It replaced the traditional forms of local file transfer with huge data exchange. This technological leap reduced the powers, in some ways, of the US firms.

The World Wide Web application is considered one of the utilities that the internet employs. It is based on the Hyper Text Transfer Protocol (HTTP) to send and receive data from a client to a server. This protocol was developed by a 'UK scientist Tim Berners-Lee in 1989 at The European Organization for Nuclear Research (CERN)' ('A Short History of the Web'). This sophisticated discovery allowed the rapid exchange of information throughout the internet.

3.4.3.The First US Networking Initiatives

In the late 1980s, the US witnessed the first form of 'formal governance' initiated by the Internet Aiming to rationalize and manage the standardization of TCP/IP, many organisations were established under the leadership of three business US giants. As a result, the Internet Configuration Control Board (ICCB) was established by Vinton Cerf in 1979 (Mowery and Simcoe 1374). In 1983, the Internet Activities Board (IAB) replaced the ICCB in the tech community; this was only recognized after the ARPANET switched over TCP/IP protocols. As many actors joined the Internet, the Internet Engineering Task Force (IETF) was incorporated to “manage the internet’s architecture and technical standard-setting processes, along with several other sub-committees” (1374).

The IAB’s role to manage infrastructure and networking in the US was highly acknowledged. Surprisingly, this organisation faced funding problems; the Internet Society (ISOC) was founded in 1992. Its funding depended on a variety of private and public resources. Though the ISOC’s objective was similar to its precursor in terms of managing the internet’s architecture, it brought together the activities of numerous loose institutions like IAB, IETF and the Internet Assigned Number Authority (IANA).

The ISOC’s contribution to the tech community had a remarkable impact on the network. The technical performance was monitored by decisions generated on the basis of those “self-governance” organisations. As a consequence, the overall network system continued to evolve. Mowery and Simcoe accredit this technological growth to ISOC as it helped in restructuring “the environment to be free of pressures of standard-setting for proprietary technologies”(1374).

3.4.3.1. Proprietary vs Open Standards

Proprietary and open standards emerged as a key to the development of the network. In fact, their value in the world of technology continues to cause a debate based on different perspectives.

4.3.1.2.Open Standards

According to Zubrinich et al., the open-source standards were developed by the Information and Communication Technology (ICT); their importance relies on ensuring “interoperability, efficiency and ease of communication between electronic devices, such as smartphones, laptops, audio systems, and televisions”. From an economic perspective, integrating open technologies permits the development of products at a lower cost. Moreover, the benefits of having many companies participating in the open-source reduce the risks and result in producing advanced products .

4.3.1.2. Proprietary Standards

Unlike open-source standards which are subject to collaboration and exchange, the proprietary standards are “developed and controlled by one company or a small group” ,as Zubrinich and others state. Such products are considered “an unavoidable technology”; and therefore, they become a subject to market competition. For instance, Microsoft Office (Office suite) and Adobe Photoshop are proprietary products.

5. Cyberspace Actors

The issue of security in cyberspace is apparently challenged as numerous actors are involved. Those actors pose threats to the information infrastructure due to the utilization of innovative cyber-tools that can exploit system vulnerabilities. Ekanayake et al. categorisation of such actors is based on their ability to “undermine the integrity of the protection status of your device’’

5.1. Cybercriminals

Cybercriminals perform attacks on systems to steal data for financial profit like money transfers and hacking bank accounts. Moreover, these kinds of criminals use the Dark Web as a cyber market for trading such as drugs, human organs, weapons, assassination operations, money laundering and white-slave trafficking.

5.2. Hackers

A hacker is a professional computer expert who can employ his skills to perform cyber operations. These skilled individuals are of two types. Firstly, professional hackers or the white hackers who are hired by organisations for improving security measures of systems. Secondly, the malicious hackers, or crackers, whose skills are hired to accomplish criminal acts against states, individuals or organisations. Their techniques involve the exploitation of vulnerabilities in systems. Surprisingly, crackers can be part of a shadow organisation like Anonymous.

5.3. Hacktivists

Because of the rapid incorporation of the Web, some states issued laws to restrict human rights movements. Thus, cyberspace became the only resort for hacktivists to denounce their oppressors' practices, aiming to gain either domestic or international support. For instance, Algerian hacktivists use the Dark Web to escape the government's restrictions.

5.4. Cyber Terrorists

The notion of terrorism has become a central issue in the real world. Surprisingly, it has been altered to the digitalised space. Cyberterrorists could freely perform attacks, mobilize adherents and raise funds, propagate their beliefs and challenge world authorities.

5.5. Nation-States

States can be responsible for cyberattacks against other states. These forms of attack are meant to achieve strategic objectives and, at the same time, avoid legal and political responsibility. Deciding which actor is responsible remains a debatable issue due to the complexity of cyber technologies and the actual performer of the attacks.

6. Forms of Cyber-Threats

In order for attacks to achieve their objectives like disabling operations, different forms of assaults are elaborated by cyber actors. Their strategies describe are perpetual and innovative in terms of their complex nature; some of which can be combined resulting in powerful tools.

6.1. Malwares

Malware is short-written computer software, also known as malicious software. This kind of software is designed to carry out specific harmful operations on the target operating systems of servers, single computers or large networks. Accordingly, their nature varies as D and H state; they can be worms, viruses, trojans, botnets, RATs or Ransomware viruses. To distinguish between them, one should consider the way they are produced and generated. As D and H put on "[…] distributed in common file types attached to your emails, circulating on social media or direct you to websites where these files are downloaded (most of the time without your knowledge" (29-33).

6.2. Phishing

Amongst the techniques to steal sensitive information is called phishing. D and H state that this technique basically depends on generating fake emails and then sending them randomly to victims. The emails contain a link that would trigger malware which steals sensitive information or even encrypt data.

Phishing incorporates other methods. First, spear phishing is regarded as one of the most dangerous techniques because it targets a specific victim. This personalized type of scam is hard to detect. Second, whale phishing, according to D and H, is designed to attack businessmen, hence forcing them to perform financial transactions. Third, voice phishing, known as vishing, utilizes phone calls to reach the victim and then gives instructions to perform transactions through pressing numbers. Lastly. SMS phishing is the process by which the hacker sends an SMS containing malware. This link can be camouflaged by a picture or simply words. This depends on the victim to trigger the malware/trojan (*41-44*).

6.3. Denial of Service (DoS)

A denial-of-service attack, a brute force technique, is a cyberattack described as traffic-based; it is achieved by directing huge amounts of online traffic towards target servers as to prevent or delay access to online services. Recent attacks were described as a denial of services attacks like Ukraine and Georgia. More importantly, DoS techniques are now regarded as part of cyberwars (‘What Is a Denial of ’).

6.4.Man in the Middle

According to Yasar and Cobb, a Man-in-the-Middle attack (MITM) is a technique that involves secret interposition between the target user and the requested web service. This technique is aimed at harvesting the victim’s personal information as well as performing traffic analysis. For example, the attacker would create a Wi-Fi network to simulate other secured networks. Once a victim connects, the attacker intercepts the traffic and extracts data. It is also possible to divert the victim to malicious websites similar to reliable ones like Facebook and any other Web services (Yasar and Cobb).

6.5. Cryptojacking

Cryptojacking is a cybercrime in which the attacker remotely obtains someone else’s personal computer in order to generate cryptocurrency. To perform cryptojacking, one should secretly install malware on the victim’s computer. When doing so, a JavaScript is to be executed which in return generates a series of algorithmic calculations, on the victim’s browser, to start mining(‘Cryptojacking’).

6.5.SQL Injection

According to Kaspersky, SQL injection attacks are designed to take over the victim’s database. Hackers use certain scripts mainly to penetrate a website’s database and then search for the vulnerabilities to be exploited. What makes these attacks potent is that they utilize scripts written in the Structured Query Language to perform commands, which is the same language websites use when intending to store users' credentials. As for vulnerabilities, they are assumed to be the consequence of improper programming (Kaspersky).

6.7. Zero-Day Exploits

A Zero-day exploit is a form of attack which target systems 'vulnerabilities. It is possible only if the system's developer is not aware of the breach. This type of attack takes the name Zero-day because "once a patch is released by the system developer, each day represents fewer and fewer computers open to attack as users download their security updates "as Kumar points out. As for techniques to conduct this assault, it is believed that they are to be sold on the dark web. Generally, different exploits and vulnerabilities are discovered by government agencies that "polemically may use them for their own hacking purposes, instead of releasing information regarding them for the common benefit" (Kumar).

Chapter 2: Cyberspace as a New Domain in National Security

This chapter deals with the relationship between national security and cybersecurity, which has become one of the significant priorities of national security policies. It is noticed that cyberspace emergence is accompanied by multiple threats which differ in nature, such as cybercrimes, cyber espionage and terrorism, and took further escalation to denote the beginning of cyberwars between different actors.

1. Cyberspace as a New Domain in National Security

National security is generally defined as the different strategies states set to protect political, social and economic existence, in times of war and peace, against traditional threats. Yet, the developments in the IT field have been recognised as a new source of peril to the existence of states. Consequently, cybersecurity was included in states' national security strategies to protect the infrastructures from cyber-attacks.

1.1. The Complexity of the Cyberspace

The complexity of cyberspace can be examined through the shift of the physical content to the digital world. Concerning national security, it is noticed that the physical attacks on states' strategic interests have also been dramatically transformed to take advantage of the virtual world. Thus, as numerous actors are involved, cyberspace has tremendously evolved to be another significant source of threats.

In computing, the notion of complexity denotes the different layers, software and hardware, by which a network is technically established. Thus, Cavelty's explanation of the term, in the light of Moore and Metcalfe's Laws, emphasises the technical aspect of the phenomenon. Moore's Law accentuates the number of transistors integrated into a circuit. This combination is expected to multiply every 18 months per square inch. Consequently, the computing power increases exponentially through time. Metcalfe's Law highlights the relativity between the number of users and communication growth. As a result, the more communication is established, the more networks, systems, and links implicitly increase to respond to users' needs (17).

As networks rapidly spread, the notion of complexity receives much attention due to uncontrolled and decentralised networks. The geographic dimension of this technical innovation is viewed as subject to accidental failures. Cavelty states that this issue is purely technical as systems interdependency. Moreover, this network is inherently vulnerable to escalating failures that challenge the anticipatory security measures. Therefore, the human brain faces difficulties reading these networks' networks-within-networks because of the non-linear cause/effect relationships (18).

The human factor interaction with the cyberspace complexity level is assumed to lead to "national-security-uncertainties" (Cavelty 18). Those uncertainties result from deciding about the nature of threats that are ambiguous and hard to expect. Thus, the national security policies would be described as insufficient or obsolete in coping with the ever-developing threats and exploiting systems vulnerabilities (18). Cyberspace emerges as a source of threat to states' national security as it evolves.

1.2. The US National Security and Cybersecurity Dilemma

Despite the US cyber capabilities, experts believe that the outlined strategies to advance its interests in the digital realm have been systematically questioned as cyber threats continue to evolve. Hoffman believes that the US cyber strategy has been ineffective. A mounting frustration thus had initiated the Congress to create a "Cyberspace Solarium Commission" to "develop a cohesive U.S. strategic approach to cyberspace," which has progressively evolved until 2003 (131).

The status of the cyber approach had reached "an inflection point" in 2018, according to Hoffman. Due to the participation of the Department of Defense's new Cyber Strategy, the US witnessed a status of relaxation. This new posture was believed to be the outcome of a national strategy directed toward a more offensive role in cyberspace. The same can be said about other countries that struggle to manage the escalating cyber competition. Hoffman argues that the subject of the international cyber competition was tackled a long time ago. He adds that "Professor John Arquilla of the Naval Postgraduate School and RAND scholar David Ronfeldt declared two and a half decades ago that "cyberwar is coming." Yet, an amassing body of literature has produced little consensus on the core tenets of a strategic framework for the use of cyber capabilities.".To secure the national perimeter, countries must develop a strategy consistent with the owned capabilities. However, Hoffman claims that this stage has not yet been reached because countries lack "grand strategists" (2). This explains why the current political debate over the utility and purpose of cyber capabilities has not reached a compromise "utility and purpose of cyber capabilities and how to deal with cyber-related problems.".Reaching a compatible strategy to deter cyber threats is considered a challenge for US administrations to have a more assertive posture.

2. Cyber Crimes

Cyberspace, as an alternative medium to human interaction, unveiled the negative side of technology where actors utilise it to damage the physical infrastructure, financial sector and identity theft or destroy sensitive data. Being the main initiator of such cyber operations, it is assumed that the human factor takes full responsibility for most cybercrimes.

2.1. Definition

The definition of cybercrime has evolved in parallel to the views of cyberspace which is a socially constructed reality (Wall,*Cybercrimes?*105). This implies the convergence of societal patterns and virtual reality. Wall believes that individuals' relationships and physical interactions have taken other forms of expression in the virtual environment. Consequently, the conventional definitions adopted in the physical realm are subject to change in the virtual one due to time, space and the involved actors. Thus, Wall's analogy to criminal activity explains the difference in conventional definitions across the physical and virtual worlds.

Firstly, the traditional concept of a crime is understood in a real-time framework and physical circumstances. Secondly, it occurs in a well-defined geographical and social setting governed by laws. Thirdly, a crime is defined on the basis of conventional social values that label what is acceptable from what is not. Fourth, traditional criminology has emphasised the offender and not the victim.

On the other hand, cybercrimes contrast with traditional crimes in many distinctive features. First, their respect for time, space and place cannot be defined as they have no clear boundaries. Second, no apparent, effective practical structure responds to all threats; Wall relates this to the necessity to change the law enforcement culture. Third, encountering such crimes involves an informed level of technical knowledge gained from higher education. Fourth, there is no set of conventional values that pose limits on cybercrimes. Yet, the debate over what constitutes the elements of cybercrimes is still unsolved. Fifth, Walls argues that the study of cyber-criminology prioritises the offensive aspect and, to a lower degree, is victim-based (110).

Based on the distinctive behavioural views of crimes, according to Wall, cybercrimes are defined in the light of juridical bodies and the acquired professional experiences that apply to law enforcement. Consequently, he defines cybercrimes with "the assault of integrity of network access mechanisms" such as hacking and cracking, cybervandalism, spying, denial of service, viruses etc. Furthermore, Wall states that "the use of networked computers to engage with victims to dishonestly acquire cash, goods or services through phishing, advanced fee frauds" is a computer-related crime. Lastly, he considers "the computer-content crimes relate to the illegal content on networked computer systems and include the trade and distribution of pornographic materials as well as the dissemination of hate crime materials" (*What are Cybercrimes?* 2).

2.2. The Contours of Cybercrimes

2.2.1. Cyber-Trespass

Cyber-trespass refers to acts that transcend the established boundaries into space. The knowledge acquired by computer hackers allows them to penetrate systems at any time. Their motive comes from a strong belief in the freedom to access all information. At first, hackers resembled the "spirit of America" and the "genius of youth" (Chandler.qtd. in Wall,*Cybercrimes* 113), but later their goals changed as a result of a successive demonisation. Their skills and beliefs have now persisted in being a threat. Consequently, Wall's classification of trespassers falls into two types according to their motives. They are the intellectually motivated and the politically or criminally motivated ones. The US army considered the latter unsafe due to the degree of risk to national security(*Cybercrimes* 114). Wall categorises cyber-trespassers into four forms which are the utopians, cyberpunks, cyber-spies and cyber-terrorists. Utopians believe that they are serving their society by exposing its vulnerabilities. Cyberpunks intentionally tend to harm targets that offend them; they are regarded as anti-establishment. Cyber-spies and cyber-terrorists are engaged with political, financial or moral motives. They aim to disrupt a constant order(113).

In order to harm systems or gain data, cyber-trespassers utilise many attack forms. In 1980, worldwide organisations received blackmail viruses that encrypted data on hard drives. The virus arrived in local drives through floppy drives claimed to be AIDS training packages. Consequently, the virus was self-activated and could only be disabled by paying an amount of money to an address in the USA.

2.2.2. Cyber-Theft

As Wall states, cyber-theft refers to “a range of different types of appropriation that can take place within cyberspace”. He identifies three kinds of acts: cyber-credit, cyber-cash and cyber-piracy (113).

2.2.3. Cyber-Credit

The act of appropriating and using stolen credit card information is referred to as cyber-credit. Thieves tend to obtain personal information and then use it to carry out financial operations such as buying goods over the internet. The complexity of this act is that it can be initiated in one place and committed in another. For instance, one can obtain the victim’s credentials in the US and perform a purchase in China.

2.2.4. Cyber-Cash

Like other sectors, financial institutions like banks have digitalised their physical services. Clients could efficiently conduct financial transactions remotely. Thus, the concept of cyber-cash is developed as another form equivalent to the physical monetary system. Yet, this concept seems to raise security issues as digital offenders developed countermeasures to obtain the personal identification numbers linked to cyber-cash credits (Wall, *Cybercrimes* 118).

2.2.5. Cyber-Piracy

Cyberspace has become a melting pot of its inhabitants’ intellectual products. Accordingly, cyber theft is more likely to occur. Wall states that cyber-piracy is the act of appropriating the different forms of intellectual property found in the digital realm (118). Wall argues that digital-theft motives are financially rewarding. He asserts that cyberspace has become a place of conflict over intellectual real estate, unlike physical objects, which are spatially and legally protected. The cyber-theft of ideas is less risky due to their high monetary value and falling out of states' juridical boundaries (119).

The piracy of intellectual products is of two types: the counterfeiting of (physical) products and the actual owner's interests in their properties. Wall points out that the counterfeiting of physical products exists in cyberspace. He defines it as the act of copying an original product and distributing it on cyber-shops. For example, a cyber-thief can appropriate a famous pop star's images and scans them. The digital image is later put in a professional format, with extra modification. Next, the new product is sold via cyber-shops. To escape legal persecution, money is thus sent to a different bank outside the national borders. The other variant of intellectual theft resides in the original owner's awareness of cyber theft. In order to prevent the reduction of the product's monetary value, real owners keep informed of any illegal appropriation in cyberspace, regardless of the thieves' motives. In the US, Elvis Presley's intellectual properties, such as images and trademarks, are protected by law. Wall points out that the Tennessee Celebrity Act 1984 is legislation set to protect the rights of Presley's enterprise. According to Wall, the aggressive and laborious policing behaviour to protect Elvis's images carried out by his descendants was known as the Darth Vader of merchandising (120).

2.4. Cyber-Obscenity

Cyberspace was another projection of societies' values and behaviours. The emergence of obscene materials over the internet usage caused a status of panic, subsequently questioning the Internet regulations. Wall points out that this panic was the result of a study related to the consumption of pornography. Despite the biased methodology representing 1% of society, the debate over internet usage and regulations became an essential issue in public discussions.

In general, discussions over obscene materials were regarded by Wall as "emotive rhetoric». This is related to a society's identification of pornography which cannot reach a consensus. For example, it is found that certain materials are classified as obscene by the

British and acceptable by the Scandinavians. The obscene materials in cyberspace, and its unconventional variant dynamics, resemble the beginning of complex future cybercrimes (124).

2.5.Cyber-Violence

Cyberspace is stated to be a suitable environment for violence. Wall defines cyber-violence as "the violent impact of the cyber activities of another upon an individual or social grouping". Though the impact of such violent activities on individuals is not directly physical, the victims may experience long-lasting psychological effects. Those cyber-activities take different forms, such as cyber-stalking, cyber-hate-speech and bomb-talk (125).

2.5.1. Cyber-Stalking

This deliberately cyber act is performed by "the persisting tracking and harassment of an individual by another. One can persistently send emails and obscene materials like images, videos or even death threats to the victim. For example, in the mid-1990s, Jake Baker was prosecuted after publishing a fantasy rape-torture story on a web newsgroup. 'Doe', the story's title, was reported to be similar to his student's name. Despite that similarity, Wall states that Baker did not stalk the girl, nor he met her. Such violent acts' impact contributed to significant worry (Wall,*Cybercrimes* 125).

2.5.2. Cyber-Hate

Unlike cyber-stalking, which violates individuals' personal life, cyber-hate is broader; it breaks social or ethnic groupings within the cyber realm, as Wall states. It is achieved by denying others social rights and disrupting the peace status with the rest of the group. Spreading hate-speech ideas over the internet is proved to have disastrous effects on the group being targeted.

2.5.3. Bomb-Talk

Bomb-talk is another form of cyber-violence. It aims at providing sophisticated technologies or instructions to target physical targets such as infrastructure, ethnic groups or individuals. This form is empowered by hate speech that circulates in cyberspace. Wall gives the example of Pryce, a hacker who could make world calls for free. The latter hacker obtained the necessary software, the bluebox, from the internet, which allowed him to manipulate different frequencies to make calls anywhere in the world (126).

2.6. Victims of Cybercrimes

The concept of crime is a crucial feature of any society, whether civilised or not; it cannot be separated from the social existence, as Das and Nayak point out. The studies conducted by the 2006 Computer Crime and Security Survey showed that 47% reported the theft of laptop computers and mobile devices in the area of e-commerce. Furthermore,3% of the respondents experienced the theft of proprietary information, 6% reported website vandalism, 9% were victims of financial fraud, and 3% were sabotage targets. These findings support the claims that cybercrimes high rates threaten societies' values like safety, money, peace and property (Das and Nayak 143).

Agreeing upon one comprehensive definition of cyber-victimization is impossible. As a phenomenon, cybercrimes dynamics are subject to "the relative socio-political and economic changes occurring in the existing system of society" (147). Consequently, cyber-victims will vary according to the level of victimisation, their status and group collectivity (Wall 127).

3.Cyberespionage

Due to the hostile geopolitical environment that governs international relations, states' national security is at risk. Thus, amongst the prominent strategies, the belief in obtaining information about potential adversaries remains a top priority. This is a key to enhancing their national security.

3.1. Definition

Cybercrimes can be a lethal weapon when they serve states foreign interests. Cyberspace is thus appearing to be another battlefield for obtaining information. Intelligence agencies have developed innovative methods to respond to new IT threats as the body by which information is acquired. Those methods, as part of cyber warfare, depended solely on what is known as cyber espionage.

Traditionally, Russel views the act of spying as a clandestine activity. It is about recruiting agents who can infiltrate the physical borders of a foreign state and achieve specific missions. Accordingly, agents'reliabilty depends on the value of the provided information, which relies on secrecy, which has become a key feature in the information age.

Cyberespionage is the consequence of traditional espionage but in a sophisticated manner—the high level of secrecy that cyberspace allowed states to take further actions at a low cost. The ability to stealth from far, access confidential data and conduct subversive activities raise cautions about the escalating utilisation of this technique in the future of state relations (19).

As far as cyberspace is concerned, states' national security is believed to fall under the influence of several factors, which are probable, seen and predictable. De Silva elucidates that those factors can be "internal /or external" threats and that they are augmented by "the skill set and access granted to the individual(s) or group(s) that can be a threat" (63). The degree of damage can be seen on two levels. First, individuals become an internal threat when they plan to harm the organisation's infrastructure, company, and employees. Second, if they exploit their access to the organisation's systems, their impact becomes more harmful. Because they utilise their skills and knowledge, insider threats are considered a security challenge. Thus, De Silva provides a clear distinction between espionage and cyber espionage. The earlier focuses on insider threats whose direct access allows them to gain information or knowledge and then give it to others. The latter refers to gaining information internally or externally by employing a computer or other remote technologies (63).

Consequently, cyber-espionage is defined by De Silva "as a form of espionage Cyber-espionage is a form of espionage that can occur locally, from a distance, or even from the cubicle right next to the person/target of interest" (63). Engaging in such espionage necessitates only a system linked to the internet, such as mobile phones or computers. Moreover, De Silva highlights the idea of insider threat which refers to the involvement of many internal and external agents. These agents' actions are considered "harmful and financially detrimental" to the company or agency they work in. To understand and determine the impact of insiders on the company, De Silva stresses the role of the insiders' background as well as their access to various projects and information. For instance, it is assumed that hiring data scientists, penetration testers and data analysts can be an insider threat. Their skill sets allow them to access sensitive data, in addition to their positions on projects. The problem behind such threats extends to affect national security and the company's participation in assuring continued stability of national security (63).

When an insider threat conducts espionage for a company, or other countries is regarded as a threat to national security. Undoubtedly, the activity of transmitting sensitive data can occur unintentionally or intentionally, as De Silva points out. Intentional espionage can happen in conversations outside the workplace like coffees, houses and restaurants. It is believed that the degree of severity is associated with the nature of the publicly-transmitted information. On the other hand, the intentional or deliberate transmission of information about "issues that affect security measures and the infrastructure of a facility is seen as a deliberate attempt to harm or affect national security" (64). Deliberate or undeliberate disclosure of information can be viewed as espionage, but when computers or mobile phones are involved as means to transmit data is therefore cyber-espionage.

Deciding about the value of the information to leak and the way to transport it are decisive to successful cyber espionage. Insider threats may find it challenging to identify the value of the information they have access to unless they have it "presented to interested individuals that wish to acquire information" (De Silva 71). For example, a data analyst, who is responsible for a project, cannot recognise the actual value of the information. Factors that limit such ability depend on expertise in the subject matter and the lack of knowledge about other disciplines. However, it is proven that individuals' knowledge would increase if their working environment provided them with partners whose experience in the subject matter is significant. Consequently, the individual is assumed to attain more analytical skills to arise as a threat (De Silva 71).

Assuming that the intended information has been successfully recognised by the internal/external agent(s), transporting a large amount of data within the limitations of networks is yet viewed as another challenge to cyber-espionage. Local networks cannot respond to the excessive remote cyber-retrieval of data due to security barriers scaffolded by a national security strategy. Hence, attackers utilise large networks and data systems to be able to transport such large amounts of information, as De Silva states. Yet, countermeasures to handle the issue of reducing information value by encryption methods arise as a new challenge in espionage.

3.2. Cyberespionage, a Threat to Information Security

Technically, it is assumed that cyberespionage undergoes a systematised process to gain access to sensitive information. According to Hermann, that process involves the violation of cyberspace's confidentiality, integrity and availability.

3.2.1. Confidentiality Violation

Cyberattacks attempting to disrupt information sources are described as violating confidentiality. Herrmann refers to such type of violation as unauthorised information disclosure. It means access to classified information without being authorised.

Hermann classifies attacks that threaten confidentiality into four types: exposure, interception, interference and intrusion. First, exposure is about accessing sensitive data due to the lack of protection mechanisms. Second, seizing data while it is being transferred amongst authorised entities is known as interception. Third, Hermann defines interception as the apparent act of observing "innocuous pieces of information such as metadata" and then predicting the missing parts of the sensitive data. Fourth, the act of intrusion is achieved by obtaining sensitive pieces of data by circumventing protection functions such as "authentication and access control" (86).

3.2.2. Integrity Violation

Deception is the second phase of cyberespionage. It is the result of an integrity violation. Attackers provide the original users with misleading data that facilitates acquiring necessary credentials that grant access to sensitive data.

The system abusers rely on social engineering tools to realise three types of attacks: masquerade, falsification and repudiation. Firstly, a masquerade attack aims at misleading system protection measures by pretending to be another authorised user. Secondly, falsification is about the presentation of manipulated data that forces the target system mechanisms to accept it as genuine. Thirdly, repudiation is a term that denotes denying responsibility for an act, as Hermann points out. For instance, when a potential user receives a blackmailing threat, he would call the police, which depends on the sender's name. The trick to successfully repudiate responsibility is that "there is no mechanism that ensures the authenticity of the sender addresses in the email system" (Hermann 87).

In addition to deception, attackers tend to take control over specific system services of the target system. This threat is known as usurpation. Consequently, controlling system resources by an entity is referred to as misappropriation. If the system resources are used to perform certain functions relevant to security, then it is called misuse (87).

3.2.3. Availability and Integrity Violation

For cyber-spies to decoy and distract the original system operators from exposing any system's anomality, they manage to target the system's availability and integrity. Herman identifies this threat as disruption.

Disruption is the consequence of incapacitation, corruption and obstruction. The objective of the three forms is to prevent the system from working correctly, modify the system's parameters or interrupt data delivery between systems by delaying its operation.

3.3. The Cyberespionage Process

Information gathering, believed to be the eventual objective of cyber-spies, is never accidental. It undergoes specific processes that depend on malicious programs to obtain sensitive information. To understand the underlying mechanisms, Rivera et al. analysis of twenty relevant cases of cyber-espionage revealed nine phases: reconnaissance, preparation, attack, infiltration, information gathering, maintenance, information leakage, information sale, and escape (5).

3.3.1. Reconnaissance Phase

This phase is conducted by gathering interesting information about the target, such as IP addresses, employees' names and email addresses. Such thorough investigation is essential to deploy attacks. Furthermore, reconnaissance encompasses the use of social engineering techniques to detect any possible vulnerabilities in the target's operating system. Notably, this phase depends on the attacker's determination and the know-how of computing skills to perform reconnaissance activities; nevertheless, most of them are now automated (5).

3.3.2. Preparation Phase

To prepare for the attack, two different vectors or techniques are employed. First, deploying social engineering which demands time, knowledge of human psychology, language and culture. Second, successful computer exploitation which relies on "the sophistication of the malware used and the technical knowledge of the attackers to exploit possible vulnerabilities previously detected over the targeted computer systems" (6).

3.3.3. Attack Phase

After defining the target system's vulnerabilities, the attacker decides which accurate vector and the techniques to use; once all those elements are ready, the attack is triggered. After that, the attacker's objective is to obtain system credentials through malwares, backdoor or APT. After the passwords are acquired, an internal reconnaissance is prompted using sophisticated programs like Nmap, Dnsenum, and Dimitry; the aim is to know more about the victim's environment and decide what malwares or keyloggers to be installed. Furthermore, he could create new backdoors on multiple systems on the same network, create a VPN connection using legitimate credentials or authenticate on web portals. These acts must be performed silently to remain linked to the system for further exploitations.

3.3.4. Information Gathering

After ensuring the penetration of the system, the cyber-spy begins searching for potentially sensitive data like emails, images, databases and text documents. One crucial fact a spy should be aware of is language; it helps to identify and sort records based on their level of importance. Additionally, it is necessary to maintain the connection to the installed malware and keyloggers. They facilitate the capture of the victims' future activity and acquire more data.

3.3.5.Maintenance

To maintain the exploitation of the target system for an extended period, cyber-spies need to perform a maintenance operation. It is described as a check-up process to adapt to unexpected failures caused by exposing the threat on the part of the victim. As a consequence, it risks stopping any future attempts to extract data. The attacker's responsibility is thus to anticipate possible connection breakdowns and provide backup plans.

3.3.6. Information Leakage

After collecting all the information needed, the attacker transmits it using proxy networks, such as the Tor network (also known as the deep web) or through the backdoors created during the intrusion phase.

3.3.7. Information Sale

Cyber espionage is also a service to other parties interested in the stolen information or technologies. The importance of the data decides the price. The value of information rests in the hands of those who seek it.

3.3.8. Escape

This phase occurs for numerous reasons. First, the attacker escapes because the objective behind information gathering is achieved. Second, it is part of a new reconnaissance that requires more time to make thorough system check-ups. Third, a spy abandons the target system to conceal any committed espionage activity.

3.4. Cyber-Espionage Cases

The creation of the National Counterintelligence Executive after 2001 helped promote counter-espionage strategy. In 2008, a report declared the arrest of the Boeing engineer Dongfan Chung for espionage. When the FBI searched his house, they discovered about 250,000 documents about the US government. Furthermore, Jonathan Pollar was also arrested for providing Israel with 1 million documents during his career as a spy (Silick 291). Silick comments on both incidents as the consequence of “foibles of human spies”, and refers to the first small-scale cyber theft that dates back to the 1970s(292). The history of cyberespionage in the US echoes an evolving nature of threats associated with uprising world adversaries that aim to undermine the US economic, military and political primacy.

The end of the 1980s had witnessed the earliest proof of computer hacking for cyberespionage, as Silick states. The researcher at the Lawrence Berkeley National Laboratory, Clifford Stoll, exposed and determinedly traced the activity of an unauthorised user on the lab’s network. After collaboration with the German authorities, the hacker was identified and arrested. The cyber-spy was a member of a West German cabal that contacted the KGB to sell US defence and sensitive technological information, which resulted from their computer penetrations. To document this cyber-hunt operation, Stoll kept a daily log of his activities in what is known as The *Cuckoo’s Egg*, one of the early landmark studies of cyberespionage, as Silick points out (292).

The Moonlight Maze was one of the most damaging breaches on US soil between 1998 and 1999. It was reported that thousands of e-documents which contain confidential information about American military technologies were stolen. Newsweek said hackers skillfully broke into the Wright Peterson Air Force base. Then, they accessed military research institutions.US officials assumed that the enormous quantities of stolen data could include classified naval codes and information on missile-guidance systems. Though the hackers left approximately no traces of their origin, the Pentagon believes it was a Russian-oriented cyber-operation. Doubts about whether the intruders had abandoned the operation or their malicious activity went extremely deep in the target system and can no longer be traced? (We’re In).

From 2003 till 2007, the US's most critical infrastructures had received growing cyber-attacks known as Titan Rain. According to Norton-Taylor, the attacks, which caused minor administrative disruptions, were initially directed at the Pentagon and other US government departments. The disclosure of the episode was based on intelligent reports confirming the penetration of "the email system used by the network serving the office of Robert Gates, the US defence secretary", as Norton-Taylor states. Although investigations revealed the involvement of the Chinese government or any of its representatives; i.e, the People's Liberation Army (PLA), no compelling evidence was reached due to the complexity of the attack. The Titan Rains cyber-operations raised cautions about the perils of cyberspace, which can decimate physical and digital borders, i.e., firewalls.

4.Cyberterrorism and Cyberattacks

4.1. Cyberterrorism

Cyberterrorism has emerged as a new threat to nation-states and their societies. Unlike traditional terrorism, cyber terrorists are believed to incorporate cyberspace as a medium to engage in attacks aimed at disseminating fear and instability. Their acts are supposed to challenge "how nation-states define their interests, power bases, security, and increasingly, their innate ability to govern and control flows of information" (Virkar 30).

In the US context, government officials and experts provided provisions for cyber-terror based on two analogies which simulated the Cold War threats. Because of the lack of "a real-world reference" to such attacks, Cavelty claims that the use of specific language and words contributed to dramatising the actual threat and made it possible to reconsider it as a priority to national security.

The two dominant analogies that approached cyberterrorism as a real threat were the "electronic Pearl Harbour" and "weapons of mass disruption". As early as 1991, the prevailing cyber-security debate in Congress warned against possible cyber attacks on critical US military infrastructures initiated by non-state actors. These attacks, as Cavelty states, disregard the vision of geographic invulnerability and assert the dangers of foreign threats. The second analogy tackles the nature of cyber threats as deadly weapons. Accordingly, their impact is believed to be similar to mass destruction weapons. This explains why cyberterrorism has been placed at the top of modern threats to the American way of life (131).

4.2. Forms of Cyberterrorism

Cyberterrorism is considered a complex threat to the national security of nation-states. This can help to explain its areas of influence. A study of various cyberterrorism scenarios by Foltz, listed many possible targets, such as: “interfering or disrupting information and communications networks, infrastructure systems, banking and finance systems, transportation systems, emergency services, and government services” (5). Foltz adds that these forms of attacks are thought to be “politically motivated”. Likewise, they are intended to cause political, economic, or violent disruptions. (Foltz 5).

As for real examples of cyberterrorism, Foltz states that “documented instances of cyberterrorism have not occurred in all the forms…” (5). Comparing the 9/11 attacks, it can be noted that cyberterrorism effects lack the subsequent results, such as damaging physical infrastructure or having people killed (Desouza and Hensgen qtd. Foltz 5). Furthermore, the presumed link of cyberterrorism to non-state actors limits the consequences of their attacks due to either lack of technical capabilities or intelligence about the potential targets.

4.3. Preventing Cyberterrorism

The fact that cyberterrorism is a form of computer crime or misuse implies the use of sophisticated technological methods to disrupt targets and exploit systems vulnerabilities. Such technical similarity explains why Kuong’s taxonomy was established (Foltz 7). The taxonomy aims to distinguish between various sources of misuse. Notably, the main element in the taxonomy which reflects the changing aspects of the current threat is defined by Foltz as "the enemy within/without refers to collusion between external individuals (the enemy without) and internal personnel of either a non-technical nature (the enemy within) or technical nature (the enemy within/within)" (Foltz 7). As far as foreign threats are concerned, the early-mentioned element accentuates the idea that attacks originating from a foreign location are difficult to thwart.

4.4. *Cyberterrorists: Methods and Tactics*

Terrorists' manipulation of cyberspace is restricted to information gathering to perform attacks on physical targets. Because they are described as loose groups, their tactics should be consistent with how they are organised. Mehan argues that the terrorists are networked into smaller units, allowing them to attack and disappear quickly, leaving a certain amount of disruption. Furthermore, it is noticed that terrorists patiently engage in "pre-attack surveillance over extended periods to gather information on a target's patterns and exposures". Moreover, those tactics are gradually evolving to meet their goals. For instance, finding and exploiting vulnerabilities has increased in speed and cost. Consequently, terrorists, in the real world, can take advantage of cyber-reconnaissance to plan efficiently and then strike multiple targets at lower risks (Mehan77-80).

5. Cyber Warfare

The fact that wars are bound by the context of their age clarifies why warfare techniques have evolved over time. The narrative of human history showed that conflicts are not only determined by the used weaponry but also by the motives of wars, such as political and sociocultural factors. Moreover, the emergence of social structures contributed to establishing central states and institutions, facilitating the growth of constant military installations. In response to modern challenges imposed by the information age, warfare defensive/offensive techniques have been revolutionised to encounter cyberspace threats (Mehan).

5.1. Definition

Cyberwarfare connotates the shift of conventional war techniques to cyberspace or interstate war. Mehan argues that some experts question the validity of this claim for numerous reasons. Firstly, the Geneva Convention, in articles 7 and 51, accentuates the protection of people in times of war; protection includes medical assistance and banning certain weapons (‘International Committee of the Red Cross’). Cyberwarfare is thus assumed to lack features exhibited in real-world wars, such as casualties or any other form of protection of civilians. Secondly, the proposition of an existing cyber war has not yet been experienced. Regarding the immediate outcome of any war, Mehan argues that Clausewitz’s definition of war, being an act of violence, has not been fulfilled. Furthermore, Mehan considers the disruption of physical infrastructures as a secondary effect of cyberattacks. Thirdly, conventional wars are dependent on lethal weapons; however, cyberattacks incorporate digital tools like codes, DDoS attacks and data breaches. Mehan states that experts are uncertain whether to consider those tools a weapon (62-63).

To solve this issue, some experts, such as William Gravell, believed in the non-existence of cyberwars and proposed a cyber component involved in real wars. To illustrate, many real battles witnessed the introduction of a known component like planes, missiles or any technology that could give an advantage over an opponent (Mehan 62-63). Similarly, modern warfare is believed to utilise cyberweapons in parallel to conventional ones.

However, recent cyberattacks, which targeted countries’ infrastructures, launched a series of debates over the issue of cyberwarfare and weaponising cyberspace. In 2017, Russia was alleged to launch cyberattacks against Ukraine, which caused massive damage to its economy; as Greenberg states, “the cyberweapon NotPetya […] It quickly spread, paralysing major companies, including FedEx, Merck, and Maersk, the world's largest shipping firm. Ultimately it caused more than $10 billion in damage” (CBS news). Variety of responses to this incident considered that such intentional attacks are similar to military ones. Others accused Russia of “undermining democracy, wrecking livelihoods by targeting critical infrastructure, and weaponising information”. According to what has been stated earlier, it can be said that cyberspace is increasingly perceived as another sort of warfare, in which responsibility can be denied in most cases, as Dmitry Peskov, President Vladimir Putin's spokesman, commented (CBS news). In cyber warfare, asymmetric opponent(s) can be visualised depending on emerging real-world powers.Additionally, US officials are worried about the kind of competition in which cyberspace becomes one of its fields. Their argument is based on the idea that new adversaries have emerged and the probability of forcing a cyberwar that they regard as a threat to the US national security.Furthermore, officials’ fear of a potential cyber war is related to the kind of easily acquired cyberweapons. For instance, the Stuxnet is a cyberweapon. Apart from its binary nature, it caused physical damage to the Natanz nuclear station. According to National Geographic, the fear that other adversaries may acquire the technology to attack the US (03:15–05:21).

5.2. Classifications of Cyberwarfare

Understanding Cyberwarfare means knowing about its manifestations. Thus, Mehan classifies this cyber battlefield into four classes. First, as the lowest conflict grade, class I cyberwar is concerned with personal information protection. However, the impact of this class on national security can be devastating. Second, Class II cyberwar tackles the issue of economic and industrial cyber-espionage. At this level, experts state that threats focus is on “nations, corporations, universities, or other organisational structures”. Third, class III cyberwar, as Nehan clarifies, is “officially about global war and terrorism, which includes cyberterrorism”.Additionally, this stage may attack other parts of the critical infrastructure.

The involved parties can be state or non-state actors utilising different cyber-tools to achieve the intended objectives. Fourth, class IV combines the techniques in classes I-II-III and military activities. The aim is “to obtain a battlefield advantage or a force multiplier” (63-64).

The concept of cyber warfare is, therefore, an information-based struggle between different actors. Furthermore, this concept suggests the violation of states’ sovereignty. Yet, states are expected to find measures to compel threats.

6.Major Attacks in Cyber History

6.1. The Cyber Attack on Estonia 2007

Estonia, a former Soviet country, witnessed massive cyberattacks in April and May 2007. The state’s major institutions and services were paralysed for about three weeks by Distributed Denial of Service (DDoS). The consequences of the attacks were considered catastrophic. Cyberattacks forced Estonians to experience an information blackout. This led to “profound economic and potential social consequences, and in the case of an attack of longer duration would have been of strategic consequence to Estonia and the hitherto solid perception of it as a safe and stable place to do business”. Economically, the disrupted banking systems were never accidental. Estonia is described as an internet-dependent country. Therefore, depriving people of performing instant financial operations could indulge them in a state of turmoil. The events exposed a Russian involvement, which was driven by political motives. The Estonian crisis depicted how cyberwars can be devastating if the cyber element is involved. Furthermore, cyberweapons can be a soft instrument to send political messages to opponents, prompting more defensive and offensive national security measures (Schmidt).

6.2.The Cyber Attack on the US in the Middle East 2008

Cyberattacks are believed to be an extension of real-world wars. The existence of US troops in Afghanistan initiated a series of cyber operations against it. Thus, the 2008 attack on US military computer systems was regarded as the most significant act of intrusion, as the former Deputy Defense Secretary William Lynn stated. The infiltration of such critical infrastructure was unintentionally executed by a within-actor, a soldier at the Camp Clark military base in Khowst province, Afghanistan. According to Lynn, the system was hacked due to a flash drive infected with a code that “spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead from which data could be transferred to servers under foreign control” (Stewart).

The 2008 cyber-attack was significant because of the acquired data from critical military systems and the tactic used; i.e. the counterfeited hardware. Counterfeited hardware refers to computer chips where malicious codes are written; they aim to facilitate remote access to information through their backdoors. The breach of 2008 was done based on such tactics. This issue was regarded as a threat to national security since the US computer systems might contain such malicious hardware. Consequently, US officials called for promoting national defence strategies to encounter such forms of threats. Lynn said that “the attack was a wake-up call for the Pentagon, which has since launched a Cyber Command and taken measures to bolster defences”. The attack had also initiated discussions about encouraging national industries in the field of high technology as a way to promote national security. Equally important, Lynn commented on the reaction of the US government, saying that “The U.S. government has only just begun to broach the larger question of whether it is necessary and appropriate to use national resources, such as defences that now guard military networks, to protect civilian infrastructure” (Stewart).

6.3. The Cyber Attack on Saudi Arabia 2012

In August, a Saudi petrochemical plant was targeted by a new kind of cyberattack. According to investigators, the attack was designed to wipe data or shut down the plant and to “disrupt the company's operations and cause an explosion” (Perlroth and Krauss). The earlier claim was based on the previous incident in China and Mexico. Although no cyberattacks were involved, the consequences of the chemical blasts were devastating; several employees were killed, and hundreds of injured people were evacuated.

The examination of digital evidence exposed how hackers could infiltrate the plant. After inspecting computers in different workstations, an odd digital file was found. At the first glimpse, the file was regarded as part of the Schnyder’s controllers, a company that designs systems to control electro-valves. The file was designed to allow remote access to the facility and sabotage the system. Unexpectedly, the facility’s production systems were shut down due to hackers’ codes malfunctioning.

Despite the offenders' identity and profits, the attacks on Saudi Arabia's critical infrastructure have projected the probable damage that modern cyber warfare can achieve. Under those circumstances, the international actors, mainly the US, have started to worry that the attacks could be replicated in other countries. Hence, posing future threats to its national security as James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, points out, “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).

6.4. The Cyber Attack on USA 2012

In the spring of 2012, many American banks were under massive attacks. Hackers could seize world servers to orientate huge traffic and deface banks’ websites. They were believed to be triggered by Iran after receiving more economic sanctions. These digital assaults disrupted any consumer/bank connection, causing banks to suffer significant losses.

Nakashima stated that the debate over this episode resulted in technical and political responses. The Obama administration rejected the proposition of offensive attacks; they would be considered a violation of Iran’s sovereignty. Instead, it favoured technical and diplomatic actions because the attacks did not reach the threshold to mobilise offensive capabilities. Therefore, 120 countries were asked to separate the traffic locally and “remove the malicious computer code from the servers around the world being used as springboards for the attacks” (Nakashima).

Despite their devastating consequences, cyberattacks can act as a soft power to force countries to change their policy. The Obama administration accepted to sign an agreement with Iran concerning their nuclear program. In addition, international cooperation advocated diplomatic solutions to encounter evolving cyberthreat.

6.5. The 2016 Elections: The Russian Meddling in US Elections

The Russian meddling in the 2016 election dominated the American political scene. According to Abrams, the significance of the Russian cyberattacks revealed how IT can disrupt the principles of democracy by manipulating the masses.

The evidence provided by Special Counsel Robert Mueller exposed how the Russian cyberattacks had altered the course of the election. Based on intelligence reports, attacks started by probing voters’ databases over different states, hacking and releasing politically damaging information about Trump’s opponents, mainly Hillary Clinton, and spreading propaganda on social media to support Trump.

After Trump had won the election, investigations continued and were backed up by more physical evidence. Trump’s campaign advisers were involved in meetings with Russian officials. For instance, Papadopoulos, a foreign policy adviser to the campaign, was found guilty of denying Russian contacts. As for Trump, he was allegedly criticised for collusion with Russia for economic benefits. However, no solid evidence was presented against him. Trump could have been in trouble if there were clear signs of Russian influence on his public policy decisions (Abrams).

Indeed, the US elections of 2016 are a credible example of how cyberspace can act out of borders to disrupt and alter politics softly yet, demonstrate a new challenge to national security strategies.

Chapter Three: Digital Diplomacy

Introduction

The context of world relations is increasingly getting complicated due to significant cyber threats. For countries like the United States, those threats have been presented as a challenge to their values and cultural features. As a matter of effect, Biden's administration has taken responsibility for restoring the US brand, which has dramatically diminished due to former external political practices.

The increasing hostility against the USA can explain the enormous amounts of cyber-attacks. Accordingly, Biden has employed cyberspace to empower public diplomacy to reduce tensions and promote world partnership. This kind of diplomacy is known as digital diplomacy, influencing cyber-entities through soft power.

1. Digital Diplomacy: a Controversial Notion

Diplomacy is "the conduct of relations between states and other entities with standing in world politics by official agents and by peaceful means" (Bull qtd. in Bjola 16). This definition, thus, addresses the nonviolent approach toward international partners. However, the current nature of conflicts has been revolutionised due to the increasing reliance on cyberspace. As a result, state and non-state actors' interrelations have taken a digital form, posing new challenges. Accordingly, it is noticed that the practices of diplomacy in the physical world have found their way into cyberspace. The result of such notional migration generated a set of concepts such as cyber-diplomacy and digital diplomacy. Though they have often been used interchangeably, Riordan distinguishes between the two terms. He defines cyber-diplomacy as using diplomatic tools like deterrence, soft power, and economic sanctions to resolve or manage cyberspace problems like cybersecurity issues. As for digital diplomacy, Riordan proposes that "it should refer to the use of digital tools to pursue wider diplomatic objectives" (Riordan 5). Digital tools such as Twitter and Facebook have been effectively utilised to gain political support, spread an idea, or even fake news. The common feature of those tools is that they are cyber-based platforms. Furthermore, digital diplomacy results from "the recent conceptual and empirical developments such as public diplomacy and soft power" and technological innovation (Bjola and Holmes 88).

2.Theoretical Beginnings of Digital Diplomacy

To understand the underlying theories that initiated digital diplomacy, it is better to consider the following definition by Holmes: it is a "strategy of managing change through digital tools and virtual collaborations" (51). The practice of digital diplomacy and specific social media tools have emerged to influence others peacefully through the power of the image. The emphasis on digital diplomacy received today reflects the role of technology in this field.

2.1.The Realist Approach

Two main thoughts recognise the realist approach to world politics: self-interested states are the most important actors, and the state of anarchy is the governing principle of the international system. For realists, world politics is never static because it is naturally conflictual; therefore, their vision of world relations is consistent with less cooperation and imminent wars. Furthermore, this approach regards technological change as an aspect of power which can shift depending on the state or other entities. These unchanging assumptions can explain the changes in the world's powers, consequently impacting cyberspace. For example, though the United States pioneered the technological stage, other units and states have emerged as a threat. Accordingly, Potter refers to the state of shifting roles as "the play of power politics". He asserts that performers are subject to change, "but not the stage upon which that play is performed". Worldwide politics will witness further actors and power distribution changes instigated by technological revolutions, notably cyberspace security. (Potter 41-42).

2.2. The Liberal Approach

The Peace of Westphalia in 1648 represented the first political and territorial division by which the concept of sovereign states arose. Within those territories, states enjoyed the peace and good life as Potter states; however, the outside projected instability and anarchy; it is argued that sovereign states share the same features by which the Westphalian international system is formulated. To settle conflicts, liberals believe that the external anarchy can be overcome by time, legislation and establishing international institutions that organise world life, as Potter points out. Indeed, managing world relations benefits individual states, the group and the whole system. Liberal traditions are therefore sought to push history's direction toward modernisation and progress (43-44). Moreover, liberals believe in the accountability of modernisation, and developments in communications, in particular, to diminish the international system's persistent insecurity in several overlapping ways. Remarkably, the promotion of internal security is assumed to be an essential characteristic of Westphalian states. These states have enjoyed "a zone of peace" due to economic globalisation and supra-natural we-feelings. On the contrary, it is noticed that globalisation "cannot generate a meaningful sense of communities," as Deibert states. As a reaction, these communities naturally tend to develop internal religious or ethnic-based identities.

In addition to globalisation, Deibert emphasises the importance of communications for liberal democracies. It is the means through which Westphalian-states maintain interaction and exercise influence on states in the international system. Evidently, the changing goals and nature of communication explain why liberals consider it an inevitable ideology. Although liberalisation and globalisation are meant to achieve prosperity, Deibert confirms that they have side effects, such as chronic unemployment, violence and crumbling health infrastructures, which do not manifest appreciation of social variables (34).

2.3. The Marxist Approach

The Marxist approach, unlike the liberal one, stresses the idea that changes in communication technologies are indebted to the productive forces in societies. In the context of world relations, Deibert states that the literature of Marxist theory does not share the same view of how the economic class determines the socio-political ties. These different views are due to their position in communications and world politics. Firstly, theorists whose focus is on the media owners and how they exercise control over its content. A classic example of this theory is Noam Chomsky's Propaganda Model. Chomsky suggests that money and power drive the content people watch, therefore, influencing them. Deibert states that the content should not be viewed as part of the conspiracy to influence others , but to unveil the systemic factors that structure news to serve capitalists' ambitions. Secondly, theorists whose attention falls on "the structural constraints which are the result of transnational capital and global communications" (35). The latter is supported by the neo-Marxist, Antonio Gramsci. Unlike the first view, Gramsci is interested in the modes of power and capital that apparently can shift and cross political boundaries because of communication technology (36). Thus, dominant cultures disseminate over others peacefully, not imposed by the elite capitals. Neo-Marxism gives account to the current economic changes driven by political motives. Indeed, the relocation of power and structures of influence has considerably increased with the internet. The World Wide Web has turned individuals into a global audience, spreading cultural models and forcing them.

2.4. The Medium Theory of Communication

The evolution of technological communications has dramatically impacted international relations. Thus, the Medium Theory of Communication revelations traces the changes in societies and politics. Harold Innis and Marshal McLuhan, tenets of this theory, propose that “changes in modes of communication such as the shift from primary orality to writing or the shift from writing to electronic communications-have important effects on the trajectory of social evolution and the values and beliefs of societies”(Deibert 38). This theory stresses the value of media as an environment that requires more study in terms of time and space. In contrast, the changes in societies mirror the rate of change in communication technologies.

The application of the medium theory on international relations contributed to defining the influencing policies and how social units have thrived in the digital space.

2.4.1. Transnationalization of Production

Producing goods on state-territorial boundaries has now been dispersed to the international level. Traditionally, transactions with other countries and vice-versa were regarded as an arm’s length variety. In the hypermedia age, countries are more dependent on the diffusion of production chains across territorial boundaries for several reasons like low labour costs and favourable regulatory climates (Deibert 40).

2.4.2-The Globalization of Finance

It is assumed that the transmogrified financial activities have led capitals to move worldwide, consequently influencing world politics. Deibert suggests that “central state authorities are increasingly bound by the dictates of the market, as the numerous changes in the direction of the privatisation and liberalisation across the world indicate” (41).

2.4.3. Transnational Civil Society Networks

Technological forces are viewed as necessary as the global market; yet, accompany one another. Within the sphere of digital networks, social units have emerged, such as activists, militia movements and terrorists. The common feature of these units is that they lack a significant decision. Deibert adds that these social structures have an interstitial influence, the power to influence the margins and specific areas (41).

2.4.4. Postmodern Mentalities

The postmodernist thoughts of scepticism of truth, plural worlds and multi-perspectivism have flourished in the age of information technologies. Thus, cybernauts and web surfers emerged as a simulation of the physical world's multiple realities and plural worlds. Derteit describes teenagers in the digital world as comfortable with the Derridean and Baudrillardian modes of thought (42).

2.4.5. International to Intra-planetary Security

The age of technological communications has brought security challenges like inter-state wars (Deibert 42). New technologies like ballistic missiles and nuclear weapons depict the escalating fear of devastating wars. Consequently, the world has arrived at a state of insecurity where superpower expansion increasingly threatened world peace. Furthermore, the state of insecurity has also taken a different shape because of the digital space. World security is not only about territory but about data, privacy, sensitive data protection, cyberterrorism and cyberwars. These threats urged states to take further precautions and organise the new space into what is known as cyber-governance.

3-WikiLeaks and Diplomacy in the Digital Age

Cyberspace and diplomacy can merge to promote US values across the world. However, cyberspace can again be a threat because it can contribute to a second WikiLeaks. In 2011, Johnson discussed the disclosure of sensitive documents in the name of freedom of speech after the involvement of a famous newspaper. Furthermore, she highlights both the benefits and drawbacks of documents leakage in diplomacy. She argues that such acts help in shaping an overall image of diplomacy and diplomats. On the other hand, she considers the leaks a potential danger to diplomats.

Actually, minimising the number of future disclosures of sensitive information is problematic. This is consistent with security measures set to encounter various cyberattacks.

4-Diplomats Role in Cyber Conflicts

Professional diplomats can play a role in mitigating the consequences of cyber conflicts; they can keep channels open while their masters cannot. However, their efforts with non-state actors are complex. Riordan suggests that diplomats have to try to socialise those actors and reach an agreement with the powers that drive them. For instance, during the Cold War, both sides used surrogates to fight for them against the other; however, channels were open always to reach an agreement.

During cyber-conflicts, a diplomat must identify areas of common concern to establish a conversation about a particular theme, such as cyberterrorism and avoiding anarchy. Because of the increasing reliance on the Internet of Things, states have become more vulnerable. Accordingly, their definition of the term terrorist remains controversial. For instance, in Russian and Chinese contexts, a terrorist is defined as a local opposition, violent or not. This example echoes the existing notional barriers between nation-states; therefore, conversations are more likely to occur. More importantly, both countries avoid causing cyberspace anarchy where all is against all.

While conducting a conversation, cyber-diplomats have two imperative cautions to consider. Firstly, cyber-diplomats have to work on attracting and socialising states in the world community of cyberspace and not exclude them. Definitely, excluding a state would free it from the limitations of world agreements, consequently generating a rogue entity rejecting cyberspace norms like North Korea. To further explain this issue, major players in the physical world agree on a set of rules and standards of behaviour. They also tend to accept limitations if they promote their security. For example, the Cold War was described as an era of mutual mistrust; however, none of the rivalling states used nuclear weapons against the other due to the signed agreements.Similarly, cyberspace is assumed to undergo the same codes of conduct. In 2015, President Obama and Xi Jinping set an agreement where China stopped intellectual property theft from the US. Secondly, cyber-diplomats have to be careful of Western exceptionalism. Riordan states that Western countries like the United States are endowed with the right to bypass the limitations of international law when their interests are threatened. To illustrate, the intervention in Iraq, and Libya, using drones to assassinate ISIS leaders in Iraq and Syria, and supporting pro-democracy groups in Russia were done without international cover. As a reaction, other countries have developed their own exceptionalism, such as Russia's attack on Georgia, the annexation of Crimea and the recent war on Ukraine. Likewise, it is noticed that Western exceptionalism can transcend cyberspace. The US attack on Iran's nuclear facilities, using a cyberweapon called Stuxnet, was considered an act of war. This cyberwar provoked the Iranians to develop their own cyberspatialities and encourage cyber-proliferation (74-77).

Cyber-diplomats' effective management of cyber conflicts depends on the international community's willingness to abide by international norms and constraints, though morally, they appear to be frustrating.

5. The Intersection of Foreign Policy and Digital Diplomacy

As a mechanism to manage global change, cyber-diplomacy relies on the amount of information generated by the government. In the US, the debate over the role of the National Security Agency (NSA) and the Snowden incident emphasised the enormous cyber-activities undertaken to extract information from foreign sources. Accordingly, the

Guardian demonstrates how the NSA could gather more than 14 billion reports only about Iran. On the hand, WikiLeaks' publication of 1.7 million US diplomatic reports in 2013 reflects the role of diplomats in information gathering.

The information age is accompanied by "information overload" or "data asphyxiation", which requires thorough analysis. The use of information systems, which transcends human capacities, provides visual analytics and quick data processing, consequently eliminating the interference of the practitioner's psychological factors and limited cognitive abilities of practitioner's information (Arias-Hernandez et al. qtd. in Bjola and Holmes).

Furthermore, utilising digital tools in the sphere of diplomacy is viewed as a promising approach. It helps in "detecting changes in the foreign policy preferences, moods and attitudes of distant publics at the population level" (Bjola and Holmes 73-79). Therefore, the US is assumed to implement cyber-tools to monitor people and entities' attitudes throughout cyberspace; and, subsequently, direct cyber-diplomacy efforts to be consistent with foreign policy preferences. Sheldon Himmelfarb, a former policy adviser, argues that:

> "Over the last three years, the U.S. Defence Department, the United Nations, and the CIA have all launched programs to parse the masses of public data now available, scraping and analysing details from social media, blogs, market data, and myriad other sources to achieve variations of the same goal: anticipating when and where conflict might arise. The Defence Department's Information Volume and Velocity program is designed to use "pattern recognition to detect trends in a sea of unstructured data" that would point to growing instability. The U.N.'s Global Pulse initiative's stated goal is to track "human well-being and emerging vulnerabilities in real-time, in order to better protect populations from shocks." The Open-Source Indicators program at the CIA's Intelligence Advanced Research Projects Activity aims to anticipate "political crises, disease outbreaks, economic instability, resource shortages, and natural disasters." Each looks to the growing stream of public data to detect significant population-level changes" (Himelfarb qtd. in Bjola and Holmes 73-79).

Moreover, it is noticed that cyber-diplomats would incorporate cyber-tools to measure the effectiveness of a specific foreign strategy in real-time. Through programs and algorithms embedded in social platforms and websites, researchers can enlarge the sample's size worldwide and investigate reactions to particular issues. Yet, this method of data collection can be biased. Bjola and Holmes argue that specific foreign policies cannot be addressed publicly; hence little data is to be analysed. Additionally, the validity of data collected about a specific issue is constrained in terms of time and its linkage to clear policy leaders; i.e, it becomes useless when variables change.

6. Social Media and Digital Diplomacy

The information revolution has impacted the field of diplomacy mainly after integrating social media to influence international politics (Stein and Seib qtd. in Bjola and Holmes 163). The ability of social media resides in transcending hierarchal chains of diplomatic communications and encouraging people to engage in political life and make their voices heard. Furthermore, it also enables diplomats to engage in familiarisation with foreign publics. These significant shifts and implications are primarily responsible for social media's status as a powerful symbol of the 'new public diplomacy'. Diplomats now have the ability to transmit insights of their original societies to other nations peacefully.

US politicians like Hillary Clinton emphasised the urgency to promote world relations. She addressed the need for influencing people through the digital age. Resorting the reputation of the US and its diplomatic power were the main issues Clinton sought to achieve as part of the foreign agenda. In contrast, Biden's view was different. He considers it a cyber threat to American society. These threats include banning ads targeting children, people's mental health and disinformation, especially during COVID-19 (McCabe). In 2020, Facebook, Twitter and YouTube were criticised for disinformation. The New York Post published a story that contained supposedly convicting documents and pictures taken from

Biden. Though there were debates over the incident's authenticity, social platforms reaction was not acceptable. "While YouTube largely did nothing, Facebook deprioritised the Post story, and Twitter initially moved to ban all links to the piece on its platform", as Roose stated.

7.Dimensional Framework of Digital Diplomacy

Integrating cyberspace aspects in the field of diplomacy is believed to empower the diplomatic efforts toward world actors. This empowerment can be noticed in different dimensions, such as "the institutional structure of diplomacy and diplomacy executives" (2) as

AKTAŞ states. The first level of influence can be spotted in the "change and transformation of diplomatic norms and customs" (2). The former US President Donald Trump is thought to be a clear demonstration of this influence. Though he received much criticism for his inappropriate diplomatic behaviour, Trump's Twitter diplomacy demarked a portent change in the diplomatic institutional structure due to the digital age. The second level of influence contributed to enhancing diplomatic executives by providing solutions to new challenges., political leaders can face new challenges and reach a large audience. It is also essential to consider another unfolding dimension, the method of execution of diplomacy. This method has been influenced due to events acceleration. AKTAŞ argues that "nowadays, with the effect of the pandemic, the density of online conversations has increased, and digital technologies have started to be used more frequently in diplomacy" (2).

8.Biden's Urgent Plan to Enhance Cybersecurity

Biden's inaugural speech is considered a cornerstone for enhancing national security strategies. His focus on critical issues, mainly the securitisation of the digital realm and its role in international relations, has been translated into launching a new bureau of cyberspace and digital policy. According to the Secretary of State Tony Blinken, this new structure " will provide us with greater leadership and accountability to drive the diplomatic agenda with the interagency and abroad, and build on the extraordinary work already taking place across the Department”. Blinken’s announcement accentuates an urgent need to change foreign policies due to persistent cyberattacks from foreign actors (Atwood et al.).

Biden’s step towards modernising state departments’ work was believed to be an extension of Trump’s strategy in his final days. Unlike Trump, whose move was rushed and unplanned, Biden seemed confident and informed as his strategy addressed a set of vital issues such as “cyber threats, global internet freedom, surveillance risks and working with democratic allied nations to set international norms and standards on emerging technologies” (Miller).

9. Biden’s Interim National Security Strategic Guidance

The recent cyberattacks on the US have urged the White House to consider cybersecurity a top priority which necessitates military and diplomatic solutions. “We will elevate cybersecurity as an imperative across the government. We will work together to manage and share risk. We will encourage collaboration between the private sector and the government to build a safe and secure online environment for all Americans” (House).

To build a safe digital environment, Heckman points out that the federal government seeks to increase cooperation with the private in computer technologies and raise the necessary financial budgets. Such procedures aim to “increase network visibility and mitigate future cyber incidents”, as Anne Neuberger, the administration’s deputy national security advisor for cybersecurity and emerging technology, stated in a press briefing. Furthermore, the guidance provides an opportunity to assert the value of diplomacy to the American public. His claim infers the reinforcement of the internal agencies, which would contribute to foreign affairs (Heckman).

10. Biden’s U.S National Security Strategy

Biden’s administration, like former administrations, seeks to craft its national strategies that reinforce the US competitive aspect and its leading role. On his first day, Biden signalled this idea, emphasising that China, Russia and other state-actors have been disturbing and destabilising national peace. Experts believe that the new strategy is unique because it is shaped by “learned lessons” from previous national strategies. According to Lettow, Biden’s national plan ought to echo the essence of former strategies, which took into consideration new challenges to the interests of that era. Moreover, Lettow points out that the importance of strategic planning and processing contributes to an overreaching strategy which, he adds, should be classified in nature. Because of the damage classified information can achieve, Lettow states that officials decide what content can be unclassified and how to convey it to the public (Lettow 151). It is viewed that Biden’s decision to withdraw troops from Afghanistan and his contribution to reaching an agreement with the Taliban demarked his obligations towards securing international, and national interests, as the debate had elevated due to financial costs.

10.1. The Role of The White House

The debate over the role of the White House in promoting national security strategies prevailed on the political scene on both levels, nationally and internationally. Recent history showed that the escalating challenges demand more engagement from the White House. However, the engagement level must be consistent with other US administrative apparatuses. Lettow clarifies that for the White House to restore its prime role, Biden’s administration should work on resolving fundamental differences with other partners such as the National Security Council. Hence, the likelihood of executing the strategy will be increased due to the united efforts and the atmosphere of mutual understanding (Lettow 152). Biden’s actions demonstrate how the White House could influence other constitutional agencies to serve his cybersecurity agenda by issuing financial budgets or legislative orders.

10.2. Engagement in Foreign Matters:

Another aspect of Biden's strategy is his engagement with geopolitical matters, which the US has always been concerned with. Foreign challenges to US interests have developed in terms of nature and state-actors. Lettow argues that the current administration is endowed, by history, the right to defend its space of influence, not only physical but also in cyberspace. Therefore, the US has to adjust its strategies accordingly to keep influential, not only at the level of geography but also in world organisations like WHO (152). For instance, the post-COVID-19 era is viewed as the stage of restoring the US role over China. Consequently, it has promoted health strategies to fit future pandemics. Additionally, it encouraged more cooperation with overseas partners like the European Union and the Americas, as Biden stated in June 2022 (U. S Department of State).Furthermore, other signs of the president's lead are seen during the Russian-Ukrainian War. Despite the voices criticising the US financial status, Biden urged the Congress "to immediately' pass $40 billion Ukrainian aid bill" (Judd et al.). The statement "Get it to my desk in the next few days" indicates how the power White House has increased in security matters and how democratic practices of Checks-and-Balances cease to work when the US, the democracy guardian, faces immediate global challenges and judgements too.

10-3-Adversaries Analysis

A successful national strategy also incorporates rigorous analysis of competitors and the United States. The rise of new powers urges the states to conduct a thorough action plan to know about the capabilities of the rising powers. Lettow argues that this process is important for building a long-lasting strategy. He maintains that Biden's administration ought to analyse the motives, interests, objectives and the underlying methods by which those competitors achieved supremacy in certain areas (153). By taking the example of China, the analysis then tries to explain the military, economic, political and technological motives that have made China an adversary.Consequently, the US officials can draw an overall image of the possible threats the adversary can deliver and how to deter them. Lettow argues that this analysis is paramount to the national security strategy as it contributes to the development and prioritisation of US policy objectives. This explains why Biden's administration has set measures to encounter the Chinese and Russian expansion in both physical and digital realms. The cyber-threats that the US is undergoing have indicated how those countries surpassed the American capabilities. As a response, governmental and private sector agencies have considered the president's call to reinforce the digital borders, as Biden stated (Gill). This step is vital to avoid the woes of cyberattacks and their drawbacks to the US economy. On the other hand, the attacks on the US designated how vulnerable the country can be. Lettow claims that the president's administration should assess measures to examine the country's weaknesses and strengths and then compare them to the competitors (153).

10.4. Technology and Soft Power

Biden's administration approach to soft power is believed to tackle transnational issues such as cybersecurity. Lettow claims that the administration should carefully consider the different factors and elements of power that interfere in the area of cybersecurity; and therefore, influence the outcomes that best suit the US interests (154).

The fact that cyberspace is borderless, the current administration has encouraged world cooperation. Indeed, the supervision of the US at a world summit which discussed possibilities to prevent and stop cybercrimes reflects the heritage of hegemonic power (Katulis). The question is how the US can use the heritage, which is economically based, to exercise its influence through cyberspace. Statistics show that the influential American technology companies hold an enormous share in the world market: “the Microsoft Windows operating system holds 92%, while Apple's Mac OS accounts for about 6% and Linux settles with a meagre 14%” (Bejarano 3). Though the complaints about the functionality of those systems in terms of security, commercial entities keep influencing the space, accompanied by the empowerment of the US model in nations’ psyche. As a matter of fact, experts expect more cyberattacks on the US national and international interests. Thus, the current US stakeholders are working to secure the digital space since it is another scope of influence.

The Security of cyberspace is considered another strategic pillar of a national policy. As a strategic cyber-tool, search engines have to be protected due to their influence on perception ideas. Bejarano claims, “It is a way of applying the soft power.
Nye mentioned,”. The practicality of search engines resides in its dependence on open-source algorithms that can “return results to the users by indexing over one trillion Internet addresses”. Consequently, Google, for instance, can decide about users’ preferences and archive them in central servers in the US. This unprecedented feature is used in other digital platforms for different reasons. Surprisingly, the same feature can be used in disinformation campaigns such as the US elections of 2016, when technology influenced voters’ choices.

The importance of this feature and other key technologies has triggered a status of unofficial distrust. Stemmed by the effects of technology on the states ‘sovereignty, China wanted Google to censor data on its territory. This demand was accompanied by cyberattacks on Google, which “relinquished and relocated its servers in Honk Kong” (Bejarano 4). Regarding national sovereignty, experts state that Google lost its control over China in favour of Baidu, a genuinely Chinese-made search engine (4).

11. Benefits of Digital Diplomacy

Today, digital diplomacy has become an essential matter of foreign policy. Its increasing importance is the consequence of "state and non-state entities which compete for influence and power in the same online space" (Adesina 10-11). Based on recent statistics, more than 3 billion people regularly have internet access, most of whom utilise mobile phones. *Without a doubt*, proper use of digital diplomacy would help countries promote their foreign policy and reach the outlined objectives. Moreover, because it is digitally based, states can influence cyberspace and expand their international reach to almost all connected entities (Lowy Interpreter qtd. in Adesina 10). Hence, Adesina points out that social media are of great assistance as they permit countries to reach their citizens in real-time. Besides, they further diplomatic objectives when they act as space for interaction about prevailing issues.

The availability of social media tools and their accessibility render them one of the most effective tools that embassies and government offices incorporate. Adesina argues that these social platforms are dynamic in that they allow more access to content such as "videos, photos, and links, than traditional methods of giving lectures or passing out pamphlets, images or even conduct surveys" (11). One other feature social media provide is that they facilitate the reach of youth populations worldwide to help them integrate with their countries of origin.

It is claimed that digital technologies are helpful in various fields such as public diplomacy, information collection and processing, consular activities, and communications during emergencies and disasters. *Additionally,* Adesina notes that "the international practice shows that competent use of digital diplomacy tools can bring big dividends to those who invest in it" (11).

At the level of the working groups, it is assumed that digital diplomacy cannot replace traditional diplomacy. Instead, it reinforces it. This diplomatic tool can advance states' efforts within the international domain of foreign policy more quickly and cheaply.

Moreover, it is important to mention that digital diplomacy does not necessarily need financial investments, as the general aim is to reduce costs. Concerning the contribution of personnel, it is argued that employees are assumed to express a "desire to grow, master new technologies, spend part of their work time on working with the target Internet audience, processing electronic data, and creating information and reference materials" (Permyakova qtd. in Adesina 10). In contrast to regular diplomacy, employees' role involves normal processes such as "instructions to embassies in foreign countries; meetings and negotiations which are not in the public focus; collecting, reporting, and disseminating relevant information; patient and slow building of constituencies of interest; and the resolution of many technical issues through intergovernmental procedures, such as international conferences, international and regional organisations, or technical working groups". In conclusion, Adesina claims that digital diplomacy cannot be a replacement to the classical one, however, if it is given much attention and the right skill, this tool "can strengthen the work of the state in international relations and foreign policy in a faster and more cost-effective way" (11).

12.Risks of Digital Diplomacy

Because digital diplomacy is proven to be effective in the cyber realm, it has received criticism. This is because it relies on cyber-tools, like social media platforms, to conduct political matters. Consequently, these tools can be vulnerable to cyber threats, misinformation and disinformation. Adesina argues that social media's probable ineffectiveness endangers politics because they are always subject to cyber-exploitation. Richard Solomon, President of the United States Institute of Peace and a former US Foreign

Service officer, states that “Information about breaking international crises that once took hours or days for government officials and media to disseminate is now being relayed real-time to the world, not only via radio and television but over the Internet as well. Ironically though, for policy-makers, instant dissemination of information about events both far and near is proving to be as much a bane as a bounty” (11).

In other words, digital diplomacy is not a safe domain as the risks are cyber. When cyber-attacks occur, digital diplomacy loses its influence. The attacks the on the personal website of Yuli Edelstein, Israeli Minister for Public Diplomacy and Diaspora Affairs. Adesina comments, “the Minister said that nothing could stop him from performing public diplomacy on behalf of the state of Israel (Permyakova qtd. in Adesina 11).

Digital diplomacy can be threatened by the internet’s “culture of anonymity”, which Adesina defines as “anyone can adopt any persona, address or even attack anyone (Yakovenko qtd. in Adesina 11). Social media and personal blogs can be a target of such threats, especially those public figures. The damage they cause can be devastating. One famous example is when Carl Bildt, the Swedish foreign minister. In 2012, Bildt posted a very politically incorrect tweet which caused a lot of criticism. He tweeted, “Leaving Stockholm and heading for Davos. Looking forward to World Food Program dinner tonight. Global hunger is an urgent issue! #davos”. Tweeter users angrily responded by condemning the minister’s tweet (Permyakova qtd. in Adesina 11).

Conclusion

Cyberspace is still conceived as a challenge to US politicians. This is because of the evolution of information technology accompanied by increasing dependence on the Internet of Things (IoT). The US national security is not only defined in geography; it also encompasses the digital world where norms are different.

The reputation of the American foreign policy is under construction after the damage it received because of the use of hard power as a means of coercion. Thus, shifting to soft power to influence and regain lost supremacy is regarded as an urgency.

The international virtual landscape is viewed as a source of turbulence and conflicts. The US stands sceptical towards the militarisation of cyberspace by various state-actors and non-actors. A future cyberwar necessitates strategic capabilities to deter those threats. This is another challenge the US faces due to the rapid evolution of sophisticated cyberweapons.

What can be understood from Biden's speeches is that the US has learned the lesson, especially after the massive cyber-attacks that are from foreign origin. Biden's strategy considers those attacks a threat to the countries' national security. Cybersecurity issues need more international cooperation.

Works Cited

---. ‘What Are Cybercrimes?’ *Criminal Justice Matters*, vol. 58, no. 1, 2004, pp. 20–21. *Crossref*, doi:10.1080/09627250408553239.

‘A Short History of the Web’. *CERN*, 17 June 2022, home.cern/science/computing/birth-web/short-history-web.

‘Cyber- Combining Form - Pronunciation | Oxford Advanced Learner’s Dictionary at Oxford Learner’s Dictionaries’. *Oxford Learner’s Dictionaries*, www.oxfordlearnersdictionaries.com/pronunciation/english/cyber. Accessed 18 Feb. 2022.

‘Cybersecurity’. *The Merriam-Webster.Com Dictionary*, www.merriam-webster.com/dictionary/cybersecurity. Accessed 18 Feb. 2022.

‘International Committee of the Red Cross’. *ICRC*, www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm. Accessed 19 May 2022.

‘Non- Repudiation - Glossary | CSRC’. *NIST*, csrc.nist.gov/glossary/term/non__repudiation. Accessed 20 May 2022.

‘SI110: Information Assurance’. *Usna*, www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21/lec.html. Accessed 17 May 2022.

‘What Is a Denial of Service Attack (DoS) ?’ *Palo Alto Networks*, www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. Accessed 18 May 2022.

Abrams, Abigail. ‘Here’s What We Know So Far About Russia’s 2016 Meddling’. *Time*, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election.

Adesina, Olubukola S. ‘Foreign Policy in an Era of Digital Diplomacy’. *Cogent Social Sciences*, edited by James Summers, vol. 3, no. 1, 2017, p. 1297175. *Crossref*, doi:10.1080/23311886.2017.1297175.

AKTAŞ, Hayati. ‘DIGITAL DIPLOMACY AND ITS IMPLICATIONS IN THE 21St CENTURY’. , , pp. 1–2, www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj-juiVsLj4AhUJgv0HHVS_AEsQFnoECBAQAQ&url=https%3A%2F%2Fantalyadf.org%2Fwp-content%2Fuploads%2F2021%2F01%2FDigital-Diplomacy-and-Its-Implications-In-The-21st-Century.pdf&usg=AOvVaw1EYKX0p4v60n2N-Pff8Fgj. Accessed 10 Mar. 2021.

Atwood, Kylie Zachary Cohen and Sean Lyngaas. ‘State Department Will Form New Cyber Bureau - CNNPolitics’. *CNN*, 25 Oct. 2021, edition.cnn.com/2021/10/25/politics/state-department-cyber-bureau/index.html.

Bejarano, María José Caro. *CYBERSPACE: HARD POWER vs. SOFT POWER*. 29 May 2013, pp. 1–6.

Bjola, Corneliu, and Marcus Holmes. ‘Digital Diplomacy’. *REALITIES*, e-book, Routledge, 2015, pp. 95–111.

Caudle, Sharon L. ‘National Security Strategies: Security from What, for Whom, and by What Means’. *Journal of Homeland Security and Emergency Management*, vol. 6, no. 1, 2009. *Crossref*, doi:10.2202/1547-7355.1526.

Cavelty, Dunn Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (CSS Studies in Security and International Relations)*. 1st ed., Routledge, 2007.

CBS News. ‘U.S., U.K. Blame Russian Military for “Destructive” Cyberattack’. *CBS News*, 15 Feb. 2018, www.cbsnews.com/news/u-s-u-k-blame-russia-for-destructive-cyberattack-notpetya.

Choucri, Nazli. *Cyberpolitics in International Relations (The MIT Press)*. Illustrated, The MIT Press, 2012.

Craigen, Dan, et al. ‘Defining Cybersecurity’. *Technology Innovation Management Review*, vol. 4, no. 10, 2014, pp. 14. *Crossref*, doi:10.22215/timreview/835.

Cuhen, Richard, et al. ‘Non- Repudiation - Glossary | CSRC’. *NIST*, NIST, 26 Feb. 2001, csrc.nist.gov/glossary/term/non__repudiation.

D, Usha, and James H. *The Pocket Guide to Cyber Security*. e-book, Independently published, 2020.

Das, Sumanjit, and Tapaswini Nayak. "Impact of cybercrime: Issues and challenges." *International journal of engineering sciences & Emerging technologies* 6.2 (2013): 142-153.

David C. Mowery, Timothy Simcoe. " Is the Internet a US invention? —an economic and technological history of computer networking." *Research Policy*, vol. 31, no. 8-9, 2002, pp. 1369-1387. *https://www.sciencedirect.com/science/article/pii/S0048733302000690,* doi: https://doi.org/10.1016/S0048-7333(02)00069-0.

Fidler, David P. *America’s Place in Cyberspace: The Biden Administration’s Cyber Strategy Takes Shape*. 11 Mar. 2021, www.cfr.org/blog/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape.

Gill, Jaspreet. “Biden Tells Private Sector to “Lock Their Digital Doors” before Russia Gets In.” *Breaking Defense*, 21 Mar. 2022, breakingdefense.com/2022/03/biden-tells-private-sector-to-lock-their-digital-doors-before-russia-gets-in/. Accessed 19 May 2022.

Heckman, Jory. ‘Biden Makes Cybersecurity “Top Priority” in National Security Guidance’. *Federal News Network*, 5 Mar. 2021, federalnewsnetwork.com/cybersecurity/2021/03/biden-makes-cybersecurity-top-priority-in-national-security-guidance.

Heckman, Jory. “Biden Makes Cybersecurity “Top Priority” in National Security Guidance.” *Federal News Network*, 4 Mar. 2021, federalnewsnetwork.com/cybersecurity/2021/03/biden-makes-cybersecurity-top-priority-in-national-security-guidance/. Accessed 10 Mar. 2021.

Herrmann, Debra. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. 1st ed., Auerbach Publications, 2007.

Hoffman, Wyatt. ‘Is Cyber Strategy Possible?’ *The Washington Quarterly*, vol. 42, no. 1, 2019, pp. 131–52. *Crossref*, doi:10.1080/0163660x.2019.1593665.

House, The White. ‘FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity’. *The White House*, 26 Aug. 2021, www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity.

Jr., Nye Joseph. *Power in the Global Information Age: From Realism to Globalization*. 1st ed., Routledge, 2004.

Judd, Donald, et al. “Biden Tells Congress to “Immediately” Pass $40 Billion Ukrainian Aid Bill.” *CNN*, 10 May 2022, edition.cnn.com/2022/05/09/politics/biden-congress-ukraine-aid/index.html. Accessed 14 May 2022.

Kaspersky. ‘What Is SQL Injection?’ *Www.Kaspersky.Com*, 30 Mar. 2022, www.kaspersky.com/resource-center/definitions/sql-injection.

Katulis, Brian. ‘5 Transnational Issues Impacting Biden’s Agenda’. *The Liberal Patriot*, 22 Oct. 2021, theliberalpatriot.substack.com/p/5-transnational-issues-impacting?s=r.

Katulis, Brian. “5 Transnational Issues Impacting Biden’s Agenda.” *The Liberal Patriot*, 22 Oct. 2021, theliberalpatriot.substack.com/p/5-transnational-issues-impacting?s=r. Accessed 15 May 2022.

Kumar, Animesh. ‘Zero Day Exploit’. *SSRN Electronic Journal*, 2014. *Crossref*, doi:10.2139/ssrn.2378317.

Lettow, Paul. "U.S. National Security Strategy :Lessons Learned." *Texas National Security Review*, vol. 4, no. 2, 2021, pp. 117-154. *https://tnsr.org/2021/04/u-s-national-security-strategy-lessons-learned/.*

Mehan, Julie. *CyberWar, CyberTerror, CyberCrime and CyberActivism, Second Edition*. 2nd ed., IT Governance Publishing, 2015.

Miller, Maggie. “Blinken Formally Announces New State Department Cyber Bureau.” *The Hill*, 27 Oct. 2021, thehill.com/policy/cybersecurity/578728-blinken-formally-announces-new-state-dept-cyber-bureau-as-part-of/. Accessed 15 May 2022.

Morozov, Evgeny. "Freedom. gov." *Foreign Policy* 184 (2011): 34.

National Geographic. ‘The Future of Cyberwarfare | Origins: The Journey of Humankind’. *YouTube*, uploaded by National Geographic, 6 Apr. 2017, www.youtube.com/watch?v=L78r7YD-kNw.

Norton-Taylor, Richard. ‘Titan Rain - How Chinese Hackers Targeted Whitehall’. *The Guardian*, 15 May 2017, www.theguardian.com/technology/2007/sep/04/news.internet.

Potter, Evan. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. 1st ed., e-book, McGill-Queen’s University Press, 2002.

R.Johnson, Susan. *President’s Views:WikiLeaks and Diplomacy in the Digital Age*. Feb.

2011, p. 5, www.afsa.org/sites/default/files/1102presviews.pdf.

Riordan, Shaun. *Cyberdiplomacy: Managing Security and Governance Online*. 1st ed., Polity, 2019.

Roose, Kevin. “A Misinformation Test for Social Media.” *The New York Times*, 21 Oct. 2020, www.nytimes.com/2020/10/21/podcasts/the-daily/hunter-biden-new-york-post-twitter-facebook.html. Accessed 22 May 2022.

Russel, Buchan. ‘Defining Cyber Espionage’. *Cyber Espionage and International Law*, 2019, pp. 19–63, doi:10.5040/978178225770.

Samuels, Richard. *Encyclopedia of United States National Security, 1 Vol. Set*. 1st ed., e-book, SAGE Publications, Inc, 2005.

Silva, Eugenie de. *National Security and Counterintelligence in the Era of Cyber Espionage (Advances in Digital Crime, Forensics, and Cyber Terrorism)*. IGI Global, 2015.

U.S Department of State. “President Biden Delivers Keynote Remarks at the Summit of the Americas - 5:00 PM.” *Www.youtube.com*, 9 June 2022, www.youtube.com/watch?v=blC7SyMeseQ. Accessed 15 June 2022.

Wall, David. ‘Cybercrimes: New Wine, No Bottles?’ *Invisible Crimes*, 1999, pp. 105–39. *Crossref*, doi:10.1007/978-1-349-27641-7_5.

Yasar, Kinza, and Michael Cobb. ‘Man-in-the-Middle Attack (MitM)’. *IoT Agenda*, 28 Apr. 2022, www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.

Zubrinich, Paul, et al. ‘Proprietary versus Open Standards in ICT’. *IAM*, 13 Dec. 2018, www.iam-media.com/article/proprietary-versus-open-standards-in-ict.