A research study towards the improvement of human security and peace in cyberspace

A Thesis Submitted to the Faculty of Graduate Studies of The University of Manitoba

In partial fulfillment of the requirement of the degree of MASTER OF ARTS

Joint Master's Program in Peace and Conflict Studies

University of Manitoba / University of Winnipeg

Winnipeg, MB

By Joshua Dogbey

The University of Manitoba,

Winnipeg, Canada

Abstract

The ever-increasing dependence on the internet for the performance of human functions blurs some distinctions between physical and virtual worlds. Tasks like the performance of surgical procedures in hospitals depend on digital tools for efficient and effective health delivery. Still, society is witnessing both new forms of violence and the transposition of violent forms from the physical world to the cyber world. Cyberspace provides an easier option for harm to be caused to individuals because both state and non-state actors can extend their actions beyond their physical reach; commercial spyware is being deployed against political opponents in many countries. Without obtaining express consent, some organizations may be involved in trading the personal data of clients for business gains. During all these, the search for cyber peace has become difficult because of divergent views on what constitutes cyberviolence and the potency of cyber weapons. This research seeks to integrate discussions among scholars and the perspectives of some cybersecurity practitioners on cyber peace and violence. The decision to interrogate cyber peace and violence from the perspectives of cyber-security practitioners will contribute towards building some stability for these evolving concepts within the peace and conflict doctrines. Four cybersecurity professionals were interviewed on the subject. The basic human needs theory, human rights, and social justice theories are used to interrogate the understanding of cyber peace and violence. The results indicate that cyber harms targeting both state and non-state actors and installations should be considered in conflict analysis. This approach helps to enhance the concept of positive and negative cyber peace as possibilities.

Acknowledgments

I am thankful to my family and friends who have supported me throughout all stages of my education. I would like to express my gratitude to my academic advisor, Dr. Maureen Flaherty for guiding me through the entire process of writing this thesis. I am also grateful to the thesis advisory committee members, Dr. Noman Mohammed and Dr. Mary O. Adedayo for all their guidance. Even though I have never met any of you in person, you have all collaborated with me in diverse ways to realize this project. Thank you.

Contents

Introduction

Cyberspace is the interconnection of computer hardware, people, and virtual networks (Buçaj, 2020). Digital transformation has brought many positive developments in security and peace. For example, fingerprint technologies help to detect crime more efficiently than before. Despite its benefits, cyber advancement comes with new threats to world peace and security such as cyber-attacks. Globally approved counterterrorism software such as Pegasus is designed with the intention of combating crime and tends to be deployed on political opponents and adversary nation-states by government agents and institutions (Marczak, Scott-Railton, Anstis, et al., 2021).

These developments make the distinction between physical and virtual worlds more difficult (Chenou & Bonilla-Aranzales, 2022). By analyzing the so-called North Korean-sponsored cyber-attacks on Sony in 2014, Sharp (2017) argues that cyber capabilities have become mechanisms through which state and non-state actors coerce others, resulting in target countries incurring heavy financial costs to fix their cyber vulnerabilities.

In previous developments, cyberviolence disrupted the government and banking sector services in Estonia in 2007, with a similar incident in Georgia by alleged Russian agents in 2008 (Christen & Bangerter, 2017). More recently, the Citizen Lab notes a rise in the use of commercial spyware and virtual attack tools by state and non-state institutions, such that two political opponents in Egypt (Marczak, Scott-Railton, Razzak, et al., 2021), and a journalist with the New York Times who criticized the government of Saudi Arabia (Marczak, Scott-Railton, Anstis, et al., 2021) were hacked by agents using Pegasus Spyware in separate incidents. The Citizen Lab is a multidisciplinary center established at the University of Toronto. The center

adopts research practices from different domains like Computer Science, and Political Science to counter issues of cyber insecurity, especially pertaining to the human rights of people (the Citizen Lab, n.d.). There are some concerns that cyber insecurity could harm human rights and threaten global peace.

The search for cyber peace is even more complicated because of the divergent views on what constitutes cyberviolence and the potency of cyber weapons. Buçaj (2020), who reviewed the extensive literature on the classification of cyber conflict, argues that cyberviolence worth the thresholds of armed conflict are those operations that are politically motivated and are targeted at another nation's important infrastructure, like electricity, directly affecting the physical functioning of the infrastructure or causing human deaths (Buçaj, 2020).

Restricting violence to physical space excludes virtual activities of espionage or exploitation. By focusing on the thresholds of cyber incidents that can lead to physical confrontations—the Laws of Armed Conflict, and some Peace and Conflict Studies scholarly articles have limited the scope of violence to physical violence that can claim lives and properties (Buçaj, 2020).

For example, Rid's (2013) definition of a cyberattack as a virtual attack that reduces the chances of politically – motivated physical violence, presupposes that online-related violence has no physical bearing. Indeed, the traditional notion of war entails physical violence or the threat to use violence to achieve a politically motivated outcome (Christen & Bangerter, 2017). This creates an additional challenge in the search for peace.

The exclusion of cyber–attack's propensity to become a disruptive tool leaves an important gap in peace and conflict practices and scholarship. Some countries take advantage of the lapses in internet governance and launch cyber-related violence as a complement to their

physical combat (Akoto, 2022). The situation becomes more complicated when private entities or individual attackers are recruited by countries to conduct violent activities on their behalf. Therefore, it becomes difficult to trace and hold attackers accountable in such circumstances.

On the other hand, Christen and Bangerter (2017) argue that cyberspace should also be seen as a physical environment. In addition to computers and other technologies, the cyber environment also includes people (Boustead & Shackelford, 2022). Human dimensions of cyberspace are as important as the mere interaction of computers. As a result, Duguin et al. (2022) explain cyber peace as the existence of "human security, dignity, and equity are ensured in digital ecosystems" (p. 213). Human security as applied to cyber peace discussions, underscores the protection of infrastructure and services that are crucial to human life.

In addition, Chenou and Bonilla-Aranzales (2022) propose four cornerstones of cyber peace as, "human rights, access and cybersecurity norms, multi-stakeholder governance, and stability" (p. 95). Though upholding freedom of expression online is espoused as an important part of cyber peace, the abuse of the same in the form of the spread of fake news tends to disturb peace. Sometimes too, the manner of tackling certain abuses in themselves could be disruptive. To ensure a country's security, governments may decide to embark on nationwide surveillance. These surveillance activities could potentially infringe on citizens' rights to privacy (Chenou & Bonilla-Aranzales, 2022).

These divided views are indicative of almost every cyber operation noted as a cyber war, making some states justify the use of repressive measures that encroach on the privacy and liberty of their citizens. The hybrid war terminology attempts to integrate different elements of war. Hybrid war insinuates a conflict situation whereby there are physical confrontations among

parties using traditional weapons of warfare such as guns—in addition to the use of new strategies such as cyber weapons (Simons et al., 2020).

Moreover, the use of encryption technology makes the identification of actors or originators of cyber actions difficult, thereby adding another layer of obscurity to international and intra – state conflicts (Buçaj, 2020; Christen & Bangerter, 2017). Encryption has become a double-edged sword; though it helps human rights activists and political opponents to escape persecution, it is also used by criminal groups, and state actors to conceal their identities.

Despite these threats, Rid (2013) suggests that cyberviolence is an exaggerated concept that is detached from reality because cyber operations are difficult to attribute, repeat, and cause no physical harm. To some scholars, the absence of well-governed cyberspace indicates that it is no longer a safe space. Alternatively, cyber peace will prevail when the space is devoid of disruptions and covert suppression. Peaceful cyber practices may also include technological innovations that could improve the stability and functioning of the internet (Marlin-Bennett, 2022). Most parts of international norms were made before the diffusion and enhancement of cyber potentials and may not be capable of handling some threats of offensive cyber practices. For example, there is confusion about what thresholds of cyber disruptions could trigger the use of relevant international laws on humanitarianism and human rights (Lin, 2012; O'Connell, 2012).

There has been little scholarly attention paid to cyberspace as a focus of peace studies. This research, therefore, looks at the links between cyberspace and peace. Consulting the literature available and experts in cyber-security, we ask, "What is cyberviolence and how does it occur? Why is cyberviolence of importance to peace and conflict studies? How can cyberviolence be addressed? How can cyber peace be achieved?". The empirical part of this

research adopts a qualitative methodology. Semi-structured individual interviews with four cybersecurity experts were conducted. These interviews are described, synthesized and discussed.

Beyond this introduction, this research report is divided into the following major segments: the context of the research, theoretical perspectives, methodology and methods, findings and discussions, and conclusions. The subsection on findings is further divided into cybersecurity roles, cyberviolence, and cyber peace. The section on findings provides a detailed description of data collected from participants and some literature. The data highlights information about how violence is occurring in cyberspace and the measures that could be employed to sustain peace.

Discussion subsections highlight the following: the meaning of cyberviolence; cyber peace; cybersecurity roles as unexpected results; limitations of the research; implications of findings; and recommendations for future research. Synthesizing the discussions on cyberviolence yields the subheadings of crimes and balkanization of the internet, human rights violations, and fake news for cyberviolence. Meanwhile, the discussion on cyber peace is regrouped into negative and positive cyber peace.

Chapter 1: Context of the Research

This research enquires into cyberviolence and peace actions by individuals, state, and non-state organizations. Some countries like China have comprehensive internet censorship schemes in the world (MacKinnon, 2008). In China, the state spends a lot of effort to block internet users' access to some social media platforms and websites like Facebook. For example, Hoang (2021) observes that websites that were reporting on the abuse of rights of the Uyghur people of China were blocked in 2021. In related instances, it is alleged that the Chinese state creates cyber-attack tools to break into foreign-based computer systems with the aim of blocking its citizens' access to external sources such as Twitter (Marczak et al., 2015).

The system designed by China to control its digital space is known in the literature as the Great Firewall (GFW). The GFW uses updated lists of keywords that relate to certain politically forbidden content to deny citizens access to web-based platforms, through filtering the Domain Name System (DNS). In the second strategy of internet restriction, forged foreign-based Internet Protocol (IP) addresses are used by the Chinese authorities to conceal the origins of their censorship acts (Hoang, 2021).

In a bid to understand the monitoring behavior of the GFW, Hoang (2021) discovered that China's censoring of websites negatively affects the worldwide internet DNS. Some censored domain names from China have polluted and disrupted the functioning of DNS – IP conversion regime for public and external websites like Google. The importance of the DNS mechanism cannot be underestimated as it helps to convert text-based website addresses into numeric formats to enable communication with IP addresses (which are numeric) of computers and other connected devices (D'Angelo et al., 2022). Due to the impact of internet monitoring tools on digital freedom of speech and the smooth operation of some useful public websites like

Google. Hoang (2021) who is affiliated with the Citizens Lab at the University of Toronto has designed the GFWatch, a system that keeps track of the evolution of GFW to inform the public about how to circumvent the online surveillance of countries like China.

The GWatch dashboard provides updated list of domains that are suppressed. This data would be helpful for the designers of Virtual Private Networks (VPNs); or for individuals who seek to bypass the internet Policing system of China. However, Hoang's (2021) inquiry offers mostly detailed descriptions of the computer-related system employed by China to control the internet space, nearly leaving out the socioeconomic drivers of China's quest to police the internet space.

MacKinnon (2008) explains that China's practice of filtering citizens' access to online media may stem from Chinese authorities fear that internet could be used to instigate socioeconomic undertones for political change. Just as in the physical realms, China does not want to lose control of its socioeconomic tradition in the digital spheres (Lindsay, 2015). Put differently, MacKinnon (2008) notes the "system of Internet censorship, control, and propaganda, while by no means impenetrable, is effective enough that the picture of the world seen by the average Chinese Internet user is skewed in the regime's favor" (p. 33).

The government of China puts the responsibility on internet providers to restrict access to online contents that are contrary to its political ideals (Lindsay, 2015). Activists like (Hoang, 2021) believe that cyberspace should have a democratic culture, devoid of unwarranted social, economic and political controls. In other words, the presence of unnecessary online restrictive measures against civil society is a semblance of human rights abuse. In peacebuilding tradition, upholding human rights principles offers the opportunity for equal and just treatment of people, to build safer communities (Byrne & Thiessen, 2020; Mani, 2007). Since human security tend to

be an essential part of human rights (Qureshi, 2018; Sandole, 2013); it could be argued that people's safety online should be regarded as a fundamental condition for stability. The penchant for abusing the rights of innocent citizens in the name of strengthening national security may be reduced if countries come to the realization that there is no need for the distinction between human security and national security, since the wellbeing and the formation of the state is the result of individuals mobilizing themselves against structures of lawlessness that erodes their liberties. In reality some societies hold the view that collective rights should override that of individuals (Christie & Hanlon, 2020).

Though cyber tools have helped some social movements like the Arab Spring to mobilize against some authoritarian regimes, they are also increasingly being used by some governments to track and silence opponents, a situation Dragu & Lupu (2021) describe as *digital authoritarianism.*

A major limitation in existing literature is the emphasis on cases of responsive surveillance, where states embark on cyber monitoring to take action against dissident persons known to have mobilized against their regimes (Dragu & Lupu, 2021). It also is important to consider cases in which governments digitally spy on everyone just to prepare for unwarranted repressive actions.

As a measure against insecurity, Ilunga (2020) argue that development agencies or nongovernmental organizations should mainstream the protection of security of individuals in their programming. I think this strategy will offer some relief to individuals as state institutions tend to sacrifice individual rights of their citizens for national security.

Though it delves extensively into comparative economic motivation for cyberviolence between the United States of America (USA) and China, the work of Lindsay (2015) does not

provide much insight into now human rights perspectives affect China's propensity to conduct cyber operations. In addition, Lindsay (2015) analyses only some underlying factors that motivates China's espionage activities, falling short of discussing specific types of cyber weapons that are being deployed. Lindsay (2015) concludes that China's vulnerability in the cyberspace is underestimated, and the country's ability to disrupt the virtual landscape is overly appreciated. That is, China's cyber strength and vulnerabilities would only cause some gains or losses in trade and not the physical occurrence of war. Lindsay (2015) again notes that inadequacies in global governance of the internet have contributed to the chaos in the cyber landscape.

While China wants internet sovereignty of countries, western countries are calling for unrestricted connection (Lindsay, 2015). China and Russia would want that the current governance arrangement of the internet, which is dominated by the USA be replaced with a global intergovernmental organization at the level of the United Nations, to ensure that no country's sovereignty is eroded. Under the current internet governance system, the worldwide domain name mechanism which is supervised by Internet Corporation for Assigned Names and Numbers, with headquarters in Los Angeles is regulated by the Department of Commerce of the USA (Lindsay, 2015). It is safe to say that some countries do not trust the current structure of internet administration, hence their eagerness to carry out cyberviolence.

Furthermore, Akoto (2021) who defines state-initiated cyberviolence as computer-originated disruption or intrusion that is initiated by state actors, proposes three reasons that influence the occurrence of state-backed cyberviolence. Cyberviolence tends to be a replacement for or a complement to displaying military strength against adversaries. Some states also conduct digital attacks to espouse their political ideologies. Other countries may embark on some

intrusive cyber actions, such as theft of trade secrets to gain trade advantages. The inquiries of Akoto (2021) explores quantitative dataset of about 24 countries, to establish the correlation between state-initiated cyber espionage and trade benefits. Akoto's (2021) investigation concludes that countries with highly advanced industries such as aerospace have higher tendency to embark on cyber espionage for trade benefits. This author's work examines just one dimension of cyber-attack, that is cyber espionage, and only from the perspective of the attackers.

Moving away from the state to individual levels, this research explores the indignities to humans happening in the digital space. Human dignity prevails when a person can enjoy shared socio-cultural rights without any forms of discrimination or inequality (Qureshi, 2018). It is argued that certain cyberviolence targeting important facilities could lead to actual death. A ransomware attack on hospital servers in Düsseldorf, Germany resulted in the death of a patient—because the necessary healthcare could not be provided to her. In other words, when internet users' privacy, security or freedom of expression is in danger through certain actions, including manipulation, censorship, and espionage then peace is said to be absent (Duguin et al., 2022, p. 217).

Chapter 2: Theoretical Perspectives

In some literature, language related to Cyber war or attacks is used instead of the term, cyberviolence. Cyber war tends to be seen as defensive or offensive actions that may cause death or injury to humans, and/or damages to property whereas, cyber peace is a condition that exists when each country provides accessible communication, protects the citizenry in the virtual space, avoids offensive cyber-attacks, and builds collaborative peace with other countries in the cyberspace (Christen & Bangerter, 2017). Due to the limitations of the naming of cyber war or attack by international legal instruments and some literature, henceforth, this paper uses the term cyberviolence instead of cyber war. The limitations of the term cyber war have been explained in the introduction.

Peacebuilding, which is also seen as system of actions for research and practice to change the direction of conflict into peaceful and beneficial alternative, has gone through some phases such as liberal, hybrid, and emancipatory (Byrne et al., 2020; Kroeker, 2020; Tschirgi, 2020). Put differently, peacebuilding entails a range of perspectives that seek to bring an end to physical violence through conflict management activities like peacekeeping, in addition to tackling non-physical violence such as income inequality (Tschirgi, 2020). The liberal tradition of peacebuilding replicates institutions and principles of western democracies in other societies recovering from violent conflicts, with the aim of achieving peace.

Criticisms against this method of peace with some traces of non-sustainable practices like the virtual neglect of inputs of local population, led to calls for either hybridized or localized peace (Tschirgi, 2020). It became somehow clear that, activities within hybrid and local peacebuilding doctrines tend to be dominated by the local elites, another level of neglect of voices of vulnerable and minority groups (Byrne & Thiessen, 2020). The need for integrative,

and inclusive approaches to peace led to calls for adoption of critical & emancipatory methodology. Byrne and Thiessen (2020) explain that critical & emancipatory peacebuilding as a methodology of peace research and practice guides the regular design, implantation, and local introspection to break the bonds of societal imbalances. This methodology calls for local actors at all levels of society to have the right to determine the content of their peace activities. Critical and emancipatory methodology leans towards qualitative studies because quantitative approaches are geared to study superficial phenomena of dominant issues. Situations of peace and conflict are complex, often requiring deeper understanding of contexts (Byrne & Thiessen, 2020).

Conflict transformation theorists seek to uncover structural arrangements that bring about violence of any form Jeong (2020) and the nature of relationship that exists among feuding parties, including how inter or intra-group dynamics fuel the direction of conflicts (Cormier, 2020; Irvine & Hansen, 2020).

With the help of the Basic Human Needs (BHNs) Theory as espoused by John W. Burton, this research will extensively examine cyber peace and violence. John W. Burton explains that basic human needs form the core of the onset, escalation, and resolution of conflicts. At the center of basic human needs are values, which are personal and shared social, psychological, or even biological beliefs that lay the foundation for human behaviour.

The work of John Burton tilts towards Paul Sites' (1973) recognition of eight equally important human needs, as opposed to the concept of the hierarchical nature of human needs by Abraham Maslow (1987) (cited in Sandole, 2013, p. 21). Though Abraham Maslow's list is organized in ascending order as; physiological, safety, love, psychological, esteem and self-

actualization needs, Ronald Fisher (1990) argues that the protection of these needs should be more important than their hierarchical organization.

Sandole (2013) criticizes John Burton's additional human form of "Role Defense"; which explains the rights of people to defend their properties and positions, as inimical to human rights protection of victims because it presupposes that even war criminals have the right to self-defense. John Burton's (1984) synthesis of the basic human needs' yields fewer versions of human needs; *identity, participation, recognition, and security* (as cited in Sandole, 2013, p. 23). Basic needs also include "food, shelter, sanitation, health and education" (Mani, 2007, p. 39). Human beings are relentless is pursuing these needs no matter the opposing forces. It is safe to say that the clash of opposing forces in pursuit or defense of basic needs escalates conflicts.

John Burton's work has also been criticized by Kevin Avruch as failing to examine the social structure, such as the role of cultural practices in perpetrating violence. When systems deprive people of their basic needs, they become frustrated, and could react violently (As cited in Sandole, 2013, p. 26). Fisher (1990) explains that the identity component of human needs theory is useful in understanding the escalation dynamics and options for resolving social conflicts. This is because, conflicting needs could lead to protracted competition, especially if competitive actions are not coordinated in orderly manner.

Identity provides a sense of belongingness to a group, and its variants such as ethnicity could become a mechanism for excluding others in full social participation. Identity could not necessarily cause conflict but could be a means through which conflict could be transformed. Conflicting parties may mobilize their interests along the line of social differences, rather than cooperating to fix the root cause of conflicts (Žagar, 2020).

Another important theory worth discussing is Johan Galtung's (1996) perspectives on violence and peace. He explains that peace research should investigate conditions embedded in society, culture, individual and time, to have a detailed appreciation of a conflict. Peacebuilding is the practice of finding opportunities to reduce and prevent violence. Violence on the other hand is any form of harm which could be indirect, as related to social inequalities or repression; cultural as in the case of stereotypes; and direct as in the case of damage to life and property (Galtung, 1996; Johan Galtung, 1969). In other words, violence is the result of different forms of influence on humans that make them fall short of their actual capacity (Johan Galtung, 1969).

When peace is seen as the absence of only direct harm or conflict, it is a negative form of peace; however, when direct harm is absent and social justice or equality is present, peace is said to be positive (Byrne et al., 2020; Syropoulos et al., 2021; Tschirgi, 2020). Basic human needs are linked to human rights principles. Human rights seek to uphold the core dignity of humans. The provision of fundamental human needs such as security, love and inclusion, is foundational for the protection of human dignity, and the mere absence of these needs reflects Johan Galtung's conception of indirect violence as discussed earlier. Qureshi (2018) notes that public authorities or institutions have the obligation of ensuring that these natural needs of humans are guaranteed, and there should be avenues to seek redress for infringements.

This research adopts the position that virtual confrontations in themselves can be violent. Violence perpetrated in cyberspace impacts people, just as violence in the physical space, and in the postmodern society. The lines between the virtual and physical spaces are becoming increasingly blurred. In the past, there were human functions, which could only be performed physically; however, the advent of technology and the internet, makes it possible for humans to organize these functions successfully in the virtual space as well. Some functions that must

necessarily be done in the physical space can only be done excellently, by indulging some virtual elements by way of internet, and technology. Therefore, state-sponsored attacks on others to disrupt the provision of essential services are as violent as that physical wars that claim lives. Therefore, this research process will adopt Galtung's (1996) theoretical approach of constructive peace.

In this approach, theoretical concepts of peace and violence will be integrated with the data collection and analysis. Since enquiries into cyber conflicts are relatively new to the field of Peace and Conflict Studies, a constructive peace approach will help to adequately discuss the importance of cybersecurity in attaining positive peace. The direction of this research differs from the position of Marlin-Bennett (2022) who argues that cybercrimes like scamming and revenge porn, though lawlessness, are not actions that should concern the peacebuilding domain. If cybercrime is only seen as cyber aggression, it brings the risk of making cyber peace even more confusing. But Marlin-Bennett (2022) allows a little room for attention to cybercrimes to be considered as potentially contributing to cyber peace-building domain; that is when they are laced with geopolitical objectives. The so-called cybercrimes just like cyber espionage and distributed denial of service cyber-attacks all have similar long-term infringement on the trust of society.

In another way, social justice principles will add a depth of richness to the research. Mani (2007) argues about the goals of justice in ensuring social harmony by bringing about balance in the implementation of all components of justice such as: “legal”, “rectificatory”, and “distributive” (p. 5-6). Yet Mani (2007) mentions that distributive justice is mostly seen as social justice. In ensuring legal justice as an element of peace, it is important to work towards ensuring that a legal system in any given context is accessible and devoid of corrupt practices. According

to peacebuilding doctrines, rectifying measures to correct the harms of conflict such as physical injuries are necessary for peace. The correction of harm caused might include the need to have victims compensated or perpetrators prosecuted. As a related concept, distributive justice explains the idea that there should be equity in resource distribution, political representation, and social representation (Mani, 2007).

This research argues that all three elements of justice are equally necessary for social harmony to prevail. For perpetrators of injustice to be punished, a fair legal system is required. And to have a well-functioning legal system, requires that the criteria for recruitment of judges, and prosecutors are objective and distributive. Qualified personnel from different ideological orientations, ethnic, and geographic origins should be equitably distributed in the system. Moreover, the codes of the International Covenant on Civil and Political Rights (ICCPR) such as the assumption of innocence of any accused person until proven beyond doubt help to build a reliable justice system (Mani, 2007).

Basic human needs theory, human rights principles and social justice arguments seek to curtail human indignity through ongoing social constructions. Specifically, social justice and human rights principles seek to stop the abuses of state power while protecting the rights of citizens, such as freedom from arrest arbitrarily and abuse of privacy (Mani, 2007). The three main elements of social justice that largely occupy the attention of peacebuilding include, "needs, rights and inequalities" (Mani, 2007, p. 39). In a society where wealth is concentrated in the hands of a few at the expense of the vast working class creates a breeding ground for conflicts. It may mean that the needs of others in the society may not be met.

This is because those who control a huge proportion of wealth tend to control social processes that help them to maintain their influence or wealth. Yet it can be said that the working

class in certain contexts is favoured by their huge numbers which could be used as a vehicle of social change, to heal any forms of inequalities (Gerlach & Hurlbert, 2011). In another layer of the discussion on social justice, Comeau (2011) explains that social suppression based on conditions such as origin, and political ideology leaning leads to other forms of sociocultural deprivations. A society where privileges and disadvantages are unevenly apportioned by structure tends to have less harmony. The beneficiaries of the inequalities may want actions that reinforce their privileges whereas those deprived may favor actions that will bring about a change in order. Social tensions among social groups could create social instability, if not managed well.

The research holds the view that leaving cybercrimes out of peace discussion, will be creating more conditions of injustice for victims of cybercrimes. To ensure ownership of peace processes, individuals must be involved in cybersecurity discussions, in as much as state activities or representatives of private organizations. Insecurity, poverty, and inequalities are part of the fundamental sources of violence. As a result, human security dimensions were introduced to tackle injustice cases in peacebuilding processes. A social justice-driven peace approach would attempt to put in measures to improve the situation of marginalized persons such as minority groups and vulnerable citizens (Byrne & Thiessen, 2020).

In building peace that is deep-seated in social justice, it is important to consider how power mechanisms like inequitable means of wealth distribution, and historical and unresolved traumas. These factors might also include marginalizing arrangements in any other sector of society like political, racial, or religious contribute towards social instability (Byrne & Thiessen, 2020; Lounsbery & Pearson, 2020). In other words, to achieve “positive peace” or “just peace”,

Byrne and Thiessen (2020) explain that it is necessary to work towards removing all forms of inequalities (p. 139).

Identifying elements of social structure fueling conflicts is important. This presupposes that the conflict environment is as important as the characteristics of the parties involved in a conflict. Though the theories of human rights, basic needs and social justice are related in some ways, this research will use each of these theories distinctly or jointly when required. That is, the theories will not be used interchangeably, but complementarily, despite their similarities. This standard for the research conforms to Mani (2007) argument that human rights are "a partial or incomplete expression of justice" (p. 47).

I argue that the existence of virtual confrontations amounts to violence, and that the thresholds of kinetic wars might be only partially applicable to cyber conflict. Violence in the cyberspace impacts people, just as violence in the physical space; and in the postmodern society, the lines between the virtual and physical spaces really blur. In the past, there were human functions, which could only be performed physically; however, technology and internet, makes it possible for humans to organize these functions successfully in the virtual space as well. In fact, some functions that must necessarily be done in the physical space, can only be done excellently, by indulging some virtual elements by way of internet, and technology. Therefore, a state-sponsored attacks on others that seeks to disrupt provision of essential services of others are as violent as that of physical wars that claim lives.

Chapter 3: Methodology and Methods

This section outlines the methodology and methods used in this research, which was proposed to and approved by the Research Ethics Board (REB) of the University of Manitoba prior to the undertaking of the actual process (Appendix A).

Research Question and Significance of Study

This research examines peace and violence in the cyberspace. Again, the following are the research questions. How does cyberviolence occur? How can cyberviolence be addressed? How can cyber peace be achieved? This study is important because though cyberviolence is becoming more rampant, scholarly domains such as Peace and Conflict Studies, International Relations and Political Science seem to be behind in the integration of cyber dimensions of conflicts in the broad spectrum of research strategies.

Previous empirical data and literature have mainly focused on theoretical discussions on cyber peace. However, this research seeks to integrate and represent the diverse perspectives on cyber peace and violence held among scholars and cybersecurity practitioners. Beyond the theoretical discussions, reflections of cybersecurity workers will be explored. The decision to interrogate cyber peace and violence from the perspectives of cyber-security practitioners will contribute towards building some stability for these evolving concepts within the peace and conflict doctrines (Marlin-Bennett, 2022) and make helpful additions to the evolving literature on cyber repression.

Methods

This research employs a qualitative research approach for data collection, analysis, and description. Qualitative research tends to examine people's in-depth experiences to understudy social phenomena. This calls for methods that allow the research participants to provide detailed and open-ended responses. The outcomes of qualitative research might be difficult to generalize because the sample size of participants is mostly not representative of the research population (Hammersley, 2013; Jackson et al., 2007). Methods here refer to the tools or strategies that will be used to gather data for this research whereas methodology encapsulates explanations to a particular approach to data collection, and interpretation (Jackson et al., 2007).

The explanation of Pertti Alasuutari (1995) sheds light on why the quantitative approach will not be helpful in finding answers to my research questions: the objective of quantitative research is to understand how frequent the occurrence of an event can be associated with different causes (cited in Hammersley, 2013, p. 1). As a result, quantitative methodology overly focuses on numerically based measurable symptoms to establish a cause-effect relationship. Not every cause-effect tendency manifests clearly, and it is not uncommon for the motives behind certain social phenomena such as cyber-attacks to be hidden. The complexities associated with the intersectional experiences of research participants or social issues like cyber conflicts highlights the usefulness of qualitative methodologies to handle these nuances (Kara, 2018).

The main method or tool used for this research is semi-structured interviews, in addition to a reviewing pertinent literature about cyber-security, and peace. These interviews took place on Zoom, which allowed connection with a variety of participants as well as some level of dialogue and follow-ups on important elements of the research objectives (Brinkmann, 2013). An interview is mostly a person-to-person interaction between a participant of an enquiry and a

researcher; which could be in-person or virtual, with the aim of collecting information on a particular phenomenon (Brinkmann, 2013; Harrell & Bradley, 2009).

Interview questions were drafted in ways to solicit interviewees' descriptions of their experiences. The technique of interviewing using somewhat open-ended questions allows for detailed and relevant data to be gathered on a technical or sensitive subject. Put differently, interviews tend to be useful techniques for finding opinions or describing facts and processes. Specifically, semi-structured interviews involve a technique in which the researcher comes to the interview session with a prepared list of questions but may ask the question according to any order. This strategy allows for a fluid conversation instead of merely adhering to a strict order of questions. Semi-structured interviews make room for follow-ups, in a manner that is comfortable for the respondents (Harrell & Bradley, 2009).

Participants

Five cyber-security experts who have had at least two years of working experience were recruited using snowball sampling technique and interviewed. These cyber professionals work in different organizations in totally different countries. Two of the participants work in the United States of America, one works in Ghana, and another participant works in France. Some participants consult for governmental and/or non-governmental organizations. The others practice cybersecurity in the private sector. I asked people working in different organizations to recommend cybersecurity professionals in their professional networks who would be interested in granting interviews for the research. The strategy is consistent with snowball sampling technique (Elo et al., 2014; Harrell & Bradley, 2009). This sampling method has helped me to obtain qualified participants for the research. The interdisciplinary field of cyber peace and

conflict is relatively new and there are few people who are willing to share their knowledge or experience pertaining to this enquiry.

The participant recruitment message was posted on my personal Facebook and LinkedIn accounts. Upon sighting my message, people in contact lists on these platforms recommended cybersecurity experts that I could contact directly for the research. I contacted interested participants directly with more details about the research. Each participant agreed to the terms of the research and signed their respective participant consent agreements (Appendix B). One of the interviewees who consented to the interview verbally with the assurance to return the signed consent form later, failed to return the form after several follow-ups. Hence the interview transcript of this participant has not been included in this report. The interviewees were asked about their professional knowledge pertaining to their understanding of cyber peace, and cyber violence. The participants were asked about how the handling of customers' or citizens' digital data constitute violence.

The cyber professionals also explained their conceptions on cyber-espionage and internet censorship within the discourse on human security and the sharing of fake news. In contrast, participants expressed their viewpoints about what cyber peace is, and how that can be attained or sustained.

The interviews were recorded into the University of Manitoba licensed Zoom clouds. Each participant turned off their camera during the interview; only their voices were captured to protect the identity of the participants. This strategy was used because the Zoom function only allows for video recording. The Zoom cloud function provided a separate text transcript of each interview. I deleted and anonymized all personal names from the transcripts that the Zoom

function may have captured from usernames that the participants may have signed in with from the interview.

To make it simpler for the verification of the contents in the interview transcripts, each transcript was mapped onto associated recording using the NVIVO software. This strategy permitted me to do the line-by-line coding of the transcript in NVIVO while verifying and correcting errors in the transcript. That is, the recordings were played alongside coding and correction of errors in the text. After the coding was completed, I took time to ensure that contents of each code matched with the actual codes.

The codes were regrouped according to broader themes. This entails finding out, describing, and presenting the components of data in systematic ways (Bazeley, 2009; Braun & Clarke, 2006). Moreover, data has been described and analyzed in a detailed way. To achieve this objective, Bazeley (2009) recommends that the researcher includes enough information about the content of each category and theme; explain the differences and similarities within and outside categories; relating data to existing literature to identify any additional trends; and using graphs.

Research Quality

As noted earlier, this research was approved by the Research Ethics Board 2 of the University of Manitoba under the protocol number HE2022-0197. Every choice of approach in this research had to be verified by the ethics board to be sound and harmless to everybody associated with the research and the entire research outcomes. All participants whose interview responses have been treated in this report signed their consent form. A sample consent form has also been attached as an appendix. Overall, I observe that the ethics approval process has been rigorous and time-consuming.

In literature, researchers use the term validity or trustworthiness to examine the extent to which a scientific enquiry can attain the research objectives (Lincoln & Guba, 1986; Mills, 2011). Applying these terms, Guba argues that qualitative research could be judged based on how transferable, dependable, credible, and confirmable the research is (Mills, 2011, p. 103). Mills (2011) explains each of Guba's criteria as follows. The credibility of an enquiry refers to how well the researcher can handle difficulties that may arise. This calls for the adoption of certain strategies such as debriefing other professionals in the field; using different origins of data and methods; checking the content of the research report with respondents; checking for research coherence; and ensuring that researcher's accounts and explanations conforms with interview transcripts or recordings.

To facilitate the transferability of the research, it is necessary to provide detailed documentation of data, and extensive explanation about the context of the research. How dependable the research is relating to the extent of constancy of data collected, and this can be tested by allowing an external personal to verify the mechanisms of collecting, analyzing and interpreting data. Research confirmability explains how objective the data should be, such that, the researcher needs to be critical and reveal key reasons behind the choices made. A useful strategy to assure the confirmability of any inquiry is to regularly document musings.

Herr and Anderson (2015) also propose five validity criteria: the extent to which the outcome of the research adds something new to existing literature; how research process empowers both the researcher and participants; how well the enquiry leads to social change; the degree to which research outcomes reflect the realities within the context of the research; and the extent to which the research methodology is aligned with the research objectives.

As a result, this research uses both primary data (on-to-one interview transcripts with computer security specialists) and secondary data (scientific articles published in journals), and other sources, as applicable to enable triangulation, as suggested by Mills (2011). The recorded interviews offer the opportunity for detailed and reasonable description, and interpretation of events and inputs. A synthesis of Guba's validity criteria and that of Herr and Anderson (2015) has been used as a quality control guide in all other areas of my research.

Chapter 4: Findings

The data collected from the interviews are organized into three main categories. Therefore, data analyses will have three main sections: cybersecurity roles, understanding cyber violence, and understanding cyber peace.

Cybersecurity Roles

This research delves into the evolving trends of cybersecurity jobs. This approach offers some explanation to specific activities that the cybersecurity personnel who were interviewed are involved. Some of the roles noted relate to the past experiences of the participants, even though all the participants are still involved in cybersecurity roles. These are the cybersecurity functions that the participants perform or have done in the past: Chief Information Security Director; Cyber Researcher and Consultant; Cybersecurity Architect and IT Security Officer; Governance, Risk and Compliance Officer; Infrastructure and Network Officer; Co-founder of a Cyber Company; Cyber Risk and Compliance Officer; Cybersecurity Researcher; Information Security Officer and Network Administrator.

A participant explained that Chief Information Security Director, a position he occupies could be called the Chief Information Security Manager in other contexts. As far as this person is concerned, anyone who assumes this role is responsible for developing a frameworks and policies for cybersecurity for the organization in which they work. Having worked within many large companies, Participant 2 proceeded to establish two different cybersecurity companies—one company focuses on winning and performing government contracts on cybersecurity while the other one trains and employs minority groups into cybersecurity. With the intentions of securing the safety of their customers, the cyber research and consultant hunts for recent techniques or tools by analyzing cyber-attacks. This person's role requires collaboration with

legal institutions around the globe, as he shares the results of investigations with authorized institutions so that the attackers could be identified. The cyber research and consultant work with his to make the outcomes of their investigation public, and blocks malware used by the attackers. As a cybersecurity architect and IT consultant, participant was conducting tasks such as Fire Wall, and e-mail gateway configurations.

As cybersecurity researcher, Participant 3 evaluates the clients' cyber infrastructure and known attack vectors to offer solutions to secure the clients' systems. Though the tasks of the cyber researcher and consultant and the cybersecurity research are similar—they both investigates cyber-attack techniques, the cyber researcher and consultant informs the public and authorized organizations around the globe about his findings, in addition to blocking those attack vectors, whereas the cybersecurity researcher works with their corporate clients to address their cyber vulnerabilities.

Participant 4 who is a cyber risk and compliance officer explains that his role includes ensuring that the information security for his organization is at a level that allows for smooth operation. He assesses the risk and security stock levels of the organization and worldwide events to conclude on the robustness of cyber infrastructure. Participant 4 also ensures that the organization is compliant with cybersecurity standards such as "ISO 27001 information security management system." He explains cyber governance as following the correct processes of getting things done.

> ...the Russia Ukraine hybrid war…When it started there was an uptaking… in cyberspace, and we needed to perform an extensive risk assessment to ensure that systems where robust enough to be able to handle any infiltration…
>
> Participant 4

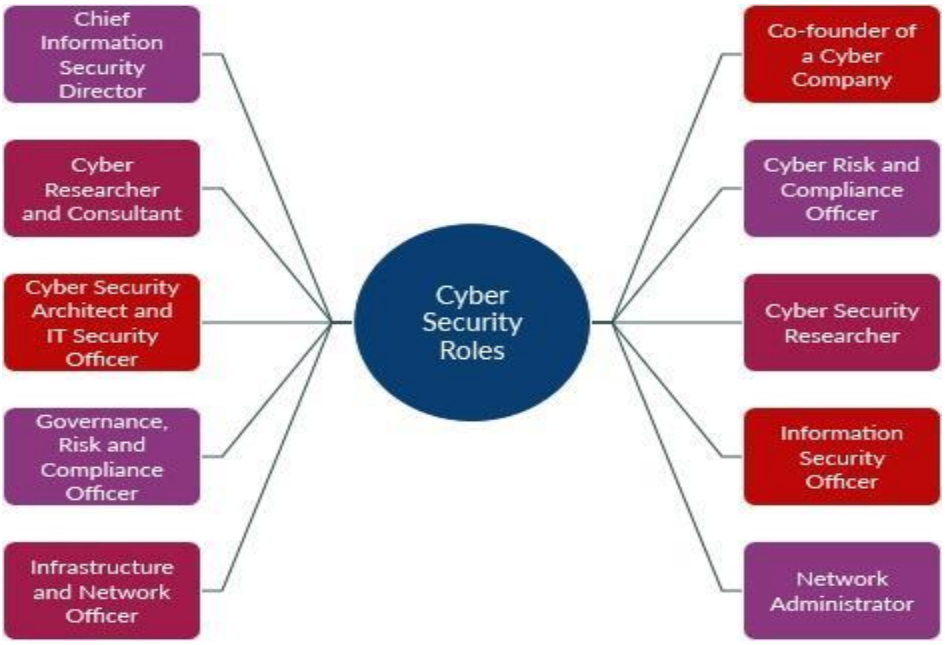
Participant 4 explains further that during major world events like the Russian-Ukrainian war, they prepare their organization to be ready for possible malware that could be used for MFA (Multi-Factor Authentication) fatigue attacks. MFA fatigue attacks happen when malware is used to disrupt the cyber system of an organization like a bank—such that a continuous request for additional authentication is triggered to frustrate the customer to authorize action their account.

The multi-factor authentication is an extra layer of authentication for customers' accounts which could be in the form of biometric verification, answer to a question, mobile phone prompts or request for PIN, in addition to the usual sign in process through user identification. If the risk for the organization is high, they may rather implement a unique password option that changes after few seconds as the organizations MFA method. The MFA has become additional process to secure customers in the cyberspace.

Participant 2 mentioned that he is involved as a governance, risk, and compliance officer in a company. Participant 2 started his career as a cyber information security officer for both public and private sectors. As an information security officer, Participant 2 was responsible for asset protection, cyber incidence detection and response to incidence, detection of vulnerability and analyses of cyber traffic to ensure safety.

Figure 1

Cybersecurity Roles

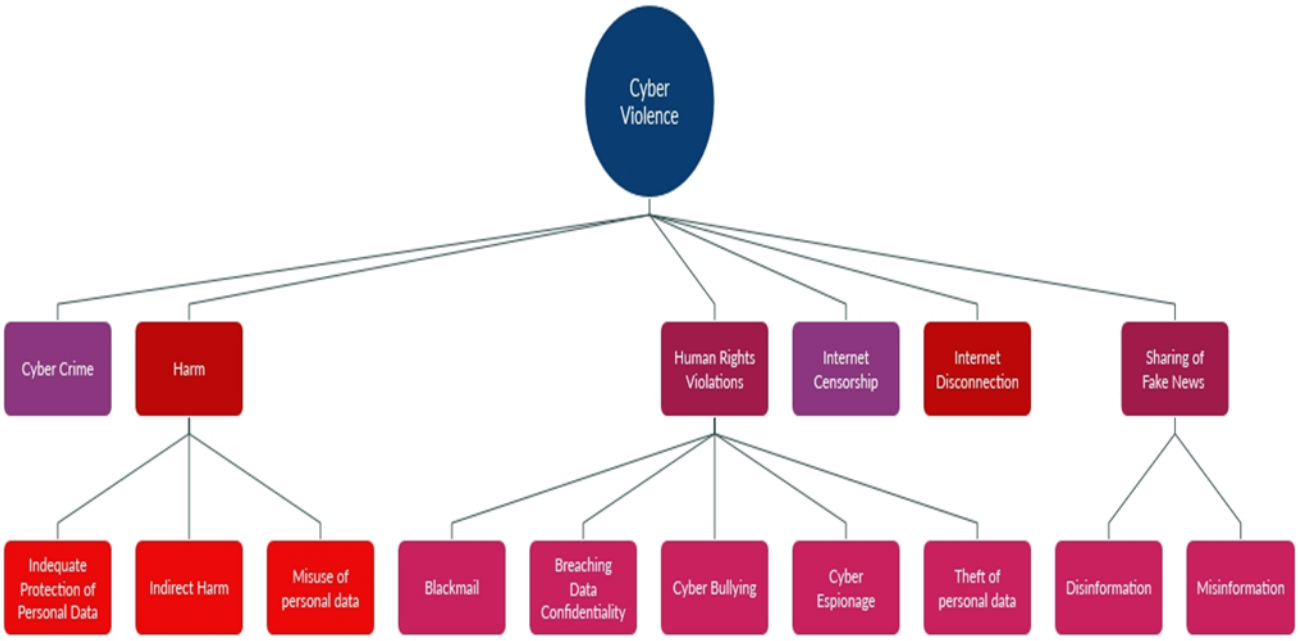


Understanding Cyberviolence

The research participants explained their understanding of cyber violence in different but sometimes intersecting ways. The subsections following will discuss the details of each component of cyber violence. Integrating the responses from participants, cyber violence can be viewed from six angles: crimes; harms; human rights violations; censorship; disconnections from the cyberspace and sharing of fake news which make the internet user insecure physically, psychologically, or financially. These conceptions of cyber violence explain the shortfalls of some existing theories and concepts among researchers and practitioners.

Figure 2

Components of Cyberviolence



Conceiving Cyberviolence as Cyber Crime

A participant describes cyber violence as an act of using a computer to cause injuries, which could include injuries to reputation or assets that should be deem as criminal. Marlin-Bennett's (2022) position that peacebuilding should be concerned with only the *crimes* in cyberspace that have geopolitical underpinnings contradicts some aspects of the conception of cyber violence as cybercrime. In other words when cybercrime is committed by state actors, or with the support of a country to achieve certain political objectives, then it should be considered as a domain of peacebuilding. This assertion aligns with the requirements established by Buçaj (2020) as explained in the earlier segment.

Buçaj (2020) differs from Marlin-Bennett (2022) in the sense that cyber action should be considered as violent only when it is targeted at the essential services of a country or state. This conception excludes violence targeting non-state institutions that are equally important.

Individual citizens make up countries so whether violence affects the individual or society as whole, it should be considered. Moreover, increasingly, non-state actors are participating in the perpetration of violence in hybrid war situations. More recently, concepts like “hybrid war” tend to incorporate non-classical approaches such as violence from criminal gangs into conventional military tactics, explaining the phenomenon that high-intensity violence is not happening only under the banner of inter-state conflicts (Libiseller, 2023, p. 5).

For this purpose, cyber weapons or violence are considered as hybrid war mechanisms. And these mixed methods are increasingly being used to make conflict atmosphere complicated and difficult to elicit reprisal attacks (Libiseller, 2023). The cyberviolence component of hybrid war might not be fully accounted for under current provisions in the Laws of Armed Conflict. International legal principles prohibit countries from using violence against another state unless for the purposes of defense against similar action from another country (Buçaj, 2020). The somewhat borderless context of cyberspace and the rise in cyber abilities of private actors make it hard for existing laws on international conflict. Again, the jurisdiction of international law might extend to only cyberviolence targeting important state-level institutions or services for political reasons.

Part of the challenge itself is that the laws on international conflict were put in place long before the advancement of cyber weapons. Meanwhile it is difficult to verify the origins of violence in the cyberspace with the advent of newer forms of technology (Buçaj, 2020). In addressing some effects of modernization, Kaldor (2013) mentions that “the distinction between state and non-state, public and private, external and internal, economic and political, and even war and peace are breaking down” (p. 2). Some important elements causing the so-called

newness of wars beyond the differentiation of actors involved, include the strategies and objectives (Kaldor, 2013).

Increasingly, the wars in the contemporary world are being fought for identity reasons than for geopolitical purposes. Identity objectives serve the interests of unique portion of a population whereas geopolitical objectives focus on attaining certain aspirations from political and ideological points for an entire population. This description of newness should allow for rethinking of some of the old norms and laws (Kaldor, 2013). What then happens when there is cyber violence targeting essential services of a country, yet the political objectives of the attackers have not been established?

Yet Marlin-Bennett (2022) explains that the so-called cybercrimes could contribute towards cyber peace in some instances. Such that, cyber tools or actions which may be tagged as illegal in some countries can be used to bypass the monitoring systems in support of the human rights of vulnerable people in tyrannical regimes. Many countries are trying to pass laws to deal with different aspects of their cyberspace. Some cybersecurity activists explain that enforcing laws criminalizing the deployment of cyber tools like advanced forms of encryption may harm the protection of human rights (Lewis et al., 2017; Marlin-Bennett, 2022). What is considered as cybercrime could be controversial because some cybercrime laws may be harmful to people's freedoms.

At the same time, there may be harmful activities in the digital space that remain unregulated. But the research argues that the cyber peacebuilding domain should be concerned about understanding issues that are labelled as criminal and not. In addition, cyberspace peacebuilding should include issues that are laced with geopolitical intentions or not.

According to the Council of Europe (n.d.-b), criminal jurisprudence may not be able to attend to some aspects of cyber violence. The Budapest Convention which was spearheaded by the Council of Europe became the first international legal instrument attempting to criminalize certain acts of violence in cyberspace such as unauthorized access, obstruction to a computer system and data; production, or acquisition of tools to destroy or have unauthorized access to computer systems and data.

Tagging this Budapest Convention as an international treaty is inadequate because many other countries have neither embraced the treaty nor ratified it. The Budapest Convention also makes provisions to render criminal activities such as the intentional faking of computerized data for fraudulent purposes; online child pornography and intellectual property infringements (Council of Europe, n.d.-a). Countries who have signed onto this convention are supposed to proceed with their own laws to bring life to the convention.

Disconnections from the Global Internet

Following immediately from where I left off is a phenomenon that one participant described using the term, “balkanization”, or carving up of the internet. This participant explains that the global internet is increasingly becoming a divisive tool whereby different countries are creating their own versions of the internet and restricting access or blocking access entirely of their citizens to the global internet infrastructure. There are certain elements of balkanization of the internet that may be related to the subsequent parts of this paper. How does this phenomenon contribute to cyber violence against people?

Janc (2017) examines the happenings pushing balkanization: increasing internet traffic from non-western countries, restrictions, or denial of certain internet networks in some countries, and some countries wanting autonomy over their data and infrastructure. Hill (2012) notes

economic interests as one the push factors of rising internet barriers. These developments are decreasing the global reach of the internet because states have begun erecting virtual barriers like the “Halal Internet” of Iran which helps the Iranian government remove internet traffic coming from the “west” (Janc, 2017).

This brings to the forefront some dimensions such as what extent a state could be allowed to control personal data on the internet and how anonymity could be ensured when it is required online (Spence, 2018). The idea of having a borderless internet, that is global internet protocols with very little controls, is also confronted with its own challenges like data breaches by some private, online attacks on essential services and the spread of counterfeit information or news (Spence, 2018).

There are two opposing ideas about how the internet should be governed. Countries like Russia, China and India propose a global institution similar in form to the United Nations and its specialized agencies that will handle issues about the standardization or global governance of the internet. The group being led by the USA advocates for the existing system that is dominated by private actors. The US, seeks to ensure that state-actors have limited roles in the management of global internet (Hill, 2012).

Within the existing arrangement, the Internet Engineering Task Force (IETF) which is an “association of researchers, academics and engineers, many of whom were instrumental in the early development of the Internet” takes the lead in effecting key changes to the global internet system (Hill, 2012, p. 51). The IETF tries to seek the inputs of other engineers in the field before making its decisions. However, the IETF approach is criticized as having little representation or participation of experts from other parts of the world and controlled by the USA scientists and experts.

Conceiving Cyberviolence as Harm

This section explores the meaning of harm itself. All four participants agree that cyber violence cause of harm. Participant 1 argues that cyber tools could be used to perpetrate direct harm to a person or assets. Using the same terminology, the participant further highlights that the misuse of personally identifiable data such as social security and phone numbers, passport, and credit card information as well as home address causes harm too.

Participant 1 explains that depending on the nature of the abuse of these data, the harm caused could be direct or indirect. In explaining the extent of harm weaponized cyber capabilities could cause, Participant 1 explains that people with malicious intent could "trigger explosions in the electric facilities…turn off electricity in multiple cities". The Council of Europe (n.d.) tries to make the argument about cyberviolence having the ability to be direct, according to its severity.

The Council of Europe also gives the hint that by direct harm it means violence that could physically harm people. Further, the Council explains that when the functioning of essential services fire service, and medical services is disrupted using cyber capabilities, then such an act may be causing harm physically. It also uses terminology like cyber-related harms such as threats and hate speech which could lead to physical actions to underscore the differences in direct and indirect violence.

This strategy gives some signal that cyberspace could be a medium through which harm could be caused but could be weaponized to cause the harm itself. In Peace and Conflict Studies doctrines, harm could be considered as direct or indirect. Agrafiotis et al. (2018) make the argument that cyberviolence could be direct in cases such as the destruction of assets, and misuse or rendering of assets incapable of performing their function. Agrafiotis et al. (2018) label humans as assets. By their logic, some of the direct harm that could be caused to humans include

death and torture. In addition, Agrafiotis et al. (2018) made references to other forms of harm such as financial, mental, and social harm.

Participant 2 equally notes that when someone's personal information leaks on the internet, that is harm caused, and then the outcomes of the leakage could cause another form of harm such as financial loss. In addition, when a person suffers from defamation through data leakage, then that person would be suffering from harm. From these statements, it could be that harm could be the actual act of cyberviolence or the effect of violence.

Data leakage could happen because of a personal error. Yet participants agree that data leakage as result inadequate protection customers' data mishandling or just mere misuse of data by companies has become a greater concern recently.

I would say first of all, if the organization does not protect the customers data…this data can be compromised or exposed to unauthorized third parties. And some of these, some of these data sets are confidential as personally identifiable information. Once they fall into the wrong hands, they can be used for …malicious activities. Participant 4.

The statement underscores the fact that institutions could be contributing towards this form of violence against a client. Yet Agrafiotis et al. (2018) note that a lot of institutions do not adequately know the extent of harm they could cause through their actions or inactions. The There may be links between harm being caused by not protecting the client's data to the effects of the action as explained earlier. Participant 3 explains that it is important for organizations to seek express consent from clients before processing their data, making risks of data misuse clearer. This gesture equally helps to further streamline the relationship between the organization and the client. The discussion

on seeking customers' consent in the handling of their data would become useful in the latter parts of the analysis on cyber peace.

Cyberviolence as Human Rights Violations

One could say that cyberviolence, whether seen from the perspective of crimes committed or from the angles of harm caused, also concerns human rights violations. How cyberviolence affects human rights is what this section of the research focuses on. All four participants agree that cyberviolence affects human rights. Participant 1 mentions how cyber bullying is damaging the rights of people, describing cyber bullying as harm caused morally or verbally to children in the digital space.

Participants 1 and 2 mention blackmailing as a human right issue happening in the cyberspace. They explain blackmailing as manipulating a person's data to illustrate a negative image about the person. Participants 2 and 4 cite that the breaching of confidential data constitutes human rights abuse. Participant 2 explains that exposing people's data means that their right to privacy has been broken down. Effects of leaving customer data not protected may include bullying, blackmailing, the harm, or threats to life. Sometimes the mishandling of personal information as discussed earlier in the section on harms, may be because of the mistakes of victims themselves, and not by third parties such as of companies and state institutions.

In other instances, organizations may try to take necessary steps to secure data, but other persons would use cyber tools to break into systems of institutions to steal data. Participant 1 mentions theft of customers' data as a human right abuse. The point is that just as unauthorized breaking into someone's private physical space constitutes a crime, doing the same in cyberspace should equally be criminal.

In the example provided by participant 4, when health records of a person are exposed by an organization, there may be serious human rights abuse. The participant explains further that health records document vulnerabilities of humans, and the information could be used by other people to bully or blackmail the victim. Thus, there must be imposed responsibilities on organizations, or people who may chance on other's exposed data to ensure its safety.

All the participants agree that cyber espionage also infringes on the human rights of people. Participant 1 mentions that some governments spy on human rights activists by stealing data about the people's location. In other cases, both Participants 1 and 2 explain that the motivation for tracking people's activities online is to gain economic or military advantage over others. Participant 1 argues that the abuse of people online in the form of espionage could be legal or not, depending on the county. In other words, certain countries may have legalized some forms of cyber abuse.

During the mobilization for inclusive civil liberties in the USA, Martin Luther King Jr. argued that there were "just and unjust laws" operating in the USA (Mingo, 2018, p. 683). Martin Luther King Jr. explained that just laws must be respected, whereas the unjust ones should be disregarded. The civil rights advocate defined an unjust law as one that dehumanizes (Mingo, 2018). Mingo (2018) observes that using existing legal arrangements such as suing, not respecting the unjust laws while making them public, and moral and civic education helped to get discriminatory laws changed in the USA. However, it is observed that not obeying unjust laws could come with consequences like arrests and imprisonment as happened in the case of Martin Luther King Jr (Mingo, 2018).

Participant 3's statements suggest that private entities may be involved in espionage as well—to understand things like purchasing trends, the client base of competitors, and to secure

favorable advantage for themselves. In a related argument, Participant 4 mentions that the source of espionage could be within or outside of an organization or a geographic location. Cyber espionage negatively affects the handling of customer data and presents direct threats or harms to people. Describing how cyber espionage affects human rights, Participant 4 concludes that spying of people or organizations makes victims vulnerable.

The foundation of human rights hinges on ensuring that human beings have a dignified life (Qureshi, 2018). The International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR) and other legal provisions focusing on children and migrants make the protection of human rights an important responsibility (Florek & Eroglu, 2019; Qureshi, 2018, p. 291). The rights to express oneself freely and personal privacy form part of the ICCPR. Situating the right to privacy within the scope of civil and political rights, it could be said, that the exploitation of person's personal data such as sex, and political preferences constitutes an infraction.

In other cases, human rights abuse might not be only about the breach of data but physical harms and crimes in the virtual realms also relating to human rights of people. Bullying and harassment on the internet are part of this. Viewing things from human rights doctrines, reputational destruction could cause harms that are intrinsically linked to the ability of a person to live a dignified life. In the physical world, some countries have used human rights arguments to explain their military action in another country. These arguments tend to focus on the universality and sacredness of human dignity as embedded in human rights (Florek & Eroglu, 2019).

Understanding Cyberviolence through Internet Censorship

As discussed under the section on internet disconnections, there are increasing barriers to internet connectivity and access to materials in the virtual space. Through discussing the extent to which censorship tends to be justified or permitted by countries, this section explores the phenomenon further. The participants are divided in their response on whether censoring the internet should be allowed or not. Participants 1 and 2 argue that censorship should not be permitted, under any circumstances. In contrast, Participants 3 and 4 explain that censorship may be necessary under certain scenarios. Participants 1 and 2 mention that limiting the flow of information or access to information infringes on free speech.

Participant 2 argues his point further— the government consists of people who manage the day-to-day affairs of the state. Since cyber censorship might also include intrusion into individuals' online spaces, people who work in government could be influenced to use data harvested to cause harm. Participant 2 also notes that when certain content is blocked online, some people may use computerized tools or software to bypass censorship, such that, censorship does not become an effective way of ensuring social control. From a different angle, Participant 3 acknowledges that because some countries are being aggressive towards others in the cyberspace, censorship may become a useful tool for cyber defense.

Participant 4 purports that combating crime is an integral mandate of the state, so there might be the need for the state to prevent the production and distribution of some services online because they are regarded as criminal. In another instance, Participant 3 notes that censorship may become a useful tool to stop the dissemination of false information.

While the challenge of fake news will be explored in the immediate section, Participant 3 explains the need to combat fake news. Fake news could inhibit the intellectual capacity of younger generations. Yet, this participant adds a caveat: countries using censorship as a

mechanism for cyber defense or to stop the spread of fake news should adhere to global human rights standards. Participant 3 mentions that if there is any censorship at all, there should be worldwide standards and institutions which guide censorship.

Participant 4 outlines three forms or degrees of cyber censorship: extensive, slightly extensive, and limited censorships. Participant 4 explains that states like North Korea employ an extensive internet control regime, where an internal system, an intranet is what is mostly available to citizens. However, an extremely limited portion of the population in North Korea has access to the worldwide internet. In the case of somewhat extensive or semi-extensive internet censorship regimes, the participant mentions that countries like China permit access to the worldwide internet for the wider population, but many websites or services are blocked to citizens. Participant 4 cites the United Arab Emirates (UAE) as a less severe scenario of internet censorship, where specific content is disallowed.

Amnesty International (2017) explains that cyber espionage could cause people to censor their own speech, knowing that they are being monitored. Yet cyber espionage and censorship are not exactly the same. Ververis et al. (2020) also acknowledge that censorship affects the arguments about online freedom of speech, open, and accessible internet. The organization mentions that censorship is much more than just stopping some services or content from working on the internet. Censorship also includes the arrest of people who have expressed themselves on digital platforms.

Dainotti et al. (2014) observe that censoring the internet may include full denial of access to the internet by turning off a central switch of an internet service equipment or causing virtual interruptions within the router or packet. Censorship can also be done on a large scale through interrupting the outgoing Border Gateway Protocol (BGP) traffic functionalities of an

important router (Ververis et al., 2020, p. 452). Through packet filtering, some conditions can be set for the router to stop communicating to some websites as a whole or some information on those websites. On another hand, packet filtering could be used to bypass censorship, when a router is configured to be resetting the block signals it may be receiving from another router. Some governments tend to use arguments about culture and religion to justify their decision to censor (Dainotti et al., 2014).

By analyzing censorship in France, Iran and Turkey, Ververis et al. (2020) propose five motivations for censorship as, "the ruling system, institutional setup, national identity, technical ability, and political opportunity" (p. 450). Some internet dependent services may be denied by some states because they may not be regarded as legal. At the onset of the phenomenon in the 1990s, censoring the internet was being associated with mostly autocratic regimes. However, censorship has since extended its reach to the so-called democratic states (Ververis et al., 2020).

Whether they are linked to history, morals, culture, politics, religion, or law, values are the bedrock of censorship. Just as religion may be the reason for which internet content bearing pornography may be stopped, the distribution of some music, books, or movies may be hindered because of legal concerns about intellectual property (Ververis et al., 2020). Since internet censorship by non-democratic states is popular in literature than democratic states (Ververis et al., 2020); how does censorship look like in democracies? In France, there are laws that prohibit the production and dissemination of materials that are not suitable for minors.

There is a 1990 law in France that also bans the making of contents that defames or discriminates, digitally or physically. The French laws require the Internet Service Providers to block content that is not permitted. A 2015 law was enacted to pave way for relevant authorities to block websites that seem to be promoting terrorism without following the full judicial

processes. Despite these restriction mechanisms, France is generally regarded as a country with unrestrained access to internet since the level control is mostly low (Ververis et al., 2020).

Ververis et al. (2020) conclude the internet censorship regime is more transparent in France than that of Turkey and Iran and oftentimes, the tribunals in France tend to provide explanations to decisions to block certain websites. Scholars and practitioners differ on the control of the internet by the state. Some people advocate for certain levels of restrictions on the internet to protect children or ensure social safety. The other scholars also argue for unrestrained connectivity to the internet on the grounds of human rights (Ververis et al., 2020). Zarras (2016) mentions free speech on the internet is particularly useful in contesting corrupt, and deceitful regimes.

Fake News and Cyberviolence

Progressing further, this research explores how the sharing of fake news impacts the debates about freedom of expression in the cyberspace. A major positive about the internet and the advent of social media is people having the platforms to communicate their opinions, and other information in an easier and faster way (Cheng & Chen, 2020). But easy access comes with additional burden for society. Society has to deal with a sustained surge in the creation and spreading of news that might not be reliable, accurate, trustworthy, and fair (Meel & Vishwakarma, 2020). The era of social media platforms like Facebook makes the development difficult to handle (Adjin-Tettey, 2022). Facebook alone offers wider reach for news—the platform had a little over one billion people using it each day, at the end of year 2016 (Tandoc et al., 2018).

Participant 1 holds a similar view as expressed by the authors above that fake news is not new to the world; it is just that technological innovations have changed the nature of it.

Participant 3 states that mobile phones allow people to access and circulate news faster than before. Making a distinction between misinformation and disinformation, Participant 4 notes the challenges of fake news to handle with care, mentioning that in some cases, people may not be aware that they are circulating fake news.

Meel & Vishwakarma (2020) use a broader category of "false information" to cover subcategories like "fake news", "misinformation", "disinformation", "rumor", "clickbait", "hoax", "satire/parody", "opinion spam propaganda" and "conspiracy theories" (p.5). Adjin-Tettey (2022) notes other terminologies used in place of fake news as: "media manipulation"; "information warfare"; "information pollution" (p.2). According to Meel & Vishwakarma (2020) fake news is the circulation of incorrect information disguised as genuine news. Meel & Vishwakarma (2020) distinguish misinformation from disinformation.

Disinformation is a premeditated spread of fake information to achieve certain objectives whereas misinformation is when someone shares information being unaware that it is fake. Fake news could also be spread when people are misinformed by way of news even if the bearer of the news is not aware that the information is incorrect (Baek et al., 2019). Coming with another perspective, Baek et al. (2019) establish that fake news occurs when incorrect information is intentionally presented in a journalistic style to achieve preconceived objectives. Some persons or organizations create or disseminate incorrect content to make financial gains whereas others may circulate wrong information that gives them political advantage over their opponents (Adjin-Tettey, 2022; Tandoc et al., 2018).

Participant 2 makes the claim that some people might use fake news as a clickbait to harvest personal information from their victims. They may then use the personal information to harm their victims. Participant 1 also provides two reasons why fake news may be distributed: to

manipulate human beings to achieve some hidden goals, and as a mechanism through which some people plant or test ideas. Participant 3 shares a similar position that fake news is just a manipulative strategy.

Participant 2 acknowledges that some negative effects of fake news on society are the damage to the personal image of victims and bringing about social deception. Participant 2 mentions the example of fake news being used as a weapon to deceive electorates during the 2016 presidential election in USA. Participant 3 explains that the fake news causes panic in society. Going further, Participant 3 observes that fake news may transform valuable social norms into harmful ones. This participant justifies the earlier statement by saying that when legitimate news is replaced with inaccurate information without any corrective measures, the wrong information may be upheld as authentic.

Talwar et al. (2020) agrees that the phenomenon has the tendency to cause or worsen social divisions, and damage to personal and corporate reputations. Fake news is equally causing some erosion of trust in democratic norms such as the gatekeeping roles of the media and free speech (Adjin-Tettey, 2022). Social media algorithms could make some people the target of some fake news by getting the targets to alter their opinions (Meel & Vishwakarma, 2020).

Talwar et al. (2020) again concludes that sometimes people share fake news not with the intention to harm but because they are just in a hurry to provide information to close associates.

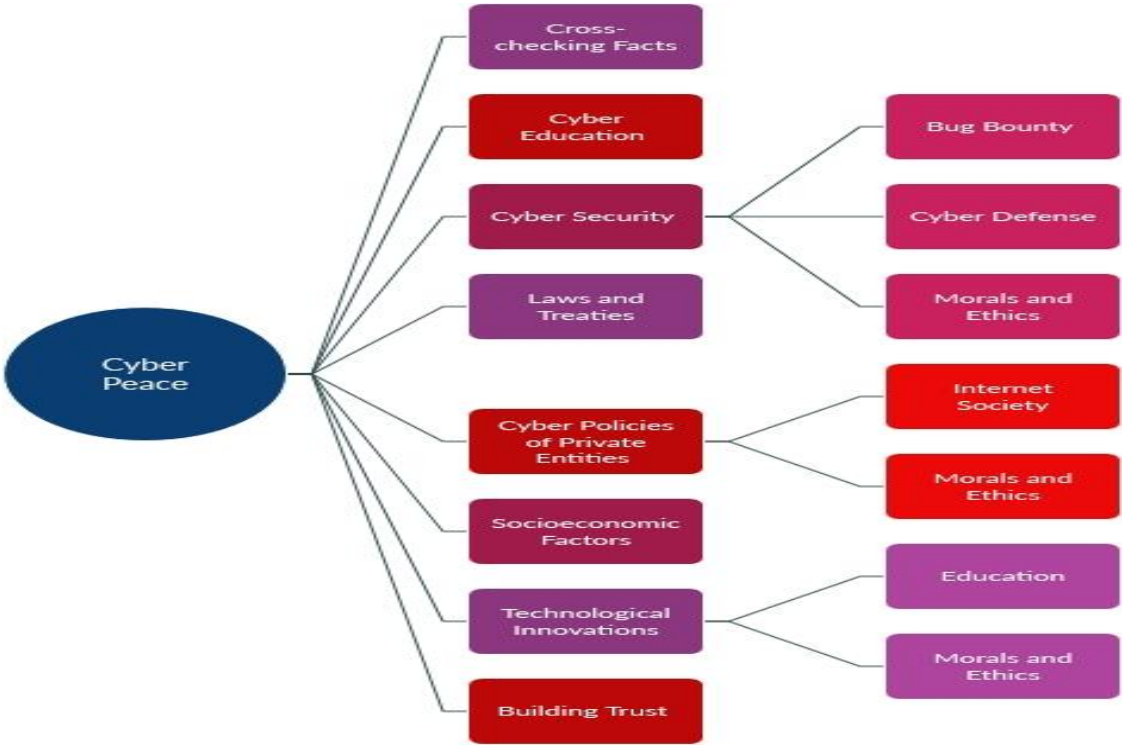
Participant 1 indicates that though new technologies will have to be invented to tackle the menace, fake news is too complex to be handled by any future technology alone. Participants 1 and 3 advocate for human focused actions that can ensure that the accuracy of information is checked. In addition, Participant 3 advocates for censorship and legislation of online content to deal with the threats of fake news. Participant 4 also recommends that freedom of speech should

be strongly protected online. However, Participant 4 also mentions that if challenges like fake news seek to weaken national security, then the action could be addressed using established standards in a transparent way. This participant notes that transparent standards are necessary in determining situations that pose threats to national security, in order to prevent abuse by authorities. Adjin-Tettey, (2022) also explains that when a person's "media and information literacy" levels are high, the person may be less likely to disseminate fake news (p.1). This is because these people would be more capable of identifying inaccurate information.

Understanding Cyber Peace

Figure 3

Components of Cyber Peace



The interviewees explained what they understand as cyber peace. They described cyber peace from the perspectives of actions of individuals, private companies, governmental and intergovernmental perspectives. The figure above identifies data collected from participants, who see cyber peace organized as conditions or actions of cross-checking information, cyber education, cybersecurity, cyber laws and treaties, cyber policies, socioeconomic factors, technological advancements, and trust building. The data from each of these elements will be presented in the sections following.

Cross-checking Facts

This section digs deeper into fact-checking as a cyber peace building activity and a solution to fake news. Following up on the last section on cyber violence, the participants are united about the increasing influence of fake news on society. Some participants argue that sharing correct news should be a collective responsible for preserving peace and stability in the cyberspace. Fact-checking in the digital era is quickly evolving into an important domain in journalism or information management, such that, new roles are being created for such activities (López-Marcos & Vicente-Fernández, 2021). Meel & Vishwakarma (2020) argue that while digital tools could be improved to filter fake news, teams could be formed to fact-check contents. Moreover, other strategies like correcting incorrect information in circulation, and blocking fictitious accounts circulating such news were proposed.

There are existing software or browser extensions such as Credfinder, Hoaxy, COMPA, and the Flux Flow, which attempt to tackle fake news. These tools are not without limitations. Hoaxy can detect fake contents almost half a day after the incidents. It is also easier for COMPA mechanism to identify incorrect news to be bypassed because it depends heavily on the social network conduct of the bearer of the fake news. The Flux flow is built to work on content generated on Twitter. Crefinder is also configured to discover incorrect information on Twitter but it fails to identify pictures that are falsified (Meel & Vishwakarma, 2020, pp. 5–7). The digital space is in dire need of tools that can unify the strengths of the existing ones, to enable instantaneous recognition and attribution of fake news across different social media sites (Meel & Vishwakarma, 2020). Please see Figure 4 to note in more detail fact-finding tools in Cyberspace.

Figure 4

Fact-checking Tools in Cyberspace

List of Fact-checking platforms.

Name	Salient features	Reference
TwitterTrails	An interactive online tool for investigating the propagation characteristics, refutation of stories shared on Twitter, origin, and trustworthiness	Finn, Metaxas, and Mustafaraj (2014)
TweetCred	A real-time web-based system with a rating between '1 and 7' to assesses the credibility of each tweet in the twitter timeline.	Gupta, Kumaraguru, Castillo, and Meier (2014)
Hoaxy	A platform for collection, detection and analysis of online misinformation and its related fact-checking efforts.	Shao et al. (2016)
Emergent	Web-based automatic real-time rumor tracker; tracks social media mentions of URLs associated rumors.	Emergent (2019)
CredFinder	Analyses user and content features to find out the credibility of tweets. Works in real-time as an extension of the Chrome Browser.	Alrubaian et al. (2016)
RumorLens	A tool to aid journalists in segregating posts that spread a specific rumor on Twitter, by traversing the size and distribution of the audience.	Resnick, Carton, Park, Shen, and Zeffer (2014)
COMPA	System to detect compromised social network accounts. Message characteristics and behavioral user profiles are used for misinformation detection.	Egele et al. (2017)
FluxFlow	Interactive visual analysis system to detect, explore and interpret anomalous conversational threads in twitter	Zhao et al. (2014)
REVEAL	Verification of social media content mainly concentrating on image authenticity from a journalistic and enterprise outlook.	REVEAL (2014)
InVID	The platform supports authentication, fraud detection, reliability and accuracy checking of newsworthy video content and files spread via social media	InVID (2017)
ClaimBuster	Allows users to perform live fact-checking with the help of finding out factual claims	Hassan, Arslan, Li, and Tremayne (2017)
TruthOrFiction	Covers Politics, religion, nature, aviation, food, medical, etc., Email rumors are classified in truth and Fiction	Truth or Fiction - Fact Check (2019)
Snopes	Covers all domains of the news; label videos and News articles in 12 categories, True; Mostly true; Mixture; Mostly false; False; Unproven; Outdated; Miscaptioned; Correct attribution; Misattributed; Scam; Legend	Snopes.com (1994)
FactCheck	Intends to reduce the level of confusion and deception in U.S. politics. Analyses TV ads, debates, speeches, interviews and news and labels them as True; No evidence; False	FactCheck.org (2003)
PolitiFact	Covers American politics; After fact-checking labels articles as True, Mostly True, Half True, Mostly False, False and Pants on fire	Fact-checking U.S. politics-PolitiFact (2007)
Fake News Tracker	Predicting fake news from data collected automatically from social context and news, also provides effective visualization facilities using NLP and deep neural networks	Shu, Mahudeswaran, and Liu (2019)

Note. Adapted from Meel & Vishwakarma (2020, p. 10). Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. *Expert Systems with Applications*, *153*, 112986.

It is equally important to circulate the facts that have been discovered in a measure that is more potent than how the fake news was distributed. Digitals tools alone might not correctly point out fake news, as these tools require enormous human interventions. Some digital companies have started putting in place teams to fact-check certain information of public interest (Li & Chang, 2022). Li & Chang (2022) acknowledge in their study that fake news circulates more quickly than factual news largely because people respond more emotionally to incorrect

information. In addition, there are inadequate proportions of news in the digital space that undergo verification.

PolitiFact is a Nongovernmental Organization (NGO) that is engaged in verifying important statements made by politicians of the USA, especially on different social media sites. PolitiFact analyses public pronouncements against publicly available information online, and opinions from specialists on the matter in question to conclude on its veracity. The organization goes further to make the results of its findings known on platforms like Twitter (Li & Chang, 2022). In addition, the dissemination of their facts is done through their newsletters that are circulated every week (PolitiFact, n.d.). The international television channel France 24 (n.d.) also has a weekly broadcast session focusing on analyzing widely circulated images, and videos suspected to be distorted. The channel invites experts to analyze and make their findings know during the live telecasts.

Cyber Education for Cyber Peace

Three out of the four cybersecurity specialists interviewed establish that cyber education is a particularly important action for cyber peace. Some participants acknowledge cyber mentorship could create opportunities for new cybersecurity professionals. Participant 1 argues for cybersecurity education for all users of the internet so that they could self-protect. Cyber education should be centered around new cyber systems that could assure some level of safety. Participant 2 mentions that he educates people about their rights within the digital environment. The education may include knowing which rights one has over personal data. Participant 2 explains that this form of education should be tailored for public office holders like lawyers and judges. Mass education is strongly recommended.

There is the need for more specialists with skills in cybersecurity. Multidisciplinary cybersecurity courses can prepare people to understand the socioeconomic aspects of digital security. (Austin, 2020). Online courses, university programs, nationwide sensitization activities are some forms that cyber education could take. Caelli (2020) mentions that security education programs tend to include systems administration and management, systems certification, risks analysis, and system security (p. 12). Sometimes using "information assurance" in place of cybersecurity may be more encompassing because it may integrate the other aspects of cyber violence beyond the popular discourse of state level attacks (Caelli, 2020, p. 13). This is because cybersecurity programs have evolved beyond the boundaries of Science, Technology, Engineering and Mathematics (STEM) fields to include business, legal, political science, and international relations domains.

Caelli (2020) cites the Australian Computer Society as having distinct certification for technological and policy aspects of cybersecurity. The goal is to get everyone to have some knowledge about staying safe in the digital space while performing their normal roles (Blair et al., 2020). The emphasis on the development of human abilities to understand the cyber world is very important because nearly two-third of cyber violence victims suffer from human-related lapses or breaches that perpetrators exploit. Linking these viewpoints to costs, about three trillion dollars worldwide were lost in 2018 as a result of cyberviolence. This confirms massive loss caused by human mistakes or other actions. Following, Shoemaker et al. (2020) recommend these important areas of cybersecurity to be included in cyber education: "data security, software security, component security, connection security, system security, human security, organizational security, and societal security" (p. 94).

Regarding data security, it will be important to have basic education on components such as encryption, authentication, safe data storage, and cyber forensics. Software security subject areas may include configurations and vulnerabilities. Component security education may be comprised of systems for identifying and managing physical cyber infrastructure. Connection security should educate on areas such as securing networking infrastructure. System security should touch on components like controls for accessing, documenting, and operating the systems. Human security would entail education centered around data privacy and social engineering schemes employed by hackers. Gaining knowledge about organizational security entails taking lessons about cyber risk, policy administration and societal security would require that people are equipped with information about how cyber criminals operate and personal safety strategies on the cyberspace (Shoemaker et al., 2020).

Cyber education should adapt some strategies from social science methodologies because the ways people behave in the cyber environment hugely affect their security. Cyber training should balance the social and technical dimensions of the digital space to promote safety (Withers & Austin, 2020).

Cybersecurity as Cyber Peace

The section examines cybersecurity actions or tools that assure stability in the cyberspace. The participants agree that cybersecurity is an avenue through which peace can be ensured. Participant 2 states that when cybersecurity tools, and actions are used to protect freedom of speech, and general safety of people, then peace is being maintained. Participant 3 makes the case that people may have peace when they are aware that they are not being spied on digitally. In addition, cybersecurity practices that assure peace may include upholding the integrity of online financial transactions as captured below in the exact words of participant 2.

> So, you buy something, you know your product that you bought. You gonna get that same product. There is nothing like you bought something, and then, before you know your credit card information is stolen.

This statement from the participant also indicates that using cybersecurity to protect people's data is included in the cyber peace domain. The participant goes ahead to explain why encryption of data should be an important cyber peace practice. Participant 3 has a similar view that protecting the financial interactions of people online is integral to ensuring peace because finances affect the survival of people. When data are encrypted, the data may be prevented from being intercepted by another person, who could use that data to harm their victims. Zero-trust policies in organizations deter their employees from unauthorized access and abuse of data.

Participant 2 observes that a zero-trust policy also means that the employees of organizations should be limited by the kinds of customer's data they have access to and, under what conditions that they have access. Examining the socioeconomic importance of cybersecurity, Participant 2 notes further that skills and tools in the cybersecurity field help to save companies a lot of money that would have been lost to attackers. This can eventually help save companies and people from bankruptcy.

Participant 4 defines cyber peace as the promotion of practices that lead to trust and positive behavior in the digital space. The participant gives an example of positive cyber behavior as bug bounty. Bug bounty is a situation in which a person who discovers cyber weaknesses in systems or software, shares same with the owners or creators to correct the. Participant 2 argues for overall cyber defense mechanisms for organizations. Professionals within the cybersecurity domain should ascribe to ethical principles that permit them to protect

peoples' data and always uphold safe conduct. It takes cybersecurity professionals with extraordinarily strong ethical principles to be involved in bug bounty (Participant 2 & 4).

Security could be explained as a state of wellbeing devoid of harms or any threats in financial, physical, and mental forms (Mishra et al., 2022). Cybersecurity itself can be described as actions that ensure the safety of data and internet connectivity of individuals and institutions.

Whereas the cybersecurity domain considers both social and technical dimensions, computer security tends to be focused on the technical things of computer hardware and software engineering (Veale & Brown, 2020). Mishra et al. (2022) explain cybersecurity as policies that shape the safe operation of computers, their networks, and data. This means that computer or cybersecurity innovation is just one phase of digital security. Therefore, cybersecurity may be comprised of actions both technical components such as Transport Layer Security (TLS), data encryption, and sociological aspects such as legislation, policies, and trust building. While these components of cybersecurity have been presented earlier, the rest will be analyzed at latter sections.

In a similar view, Kavak et al. (2021) explain cybersecurity as intermittent cyber risk assessment and designing requisite technological, and policy innovations to seal any identified risks, or to sustain the resilience of cyber infrastructure. The Transport Layer Security which is a technical element, helps to encrypt data travelling through the internet, yet this mechanism tends to be complex for some software makers to integrate (Veale & Brown, 2020).

Technical Innovation and Cyber Peace

The current section explores how technological advancements help to maintain peace. The details of this section will be about technical tools in the cyberspace that uphold people's right to privacy, expression, and access to the internet. According to all four interview

participants, technological innovations are crucial tools supporting cyber peace. Participant 1 explains that where there is appropriate regulation and governance practices, it will necessitate the development of new cybersecurity tools to achieve compliance. Invention of tools that can trace cyber operations, especially harmful ones, could be important. But cybersecurity innovations could pose another layer of challenge to peace if they are not used in transparent and fair manner—as previously explored under the discussion about the balkanization of the internet. As a result, technological innovations must go together with legal innovations that seek to uphold the freedom of everyone. These innovations must include a guarantee for accessible internet for the citizenry.

Cyber innovations allow for socially beneficial content such as some news channels that may have been blocked by some local authorities to be accessed (Participants 1 & 4). Participant 2 argues that cybersecurity innovations though important in ensuring stability, can also be exploited by dangerous actors to advance their activities. Unlike Participant 1, Participant 2 advocates for techno-legal balance, while Participant 1 argues for balance in technological innovation and user education in cybersecurity. Participants 2 and 3 explains further that cybersecurity inventions will not be of much benefit if most users do not understand how those innovations work or can be used. From Participant 3's viewpoint, inventions like Virtual Private Networks (VPNs) help to protect human rights like freedom of expression online because VPNs help people to escape from monitoring and censorship regimes.

Participant 4 observes that through VPNs activists' actual locations could be hidden. On another hand, security products like VPNs can enable people to abuse the guarantee of their rights. Since VPNs make attribution difficult, excesses such as the spread of fake news becomes a major social concern (Participant 3). The issue of fake news has been extensively examined

under the chapter on cyberviolence. Participant 3 notes that technological innovations should be accompanied with commensurate data protection laws to assure users' safety. Participant 3 adds another important feature for new cybersecurity tools; they should be less complicated to use. Encryption and decryption technologies could help protect personal information. Moreover, privacy settings permit individuals to have direct control over what kinds of data is collected from them.

The transport layer security (TLS) works with hypertext transfer protocol to facilitate internet communication from a sending server to that of a receiving server safer. Therefore, the function of TLS is to protect data in transit on the internet. The TLS protocols works faster than the protocols of Internet Security (Turner, 2014, p. 60). The TLS mechanism has the ability to encrypt the data to the servers and decrypt data coming to the users (Turner, 2014). Yet how well the TLS performs depends on how the server settings are reconfigured. Since encryption techniques of the servers can weaken, the TLS performance requires regular human monitoring, so that the system is always configured to work with stronger encryption algorithms. Some of the tasks within the human interface of TLS server configurations may make the internet network susceptible to exploitation by attackers (Turner, 2014). Encryption is a way of converting data into a format that makes it highly improbable for unsanctioned access and changes (Lewis et al., 2017; Schulz & Hoboken, 2016). This in turn helps to keep data safe and private.

The United Nations Educational, Scientific and Cultural Organization (UNESCO) explains that encryption is important in ensuring a safe, accessible and, liberal internet (Schulz & Hoboken, 2016). Where the servers of the internet connection points may not be configured to encrypt data (Schulz & Hoboken, 2016; Turner, 2014), encryption technology offers human

rights activists the opportunity to plan for their own safe communication (Schulz & Hoboken, 2016).

When there are inadequate policies guiding the handling of data, encryption may not be as useful—a compromised individual who has a legitimate access to data may mishandle the data. Some organizations prefer to use the end-to-end approach to encryption, where they claim to not have access to their client's personal data. Mobile phone makers like Apple have begun integrating "full disk encryption" on their products which, according to the company, denies them any room to customers' data (Lewis et al., 2017, p. 8). The policy and legal dimensions of encryption will be explored later. Sometimes, encryption techniques in certain forms can be bypassed (Schulz & Hoboken, 2016).

There are browser extensions and mobile applications that offer to encrypt and secure communication on the internet, at the individual levels. An example is an application that seeks to encrypt e-mail content, "Pretty Good Privacy" (Schulz & Hoboken, 2016, p. 48). The use of encryption technology also presents challenges to the investigation of criminal activities and security. Schulz & Hoboken (2016), and (Lewis et al., 2017) explain that there could be a situation where an instigative body goes through a fair and transparent process to gain access to personal data but encrypted data could make the control of the data impossible or extremely difficult. About 13% of portable phones ceased by the USA's Federal Bureau of Investigation between October 2015 and April 2016, were not within reach due to encryption technologies embedded in them (Lewis et al., 2017).

Private Virtual Networks (VPNs) are fast becoming an additional tool through which people can connect to the internet. VPNs authenticate and encrypt data to keep a safer internet connectivity. The use of VPNs is more popular in highly censored or controlled jurisdictions

(Lewis et al., 2017). VPNs work on the user's existing internet but convert identifiable information about the user into encrypted data that is not possible or extremely difficult for another person to read. That is, VPNs offer some levels of anonymity in internet connections while protecting data and connectivity. VPNs also help to overcome internet content limitations put in place for users at some locations. There are mobile and desktop versions of different VPN applications (Kaur & Sharma, 2020). The VPN supplier could have a policy to document a user's online interactions and provide the same to law enforcement agencies when requested. This also means some VPN suppliers may not keep a log of activities (Kaur & Sharma, 2020).

Cyber Policies of Private Entities

The interview participants explain that nonstate organizations have important roles to pay in sustaining peace in the cyberspace. Participant 1 explains that the legal provisions surrounding cybersecurity could have some loopholes that can be exploited by some companies. Moreover, policy on cyber education should make people aware that the harms caused by cybersecurity should not be limited to losing one's life or finances. According to Participant 1, private organizations can do much more than adhere to legal arrangements within their jurisdictions. Participant 2 notes that organizations should act beyond legal requirements and assume ethical responsibilities to ensure peace in the digital world. Participant 3 shares a similar opinion that since the evolution of technology is faster than accompanying laws private entities would have to assume some moral obligation to ensure the protection of society and individuals.

Organizations like the NSO Group who develop cyber tools to bypass some vulnerabilities in the digital world should adopt a stronger position that their products will be sold to only law enforcement agencies within countries that tend to follow transparent, and fair processes in accessing personal data (Participants 3 & 4).

Encryption could be a useful policy for organizations to secure data as part of their privacy policies, and organizations should enforce zero trust controls. The principle of zero trust is an internal control that permits organizations to limit an employee's unapproved access to clients' data (Participation 2).

Participant 2 argues further that threats to cyber stability might also come from some employees of organizations; therefore, actors within organizations should not have excessive access and control over sensitive data of customers. In addition, Participants 2 & 4 suggest that organizations should conduct ongoing cyber risk assessments to understand the evolving nature of cyber threats. Organizations should also have policies to train their employees about privacy laws and cyber threats (Participant 2). Nongovernmental Organizations like the Internet Society could intensify their collaborations with governments to propose unique and global privacy laws that uphold the safety of individuals within the digital world (Participant 3).

In their report for UNESCO, Schulz & Hoboken (2016) explain that private actors should integrate end-to-end authentication and encryption into their security policies. Schulz & Hoboken (2016) add that this policy is essential to the protection of privacy and other human rights. But more private organizations prefer to use types of encryptions that would allow for data to be retrieved, in specific instances like a request from law enforcement agencies. This mode of encryption is preferred because private actors want to avoid being held liable for some illegalities.

Yet other private organizations may not use zero log encryption because of customer preferences—these customers would like to recover their old data or synchronize their information from different internet sites (Lewis et al., 2017). Still, Lewis et al. (2017) explain that harms caused by the inability for individuals to access data due to encryption would be

nothing compared to its importance in protecting people and data. Ilvonen & Hellsten (2015) mention that companies should focus on having holistic cybersecurity guidelines since cybersecurity challenges are multifaceted.

Ilvonen & Hellsten (2015) define cybersecurity policy as a framework having ideas that could be used for containing cybersecurity challenges. Cybersecurity policy could include computer-related and management techniques. The cybersecurity policy should also explain various duties assigned to the different job positions regarding the assurance of the organization's security.

In addition, a policy on cyber safety should provide processes to follow in event of security breach (Ilvonen & Hellsten, 2015). Ilvonen & Hellsten (2015) cite examples of desisting from clicking on unknown links; using antivirus scanning features on electronic mail; and avoiding the use of unapproved storage devices or platforms as important things to be included in a cybersecurity policy. In general data and network encryption, and simulation software should be added to any meaningful policy seeking to secure computer systems (Mishra et al., 2022).

Mishra et al. (2022) group elements of a cybersecurity policy into ten categories as: "Privacy, Website, Email, Data Protection, Access Control, Data Retention, Physical, Information, and Cloud" policies (p. 8). Macnish & van der Ham (2020) note that ethical elements are not commonly considered in frameworks and governance practices in the cybersecurity domain. Though in the academic world, ethics committees tend to offer some not-so-sufficient guidance on cybersecurity, the practice of having some ethical policies and guidance is almost nonexistent outside of the academic environments (Macnish & van der Ham, 2020).

Ethical cybersecurity policy should capture topics such as compassion and respect for humanity, the law, and the entire society. Organizations should have clearly defined processes and tools through which customers could provide consent regarding their personal data. Companies should have it as ethical principle to take immediate actions that will fix security weaknesses that may be detected in their systems (Macnish & van der Ham, 2020).

Cyber Laws and Treaties

This section discusses the actions of governmental and intergovernmental actions within the cybersecurity field. The focus will be on laws that seek to protect rights of people in the digital world. Promulgating the accompanying laws to govern the making and deployment of cyber tools will shape the conduct of private entities (Participant 1). To achieve stability and peace in the cyberspace, there must be more harmonized and global treaties among countries (Participant 1).

Participant 2 explains that when all countries of the world join extradition treaties, it will help to bring perpetrators of cyber harms to book, irrespective of their locations. Participant 3 equally believes that a collective legal regime to tackle actors of cyber harm will be coherent with the largely borderless nature of cyber incidents. Beyond this, all countries should have national policies on cybersecurity training.

In citing a positive example of a national cybersecurity policy, Participant 2 notes that when legal personnel like the judges and lawyers are educated on cybersecurity, they could be in a better position to adjudicate issues pertaining to the domain. As part of national cybersecurity action, countries should commit to passing and enforcing laws that protect the privacy people. Participant 2 argues that privacy should be seen as a universal human need, such that, there should be global standards of upholding privacy in the digital world. Therefore, Participants 2 &

3 decry the fragmented handling cyber privacy in forms such as the GDPR in Europe and the California Privacy Law. Even though local laws about privacy are evolving, they should reflect the norms of international laws about the subject. But international law on privacy in the cyberspace is almost unavailable (Participant 3). Proposed changes will help law enforcement agents offer a more inclusive help to victims of cyberviolence. In participant 3's views, there should be universal policy that allows for internet access and security to be upheld as basic human rights.

A clear law to tackle fake news will be useful in society and successive generations well-informed. There should be a well-defined process for certifying technological products including software before permitting public consumption of same. Participant 4 advocates for a norm of an even distribution of power over the governance structure of the global internet noting that competition between eastern and western countries on the control of the internet is hindering finding collaborative solutions for internet governance issues. Participant 4 also mentions that a national or global cyber policy should seek to enhance freedom of speech, rather than limiting it. This is because free speech is an important engine for innovation.

Some countries are calling for different range of laws to manage technological innovations. Some western countries like the Netherlands acknowledge that encryption may pose challenges to law enforcement and national safety, yet they would not want to introduce strict legislation to inhibit its use (Schulz & Hoboken, 2016). The General Data Protection Regulation (GDPR) of the European Union which became operational in 2018 (Schulz & Hoboken 2016), makes organizations liable for their shortcomings in handling people's data in a secure way (Barolli et al., 2022). Companies operating within the EU that do not comply the GDPR will be surcharged at the rate of about 4% of their yearly income or a fixed financial cost. The United

Kingdom (UK) also have their General Data Protection Regulation guiding how people's data should be accessed or shared (Lam & Seifert, 2023).

Though states like California have promulgated the Consumer Privacy Act in 2020, there is yet to be a federal-level legislation with a particular focus on protecting consumers' digital data in the USA. However, the USA tends to rely on some provisions in the Trade Commission Act at the national level to compel companies to adopt fairer mechanisms in dealing with customers' data. This strategy of protecting the abuse of peoples' information might be inadequate in the USA (Lam & Seifert, 2023, pp. 144-145).

In another instance the authorities in the USA rely on indirect provisions in Health Insurance Portability and Accountability Act (HIPAA) to demand a country-wide data security (Schulz & Hoboken, 2016). But the US has the 2014 Federal Information Security Modernization Act which seeks to strengthen cybersecurity (Schulz & Hoboken, 2016; U.S. Chief Information Officers Council, n.d.).

Though data protection and cybersecurity tend to intersect in many ways, the existing laws tend to make some distinctions between the two principles. For data to be adequately protected, it may require some cybersecurity innovations like data encryption (Schulz & Hoboken, 2016).

Data protection and privacy legislations could be preventive measures which seek to stop businesses from collecting data from clients in a clandestine manner. Data protection also means proper treatment of legitimately collected personal data. But cybersecurity measures are mostly aimed at preventing breaking into data and computer systems by external actors. Therefore, the trends reveal that data protection tends to be titled and legislated separately from cybersecurity (Mantelero et al., 2020).

The EU passed the cybersecurity act in 2019 to guide the protection of vital state or company assets, connections, and individuals from harm through computer-related and physical means (Papakonstantinou, 2022). Mantelero et al. (2020) indicate that Europe's GDPR explains approaches for managing data rather than technical tools. Data protection strategies should include respecting confidentiality, limiting data collected, monitoring the evolution of cyber threats and the efficiency of countermeasures, and informing those affected by data infringement (Mantelero et al., 2020). The General Data Protection Regulation (GDPR) requires that only basic data relating to the function should be collected. Personal identifiable information must not be kept for a duration beyond the performance of the tasks of origin.

To comply with data protection laws, cybersecurity tools would have to be deployed to help to secure the sanctity of data. For example, GDPR encourages encrypting, and anonymizing strategies to achieve data security. A provision within the GDPR for audit personnel to verify companies' adherence to data safety regulations (Mantelero et al., 2020). Beyond the GDPR, the EU has the Payment Services Directive (PSD) which regulates how clients' data could be moved and secured during financial transactions.

The PSD also requires that companies rendering payment services put in place data protection policies that should anticipate appropriate measures against data and security events, necessary data sharing mechanisms with regulatory and coordinating institutions; and the handling of external employees and partners (Mantelero et al., 2020). In addition, the PSD offers actions to be taken in case of cyber events that could compromise financial data. Such actions must involve making enquiries within the organization, collaborating with regulators and public prosecution bodies, notifying affected individuals, and where needed the general public, and getting ready for court cases (Mantelero et al., 2020).

The third layer of legal instruments protecting the interest of consumers in Europe is the Electronic Identification and Trust Services (EIDAS). The EIDA brought about the adoption of seals in digital format permitting digital content to be matched to its individual or business owner, to secure originality of data. The EIDAS also helps to handle cyber risks while offering a regime for cross-checking information during digital business (Mantelero et al., 2020). A very recent strategy by the EU to uphold the safety of people in cyberspace comes in the form of Network & Information Systems (NIS).

The NIS touches on the security of computer systems and connections. Seeking to secure critical infrastructure, the NIS offers guidelines to discover and withstand cyberviolence, or potential threats (Mantelero et al., 2020). Therefore, in Europe, there are tailor-made regulations to manage different aspects of cyber safety such as data and network security, and a general data protection law in the form of GDPR.

Retribution and restoration have become important in the concept of peace. Having effective ways of bringing perpetrators of cyber harm could be a way to bring peace to victims. Cybercriminals may cause harms that have impacts out of the reach of their local confines. Arnell & Faturoti (2023) argue that national adjudication systems should be mostly used to handle cybercrime cases, but international collaboration should be used as a complement when needed. The United Nations Office on Drugs and Crimes (n.d.) mentions that having an international treaty on cybercrime will offer some guidance on how countries could interact to bring justice to victims.

In the absence of any UN-level laws, the Budapest Convention which provides some rallying points for criminal jurisprudence on cybercrimes has only about 66 out of 193 UN countries accepting to join the convention. It is important to mention that the Budapest

Convention permits non-European countries to join (Arnell & Faturoti, 2023). The Budapest Convention has been previously discussed under cyberviolence. This is because sovereign state-level laws on crimes are different in countries across different regions of the world. Cyber laws are yet to be harmonized at the global level.

Moreover, some countries do not trust that accused persons will have access to a fair judicial process when extradited to another country. For instance, the demand for Gary McKinnon to be extradited from the UK to the US, to face prosecution for computer-associated charges was not accepted by the authorities in the UK on the grounds of upholding the human rights of Gary MacKinnon (Arnell & Faturoti, 2023, pp. 32-33).

Outside of the human rights domain, the UK's legal institutions did not permit for some alleged perpetrators of cybercrime to be sent to the US for court cases since accused persons' health conditions were likely to obstruct proceedings. In situations where injured parties live in other countries within the context of other facts of the case, a UK judge may approve extradition requests (Arnell & Faturoti, 2023).

Socioeconomic Factors

Participant 2 argues strongly for improvement in socioeconomic situations as a condition for cyber peace. When the unemployment rate is reduced globally, and people can earn decent wages, they will be capable of taking care of their families. Citing examples of Scandinavian countries like Sweden, Participant 3 explains that when the quality of life is high, crime rates are reduced. Technological innovation is insufficient to tackle cyberviolence as people's socioeconomic underpinnings influence their decisions in the digital world.

Chen et al. (2023) agree that socioeconomic issues impact the occurrence of cybercrime. Specific factors like corruption and job unavailability tend to influence perpetrators'

predisposition to be involved in cyberviolence. From a different view, financially wealthy countries tend to be at the receiving end of cybercrimes more than others. Country-level riches equally affect the readiness to foil attackers, since countries with more human and financial capabilities can construct the needed cyber defense logistics.

In another instance, the political system of a society influences the likelihood of cyber offence or defense approaches (Chen et al., 2023). Regimes with weak or no laws to curb harmful activities such as cyber fraud may be attractive places for cybercrime.

Financial capabilities also determine whether one would be connected to the internet or not. If people do not have the devices to remain connected, they may be cut off from the benefits of digital services in the first place. When more people who are connected to cyberspace have lesser chances of finding gainful employment, they may be susceptible to using their cyber capabilities for the wrong activities (Chen et al., 2023).

Learning from the principle that distributive justice is a cornerstone of social justice, (Mani, 2007); ensuring that social goods such as education, employment, and wealth are evenly allocated within a given context will go a long way to bring peace in the digital world as well. The just distribution of social dividends is important because Chen et al. (2023) note that some cyber-savvy persons who are denied opportunities for economic participation may find alternative livelihoods which might not be legitimate. Said differently, there may be an inverse relationship between tech-savviness and the availability of genuine job opportunities within the equation of the probability of someone being engaged in cybercrime (Chen et al., 2023).

Building Trust

Participant 2 explains that peace in the cyber world includes building a trustworthy environment. When people and their organizations build credible brands, information in the digital world will equally gain some stability. Cross-checking facts could help in sustaining a good reputation in cyberspace. Participant 2 also mentions that trustworthiness must be extended to digital platforms. When technology is safe to use, people will have trust and peace of mind.

Sometimes social trust is weakened by the business interest action of companies other than from external sources. The Zoom telecommunication company has been sued for making clients' data available to other companies. Facebook also came under serious public scrutiny because the Cambridge Analytica collected an enormous volume of data from Facebook without the users' consent (Lam & Seifert, 2023).

Inversini (2020) explains that trust is the foundation of any meaningful actions seeking to keep society secure. Building peace in the digital world will require that people from different societies and professions work together. Sometimes people working through the cyber medium will never meet in person. Trust is a necessary ingredient for interstate cooperation, for stability on the global internet to be achieved. Countries with closely related sociopolitical values may have trust among themselves (Inversini, 2020).

Geiger (2021) concludes that democratic tendencies reduce the chances that two countries having democracy will experience interstate violence. Though Geiger (2021) agrees with the principle that two democratic states may be less likely to oppose each other, the author explains that some scholars argue that it is the economic interests and strengths of countries that make them to declare open conflict or not. Two states with democratic values are likely to have institutions that might check the executive's intentions of full-blown conflict (Geiger, 2021). As

presented earlier, financially capable countries tend to build more cyber defense and offense tools. Countries cannot use cyber weapons that they do not have. Yet countries with a lot of financial resources are more likely to be attacked by cyber means (Chen et al., 2023; Geiger, 2021).

The resistance of citizens of democracies against the use of aggressive forces towards another democratic state is another reason that may keep two democratic states away from violence. But when the managers of democratic states realize that their citizens support aggression against another democratic state, the leaders may execute the views of the masses to avoid incurring the wrath of citizens.

Though one may suggest that democratic tenets like independent and transparent judiciary provide peaceful alternatives, there have been instances where some democracies have been aggressive towards other democratic states. While some states' departure from democratic peace principles may be related to the quest to uphold their nationwide security ahead of other democratic countries, the extent to which democracy has advanced in particular contexts may be an important variable of democratic peace arguments (Carnegie et al., 2023).

Moreover, Inversini (2020) argues that international laws help to form global values and norms, through which trust could be built. When institutions of the state operate in a transparent, and fair manner, private individuals and entities will be at ease to collaborate with them for peace and stability. Technological innovations that are efficient and safe boost the levels of trust. Stability in cyberinfrastructure in a given country is also dependent on other things like uninterrupted supply of electricity, and network stability (Inversini, 2020).

If there is a perception of mistrust, actors may resort to some harmful cyber practices. In some instances, a lack of trust worsens existing cyber conflict situations. When there is trust,

people are more confident about having positive cybersecurity behaviours and outcomes. Confidence in the abilities of people, institutions, and technology also raises people's trust. Inversini (2020) thus proposes "confidence-building measures (CBMs) to obtain some stability in cyberspace (pp. 270-271). CBMs may include transparent interactions among countries, having globally representative cybersecurity taskforces, and establishing ethical standards for not attacking essential services.

Chapter 5: Discussion

This chapter presents a synthesis of literature and interview data as presented in the previous chapters. By attempting to harmonize the meaning of cyberviolence, chapter 6 is organized as follows: the meaning of cyberviolence; cyber peace; cybersecurity roles as unexpected result; limitations of the research; implications of finding; and recommendations for future research. The meaning of cyberviolence has been further classified into crimes and balkanization of the internet, cyberviolence as violation of human rights, and fake news and cyberviolence. Meanwhile, the meaning of cyber of cyber peace is regrouped into negative cyber peace and positive cyber peace.

Improvements in the digital world bring enormous benefits and challenges alike. For instance, biometric technologies help society to be more organized in terms of crime detection and prevention. But the same technologies come with renewed forms of threats for individuals and society. Some cyber tools which were bought for social good at their origins are now being utilized by state actors, private individuals, and businesses to endanger some longstanding and positive norms of humanity such as human rights (Chenou & Bonilla-Aranzales, 2022; Sharp, 2017). Whereas some security software is being used by some state and non-state agents to spy on civilians, some businesses also collect and conduct financial transactions with customers' data without their consent (Lewis et al., 2017; Marczak et al., 2021)

At the same time, scholars and practitioners have different opinions on what measures could be adopted to assure peace. Some scholars propose that only cyberviolence perpetrated against crucial state infrastructure should be worth the attention of peace enquirers and practitioners (Buçaj, 2020; Christen & Bangerter, 2017; Marlin-Bennett, 2022). But scholars like Boustead & Shackelford (2022); Duguin et al. (2022) argue for a more holistic and human-

centred approach to cyber peace. This brings the dimension of the impact of cyberviolence on individuals because humans are important components of cyberspace. This objective is ever important because of the fast pace of thinning of the gap between physical and virtual functions. How cyberviolence and cyber peace are understood is affecting the nature of legal and technological innovations that are brought forth.

To expand the discussions about violence and peace in the digital era, this research paper asks three questions:

How does cyberviolence occur?

How can cyberviolence be addressed?

How can cyber peace be achieved?

The Meaning of Cyberviolence

Cyberviolence is said to be occurring when computer-based technologies are used to commit crimes, cause harm, infringe on human rights, censor, and disconnect the internet, or share fake news.

Crimes and Balkanization of the Internet

Explaining cybercrimes as damages caused to assets, emotions and bodies of a person creates ambiguity within some existing laws. To tag an act of violence as criminal within the Laws of Armed Conflict, the target state must have been identified, as having used similar force against another state. It is much more difficult to link actors involved in cyberviolence to their intentions (Buçaj, 2020). Many provisions in the International of Armed Conflict may not handle other aspects of cyberviolence involving non-state actors. What then happens when there is cyber violence targeting essential services of a country, yet the political objectives of the attackers have not been established?

Though the Budapest Convention expands the scope of cybercrime by including individual-level acts like gaining unsanctioned entry into computer systems, not many countries have accepted it as part of their national laws (Council of Europe, n.d.-a). The attempts by individual countries to pass their laws to regulate crime in cyberspace have birthed another challenge known as internet balkanization. Even though it is gaining traction in existing literature, the balkanization of the internet was not discovered in my literature reviews before the interviews. An interview participant cited it as an evolving example of cyberviolence. The term permits for different phenomena associated with not-so-harmonized country-level criminalization of certain cyber acts to have some naming.

Balkanization connotes barriers to internet connectivity, such as censoring and banning some internet services in certain locations, sometimes because of nationalistic economic interests (Janc, 2017). Balkanization of the internet is being caused by division among world powers about which appropriate global internet governance strategies could be upheld (Fick et al., 2022). Restriction of internet access for somewhat narrow reasons tends to defeat the original principle of having a global and interconnected digital realm where everyone connects to receive or deliver information (Chenou & Bonilla-Aranzales, 2022; Fick et al., 2022; Lemley, 2021). Yet local legislation to criminalize certain harmful cyber activities could prove useful, provided they conform with international norms like human rights. UNESCO supports legal and technological innovations in cyber realms that seek to uphold fundamental freedoms and privacy (Schulz & Hoboken, 2016).

The Council on Foreign Relations also supports the position that disruptive use of cyber tools against state, private institutions or individuals should be denounced in law; however, this should be done through international collaboration (Fick et al., 2022).

Countries would have to build a consensus around having an institution that is representative enough in managing the governance of the global internet. Now there is no perfect internet governance regime. As states' scramble for dominance in cyberspace continues without a more inclusive solution, citizens are being denied opportunities for full enjoyment of their rights through censorship and espionage. In another world, citizens' rights are being trampled upon through data and privacy breaches by large private companies. If the status quo for internet governance is to be maintained, it would be important that the USA advocates for arrangements that will allow for inputs from scientists and engineers from different parts of the world, regarding internet standards and future changes (Hill, 2012).

This aspect of cyberviolence helps to understand some underlying causes of the increase in the nationalization of cyberspace by countries. It would be important to further explore the challenge of representation and decision-making at the Internet Engineering Task Force (IETF) but that is beyond the reach of this research.

What kinds of harm could cyberviolence cause? Different dimensions of cyberviolence remain unregulated, and so leaving those unregulated portions out of the discussions about violence only compounds the problem. But the research argues that the peacebuilding domain could be concerned about issues that are criminal and not. This is because harm is much more than what is regarded as a crime. Against this background, I maintain that all acts of disruptive use of computer-based innovations, whether regarded as criminal or not and—irrespective of their magnitude or the actors should be considered violent and be treated in peacebuilding. This position is rooted in practices in the peace and conflict field, that treat both direct and indirect harms as problematic (Agrafiotis et al., 2018; Council of Europe, n.d.-b). Some indirect harms

could lead to direct harm, and some direct harms could come with additional layers of indirect harm, or systemic violence privileging one group over another.

Rather than treat direct and indirect harms as hierarchical representation, I would rather suggest they are treated as equal in causing similar disruptions in the normal operation of humans or society. Malware attacks may be targeting computer systems but could have an inadvertent effect of death because it has prevented the normal functioning of basic and critical services like medical operations.

Cyberviolence as Violation of Human Rights

All participants accept that violent measures such as bullying, blackmailing, mishandling of personal data, stalking activities, and censorship on the internet infringe on people's basic rights. This position is consistent with current literature that sees cyberviolence as greatly affecting human rights (Chenou & Bonilla-Aranzales, 2022; Lewis et al., 2017; Schulz & Hoboken, 2016).

Yet Participant 1 mentions that some countries have legalized cyber espionage. Does the legalization of abuse make it not abuse? Asking this question does not suggest that Participant 1 thinks abuse is no longer abuse when permitted by law. Martin Luther King Jr.'s naming of just and unjust laws reveals that certain laws do not sustain the ability of humans to live a dignified life (Mingo, 2018).

Some participants mentioned that businesses are also involved in spying on people for mostly commercial reasons. Surprisingly, espionage activities by governmental agents receive much more attention among scholars and human rights activists than that of private businesses. Discussing violent cyber actions in their report, the Council on Foreign Relations focused heavily on state actors (Fick et al., 2022). Even the discussion on the roles of private actors is

mostly limited to actions concerning the external threats to their cyber infrastructure in studies such as (Fick et al., 2022); (Chenou & Bonilla-Aranzales, 2022); and (Schulz & Hoboken, 2016).

Not many issues are being raised about how private corporations are collecting and selling data about consumers without their consent. But Schulz & Hoboken's (2016) enquiry done for UNESCO, and Chenou & Bonilla-Aranzales (2022) briefly discussed that espionage has become a profitable action for businesses. Whether done by state agents or private corporations, espionage tendencies intrude on the right to privacy and consent.

When it comes to censorship, participants have divergent positions. Some participants would argue that censorship should never be done because of three reasons. Blocking information on the internet breaches the right to information and freedom of speech. The people tasked to block contents may be exposed to the personal data of others, which could be used to score political points in some jurisdictions. The third reason cited for which censoring the internet should not be encouraged is that people could use cybersecurity software to circumvent censorship systems. This argument when put differently would mean that there will be no need to block the contents when people would still be able to access them. There is no consensus in the existing literature on the extent to which internet censorship may be allowed. Some scholars argue for minimal censorship under some scenarios such as crime prevention, and discrimination (Bambauer, 2013; Hellmeier, 2016; Ververis et al., 2020).

Those who are for censorship argue that the phenomenon, which might be needed under certain instances is already happening in many democracies. In this regard, Participant 4 points out that internet censorship could be as subtle as legal requirements requiring internet service providers to document their customers' activities on websites tagged as dangerous and illegal. Moreover, censoring digital content could become a means of suppressing political opponents.

Because of this, proponents from the other side explain that censorship should not be allowed to continue under any circumstance because of its damaging impacts on human rights. Both democratic and non-democratic states conduct some censorship, but censoring content in non-democratic countries tends to be more researched (Ververis et al., 2020). Even though it would be helpful in further understanding of the grouping of internet control jurisdictions, deeper analyses of internet censorship tools and strategies of multiple countries are beyond the boundaries of this research.

Companies may use information collected on clients to deny future access to those services. In addition, conceiving digital violence from human rights perspectives is useful in understanding the enormity of harm being caused in the cyber world (Chenou & Bonilla-Aranzales, 2022).

Viewing cyberviolence through a human rights lens will help to understand the kinds of national laws that are conforming to international humanitarian laws. Human rights are regarded as important in the physical world, therefore much more attention could be accorded to them in the digital world also. But it is important to use the notion of human rights arguments cautiously since some countries may have different interpretations of them.

Fake News and Cyberviolence

Some participants hold the view that fake news is not a new phenomenon. What is different about fake news this time around is that the advent of the internet and social media platforms make fake news spread like wildfire. Other participants explain that fake news could be misinformation and disinformation. Misinformation is when fake news is disseminated without being aware that it is fake. Meanwhile, disinformation connotes a planned distribution of distorted content. Some large corporations and government agencies may use fake news as a way of ascertaining or changing public perceptions. The participants acknowledge that fake news has many harmful effects. It causes reputational harm and social deception. Fake news also destroys positive social values and trust. Using the increase of fake news, as a decoy, some regimes may be promulgating new laws to curtail the long-held freedom of expression of their political opponents. These observations of participants are consistent with the views of different scholars about the challenges of fake news (Adjin-Tettey, 2022; Meel & Vishwakarma, 2020; Talwar et al., 2020).

According to the results presented earlier, cybersecurity professionals differ in approaches to tackling the menace of fake news. Some professionals suggest using cyber censorship in a transparent way to counter the spread of fake news. Censorship as suggested should come with legal and digital mechanisms to stop the threats of fake news. But censorship is a controversial matter as presented earlier. Adjin-Tettey (2022) concludes that training people with some techniques of information management may help them to recognize what is fake news or not. As the phenomenon of fake news is advancing, cybersecurity professionals and researchers continue to search for possible solutions.

Conclusion of Cyberviolence

As explained earlier in the introduction, using certain terminologies such as cyber warfare and cyber-attacks in themselves tend to be limiting in the phase of existing frameworks, laws, and conceptualization of violence in the digital world. How can the explanation of cyberviolence through the lens of crimes committed in cyberspace bring about some more common understanding and steadiness to the terminology?

Defining cyberviolence as cybercrime under international legal norms will only permit some online activities that disrupt important services of another country to attain certain political gains as cyberviolence (Buçaj, 2020). Moreover, social justice activists do not only see violence from the standpoint of the law because other elements forming the structure of a society exist. Beyond the law, scholars like Mani (2007) support analyzing social structures through other indicators like access to basic necessities of life and the understanding situations of minority groups. Applying this to the context of cyberviolence, it is important to investigate how the inability of certain people to access certain basic modern computerized tools makes them victims of cyber violence as captured under the balkanization of the internet. Participants and some researchers alike agree that cyber activities could cause direct and indirect harm.

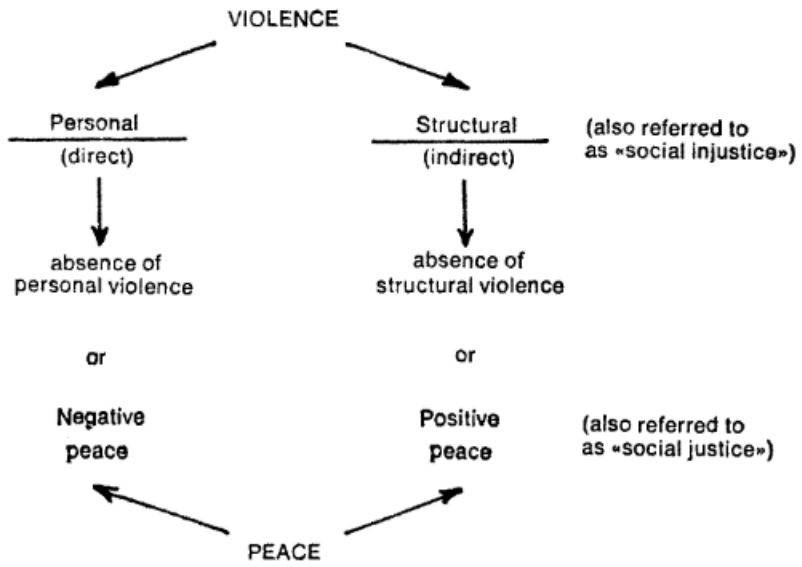
As noted above, each of the components contained in the definition of cyberviolence as presented has some limitations. Dwelling on one component ahead of another may exclude some salient happenings in cyberspace from the conception of violence. These terms must lend themselves to the explanation of cyber violence.

The Meaning of Cyber Peace

Cyber peace could be described as laws, policies, and practices of cross-checking facts, cybersecurity, cyber education, trust-building, improving socioeconomic factors in general, and digital technology, to correct the harms being caused in the digital space. Some of the actions are not only correcting harm. In the absence of violence, some of these practices are just a necessary state of peace and stability in the digital world. Peace may be seen as the "absence of violence" in direct and indirect forms (Johan Galtung, 1969, p. 167). If peace is to be conceived of as a countermeasure for violence, the meaning of violence should be both larger and more detailed in scope. This will in turn broaden the horizons of peace (Johan Galtung, 1969). In peace and conflict studies doctrines, tackling the structural origins of violence is as important as stopping direct violence.

Figure 5

Relationship between violence and Peace



Note. Adapted from Johan Galtung (1969, p. 183). Violence, Peace, and Peace Research. *Journal of Peace Research, 6*(3), 167–191.

Thus, tackling direct violence will only lead to temporary peace, which is usually called negative peace. But when conditions of indirect harm are corrected, peace can be more enduring, and enduring peace is what Johan Galtung (1969) calls positive peace. The most obvious sources of indirect harm are social injustices (Johan Galtung, 1969). Social injustice occurs when basic human needs are absent for reasons such as unfair distribution of social resources, abuse of human rights, and widening social gaps. (Byrne et al., 2020; Johan Galtung, 1969; Mani, 2007).

Said differently, peace could be mechanisms to prevent violence from occurring in the first place, and peace may include measures to stop violence from continuing. Establishing the relationship between peace and violence makes it possible for cyber-related violence to be included under peace and conflict doctrines. Revisiting these concepts allows for appropriate regrouping of peace practices in the cyber world as follows.

Negative Cyber Peace

Participants had suggestions that assist in dealing with negative cyber peace, such as fake news. Participants indicate that fact-checking could be a useful way of controlling the phenomenon of fake news; however, they did not reveal how fact-checking should be conducted. Perhaps the interview question was not framed in a way to elicit details about fact-checking. Though this part of the interview was focused on how the sharing of fake news is affecting freedom of expression, fact-checking was not anticipated. However, fact-checking is an important notion that corresponds with the position of some scholars (López-Marcos & Vicente-Fernández, 2021).

Meel & Vishwakarma (2020) went further to describe some digital tools like COMPA, which could help in fact-checking. These tools try to identify and limit fake news. Existing

technologies for fact-checking are at an early point in their evolution. Moreover, fake news of different kinds could escape from the radar of these tools. Other fact-checking software depends heavily on human interventions during their operations. Some of the tools are designed to work on only specific social media sites (Meel & Vishwakarma, 2020).

Some news and tech companies are creating job positions for fact-checking. People tend to depend on their intuition and some cyber tools to discover fake news. Human measures in fact-checking might include responding with the correct narrative of the news at an equal or faster rate than how the fake news was circulated. In addition, humans may be needed to block or filter fake accounts that are spreading incorrect news (France 24, n.d.; Li & Chang, 2022; Meel & Vishwakarma, 2020; PolitiFact, n.d.).

Participants explain that cybersecurity includes computer-based innovations and physical actions, laws and policies that seek to protect people's fundamental human rights. Cybersecurity should uphold freedom of speech, the right to privacy, consent, and safety. Data safety and human safety are at the center of cybersecurity. But Kavak et al. (2021)'s definition of cybersecurity is much more reflective of the perspectives of the cybersecurity professionals interviewed. This is because Kavak et al. (2021) consider cybersecurity to include human-dependent actions like risk assessment, and application of technology-based innovations. Beyond encryption, existing technical dimensions like VPN and TLS connections add some layer of safety to computer connections (Schulz & Hoboken, 2016; Turner, 2014).

For instance, although VPNs may be used to hide nefarious activities, they may also allow human rights activists to hide their physical location on the internet, thus allowing them to work more freely. Some VPN features permit people to access internet contents that are blocked by repressive governments, for political reasons. This is an important safety measure that can

safeguard people whose lives are under threat. VPN functions of concealing user location and activities may, if used for good, be referred to as negative peace since this research argues that cyberinfrastructure should not leave private information easily accessible. Putting all these together, it is safe to say that cybersecurity is the intersection of some physical human actions, technological innovations, and dignity-upholding laws and policies to keep human beings and digital connections safe.

Positive Cyber Peace

Participants argue that cyber education is an important condition for cyber peace. Every user of the internet must be educated about some foundational things about cybersecurity, and their fundamental rights within cyberspace. Mass education could serve this purpose. Outside of the profession of cybersecurity, it will be important that staff within institutions such as law enforcement agencies are equipped with more than fundamental cybersecurity training or education. The contents of cybersecurity education should include computer and human-based dimensions of security (Austin, 2020). Specific contents like cyber risks, data safety, system administration and security could be useful additions (Caelli, 2020).

People deserve to know what is happening to them each time they connect to the internet. In an era where the Internet of Things (IoT) is ever present, education on Internet security cannot be overemphasized (Blair et al., 2020).

Overall, cyber education should integrate the approaches of social sciences and STEM courses since people's mistakes cause them to become more susceptible to computer-related attacks (Shoemaker et al., 2020; Withers & Austin, 2020).

Going by the arguments of basic human needs, human rights and social justice, security is a cornerstone of social structure (Fisher, 1990; Mani, 2007; Qureshi, 2018; Sandole, 2013).

Mishra et al. (2022) argue that the goal of security is to keep people secure from physical, and emotional harm.

Mishra et al. (2022); and Veale & Brown (2020) also consider cybersecurity as actions that guarantee the safety of data, computer, and internet connectivity. Since human beings are depended on these connections for their essential tasks, it could be said that cybersecurity directly affects humans. Therefore, this research claims that cyber innovations should always have security measures embedded in their design. Every security measure integrated with the design of computer-based technologies to keep people safe is what would be called positive cyber peace.

Encryption has become an integral cyber innovation and policy that is being employed to ensure digital safety. Per the results of the interviews, technological innovations such as encryption should be supported with favorable laws, and policies that uphold the universal dignity of humans. When laws relating to the ever-growing technology industry are not humanity-centered, internet users will have an increased risk of being harmed by both governmental and private actors.

Going forward, TLS and encryption functions should be considered as part of the structural design of computer systems and their connections. With the right policies and actions, TLS and encryption could help internet users to be somewhat protected (Lewis et al., 2017; Schulz & Hoboken, 2016). Narrowing the scope of some earlier arguments made by participants and research papers would mean that encryption technology could be supported with zero-trust, full disk, and end-to-end policies. Interview results also support the position that companies and state agencies should have ethical policies like bug bounty. Ethical considerations like bug bounty permit people in official capacities and individuals to inherently support the protection of

people and their data, whether there are policy and legal implications or not. But from a technical angle, bug bounty tends to be a negative peace gesture because it is an avenue for signaling security lapses that may be detected from cyber infrastructure.

Qualifying these aspects of cybersecurity as positive peace is also consistent with Johan Galtung (1969)'s conceptualization of actions that seek to improve structural stability as positive peace. There is also a common understanding that cybersecurity measures like end-to-end encryption may help secure the human rights of people. Yet some law enforcement and national security proponents explain that such encryption techniques do not allow for people's data to be recovered when needed, and this could hinder criminal investigations (Lewis et al., 2017; Schulz & Hoboken, 2016). Contributing to this debate, Schulz & Hoboken's (2016) report for UNESCO adopt the position that the benefits of full-scale encryption far outweigh the challenges that it possess.

Beyond bug bounty, private entities should assume more responsibilities like respecting laws that uphold human rights. Where relevant local laws are not available to protect users of new technologies, companies should be adopting ethical standards that protect the basic rights of consumers of their products and services. For example, the NSO Group should adhere to ethical standards that prevent the sale of the Pegasus security software to repressive regimes that have the propensity of using it to abuse the privacy of political opponents and civil society.

Companies should regularly do cyber risk assessments on their systems. Many cybersecurity researchers equally believe that private organizations have integrated policies to secure customers and their data (Ilvonen & Hellsten (formerly Virtanen), 2015; Macnish & van der Ham, 2020). Principally, cybersecurity policies could serve as techniques for the assurance of safety. But cyber policies should also anticipate remedial actions against any forms of violence

that may arise in cyberspace. It is not enough for individuals to have ethical principles as discussed in the section on cybersecurity. It will serve the greater good for organizations to have ethics well documented in their policies.

The research suggests that countries should work together in developing international cybersecurity laws to promote positive behaviour in the cyber world. As mentioned earlier, such laws should mainstream human rights principles. A globalized approach to building legal norms would be useful because cyberspace transcends national boundaries. Though country-level policies on cybersecurity education would be helpful, they must reflect international norms (Arnell & Faturoti, 2023).

Cybersecurity professionals and researchers decry the existing piecemeal approach to regulating the protection of digital data. The General Data Protection Regulation (GDPR) of Europe and the California Privacy Law remain popular attempts to champion people's right to privacy and control over their data (Barolli et al., 2022; Schulz & Hoboken, 2016). Europe has also promulgated the Cybersecurity Act to safeguard essential services (Mantelero et al., 2020). The Budapest Convention of the Council of Euro lays some foundational stones for international legal norms for cybercrimes (Arnell & Faturoti, 2023). The inability of the country to build a consensus around redeveloping a more inclusive governance regime for cyberspace complicates the absence of a globalized data protection regulation. Laws are part of the social structure. This research explains that more global-level engagements are necessary to find an appropriate mix of legal norms that should govern the global internet.

Outside the zone of legal structures, some interview participants note that improvement in socioeconomic conditions like employment will reduce the rate of cybercrime in some regions of the world. Chen et al. (2023) explain that corruption and joblessness are important factors

increasing the rate of cybercrime in some countries. Because richer countries tend to be at the receiving end of cybercrimes more often than not, those wealthy countries build strong cybersecurity capabilities to foil attackers (Chen et al., 2023).

In other words, income inequalities among countries could make cybercriminals target countries perceived as rich. Even though there might be geographical and financial gaps, cyberspace enables actors with malicious motives to target people without facing many barriers that would be present in physical interactions. Human capacity affects a country's cyber strength. In another instance, the political system of a society influences the likelihood of cyber offense or defense approaches (Chen et al., 2023).

Poverty also denies people the opportunity to acquire internet-based devices and enjoy the freedom of expression that internet connectivity may offer. And at the same time, poverty may influence a cyber-capable person to result in cybercrime. What this means is that wealth or poverty should be analyzed at both micro and macro levels to gain a detailed understanding of conditions for cyber peace.

Comparing viewpoints from the cybersecurity professionals interviewed, it can be said that trust is an important ingredient in building cyber peace. Because of that, the following deductions could be made. When security is adequately provided, people will have some trust in using internet-based services. Cybersecurity innovations, safety-driven laws and policies increase the confidence of people on digital platforms. Moreover, the absence of trust leads to chaotic actions in the cyber realms. When countries build a more inclusive decision-making structure that is representative of the different geographic and economic regions of the world, trust levels in the global internet might increase. And a rise in trust levels for the governance structure of the global internet may lead to more collaborations to bring stability. When people

and their organizations build credible brands, even outside of cyberspace, information in the digital world will equally gain some stability.

Generally, people prefer to access online content from organizations that are associated with some credibility both in digital and physical spheres. In addition, when organizations provide official responses to fake news, it could help in ensuring long-term social trust and cohesion. And most importantly building trust in the safety of internet-related technologies gives people peace of mind.

Lam & Seifert (2023) notes that the correct treatment of clients' data by big corporations could enhance the trust of the public in their products and services. In this digital era, tech companies are competing to gain control over data, for competitive advantage. At the same time, customers may attach a similar level of importance to the safe handling of their data just as they would to the quality of products or service being offered by the companies. Stability in cyberinfrastructure in a given country would be dependent on other things like an uninterrupted supply of electricity, and network stability (Inversini, 2020).

Inversini (2020) mentions three important ways to build trust in cyberspace: having an inclusive cybersecurity security task force at the international level; setting up clearly defined ethical principles; and operating a transparent internet governance institution. Citing trust as the foundation for peace and security, Inversini (2020) argues that where there are common values, it becomes easier for people and nations to trust. Though arguable, some scholars assume that economic interests and values would not motivate two democratic countries to attack each other (Geiger, 2021). Still, the relationship between democratic values and peace has not been explored much in scholarly articles concerning cyber peace.

Cybersecurity Roles as Unexpected Result

This research did not set out to create an inventory of job positions in cybersecurity. The question that necessitated answers for the creation of this list of job positions is: what does your current job entail, and how long have you been working in this role? I was expecting answers about the description of tasks, and how long the interviewees have been performing those tasks. The objective was to gain a more technical understanding of the kinds of activities the cybersecurity professionals are engaged in.

Beyond giving the expected answers, the participants went further to list their current and previous job positions. Still, this inventory of cybersecurity positions provides some insights into the readiness of organizations to sustain the safety of people on their digital platforms. This listing of cybersecurity roles helps one to understand which personnel will be performing both negative and positive cyber peace activities explained earlier.

In reference to the cybersecurity roles that were noted earlier: Chief Information Security Director; Cyber Researcher and Consultant; Cybersecurity Architect and IT Security Officer; Governance, Risk and Compliance Officer; Infrastructure and Network Officer; Co-founder of a Cyber Company; Cyber Risk and Compliance Officer; Cybersecurity Researcher; Information Security Officer, and Network Administrator. While there are similarities in these positions, there are also some variations. In some cases, new responsibilities were added to existing roles that would lead to new variances in job titles or names. In other cases, the specific tasks being performed vary across different organizations.

There are also different job titles with different tasks across various organizations or within the same organization. Some of the roles are revisited as follows. The Chief Information Security Director or Chief Information Security Manager may be responsible for developing

cybersecurity frameworks and policies for organizations. A cyber researcher and consultant conduct investigations into techniques or tools used by attackers. This is done by analyzing previous cyberattacks. While taking further actions to make the results of investigations public, the cyber researcher and consultant share the results of investigations with authorized institutions so that the attackers could be identified. Making the outcomes of results public will be consistent with earlier recommendations of educating the public about evolving threats in cyberspace.

Analyzing existing attacks and systems could be a way of conducting cyber risk assessments. Other organizations may prefer having an actual cyber risk and compliance officer to perform a risk assessment and tasks relating to regulatory and legal compliance. In other setups, organizations may prefer to have governance, risk, and compliance officers. I did not follow up with participants as to what the latter roles entail.

Due to the resemblance of the job the titles of cyber risk and compliance officer and cyber governance, risk and compliance officer, the details from Participant 2 about this role would have allowed for useful comparison between the roles. Again, the specific tasks involved in cyber roles such as cyberinfrastructure and network officer, and network administrator were not provided. I did not follow up on these details because, though they are important to give a general perspective into cybersecurity, the cybersecurity titles are not the focus of this study.

Conclusions on Cyber Peace

The discussion on peace is grouped into negative and positive peace. When cyber peace is conceived of as an action necessary to contain violence, that peace would be regarded as negative peace in cyberspace. Negative peace does not suggest that the peace is bad. It rather explains a situation of insufficient peace. Some of the negative cyber peace practices discussed in this research report include fact-checking. Fact-checking is evolving into an important task not only among traditional media organizations. Even big companies working in other domains see the need to have active social media teams to fact-check and counter fake news that circulates about the products. Most of the digital tools for fact-checking would need to be upgraded to be compatible with multiple digital platforms, while providing live updates about content detected to be fake. This is something that cybersecurity professionals and peace researchers think might be too much for technology to handle, since identifying and correcting fake news would need a lot of human intuitions (Meel & Vishwakarma, 2020).

This report also considers the cybersecurity invention of VPN as negative cyber peace. VNP offer some opportunities for internet users to enjoy their privacy rights, especially under political regimes with severe forms of censorship and espionage in the digital world. VPN has been classified under negative peace because it mostly comes as a software to be installed to assure some layer of security. Moreover, people use VPN as a measure against some vulnerabilities in cyber infrastructure (Lewis et al., 2017). For example, some people use VPN to hide their geolocation. In certain repressive regimes, people's geolocation could be used to trace and harm them.

Positive cyber peace considers policies, laws and cybersecurity innovations that are inherently part of the social and cyber infrastructure, to assure structural resilience and safety of

internet-based connections. The discussion on positive cyber peace does not consider reactive measures against internet-related violence. This report considers proactive actions like cybersecurity education, technological innovations in encryption, and Transport Layer Security (TLS), with their corresponding laws and policies that uphold fundamental human freedoms, privacy, and security as positive cyber peace. Technology companies and other stakeholders should consider encryption of data and internet connections as a basic infrastructural requirement. Encryption is gaining some popularity as a technical provision that is built into some devices or software. By this, the research captures encryption that is already embedded into internet infrastructure and devices as positive cyber peace. Since cyber realms transcend physical borders, global-level collaboration should be treated as a necessary condition for positive peace. Discussions uncover that the adoption of the strong ethical position of all organizations could help in the protection of people in cyberspace. Providing more dignifying socioeconomic opportunities will provide people with the proper alternatives to cybercrime and other social vices. Meanwhile, the amount of trust people could have in cyber systems may be dependent on security policies and innovations.

Chapter 6: Conclusions

Limitations of the Research

The first and most important limitation of this research is the sample size. Five cybersecurity professionals were interviewed but one participant was opted out of the research after the interview. The results as presented are based on the interview responses from four professionals. This sample size is not representative enough for a more expanded conclusion to be made. But many years of experience of the four participants in the cybersecurity field enable the researcher to obtain detailed and relevant descriptions of the phenomena and concepts.

Second, considering the small size of the participant sample, it would have been more helpful to have an interview with a duration of more than 45 minutes as planned. More time allocated would have permitted more follow-ups on some concepts and developments. However, the interview questions provided a useful guide to stick to the objectives of the research.

Third, the snowball sampling technique used may have some biased tendencies. But this technique has helped in recruiting professionals in the cybersecurity field as it is more difficult to get interested participants recruited for a sensitive research subject like cyberviolence and peace. A more randomized sampling technique would suffice for future studies.

Fourth, I missed out on framing and asking for participants' views on what actions could be taken to address the phenomenon of fake news. The interview question got participants to state their views on how fake news could be impacting fundamental freedoms. Perhaps, had a question been asked on ways to handle fake news, other solutions would have been emerged.

Implications of Findings

This research report makes modest contributions to cyberviolence, and peace as follows. First, the research integrates the direct thoughts of cybersecurity professionals with theories and practices in peace and conflict studies. So far, much of the scientific research seeking to integrate the digital dimensions of violence and peace into broader discussions in the field has relied on secondary data and quantitative approaches (Chenou & Bonilla-Aranzales, 2022; Geiger, 2021; Mantelero et al., 2020; Ververis et al., 2020). But François & Ankersen (2022) had one cyber peace practitioner interviewed, and the interview transcript was published without any comparisons with existing literature.

The research also seeks to add to the definition and stability of the evolving concepts of cyberviolence by uncovering elements such as internet censorship, fake news, cybercrime,

internet service disruptions, and other human rights violations. This research tries to expand the discussion on activities in cyberspace that should be considered in conflict analysis. This approach encourages the consideration of cyberviolence that is not targeting non-state institutions or critical infrastructure in peace and conflict analysis. This paper compares cybersecurity practices to negative and positive peace concepts in peace and conflict doctrines, to narrow the distance in the two fields.

In addition, this research demonstrates the intersection of the basic human needs' theory, human rights, and social justice principles. They all seek to uphold human dignity and social cohesion. For instance, all three theories seek to ensure the safety of humans.

Except for a few, the research used to formulate the literature review mostly comes from peer reviewed journal articles, and books that are less than ten years. This strengthens the empirical base of the research.

Recommendations for Future Research

Future research should consider exploring what kinds of decision-making systems could be more helpful in global Internet governance. Moreover, further research should be done to investigate what suitable international norms could be formulated to regulate the excesses of internet usage such as fake news, censorship, data privacy breach, and espionage.

In addition, researchers and practitioners alike should explore further what kinds of cybersecurity standards should be met by technological innovations before they become available for consumers. Finally, it is necessary for future research to explore, the internal control measures that companies tend to adopt to assure the safety of their clients in the cyber environment.

Final Thoughts

This research seeks to understand how cyberviolence occurs, how cyberviolence can be tackled and, how peace in the cyberspace can be achieved or sustained. This research goes further to integrate personal and country-level harms as well as indirect and indirect harms in the cyberspace in the description of cyberviolence. Meanwhile, many cybersecurity researchers tend to focus on cyberattacks that appear to be directed at important state-level infrastructure (Christen & Bangerter, 2017; Lin, 2012; O'Connell, 2012; Rid, 2013). These cyberattacks that seek to disrupt the normal functioning of crucial services may be more popular with peace and conflict scholars because they tend to be laced with certain political objectives (Christen & Bangerter, 2017).

The results from the study prove that violence in the cyberspace, whether targeting a person or country has a serious impact when viewed from human rights, social justice, and basic human needs arguments. This approach is necessary to emphasize the need for a holistic solution to cyberspace challenges of cybercrimes, internet censorship, internet disconnection, sharing of fake news, and different human rights violations such as data breaches and cyber espionage. Tackling cyberviolence would require some negative peace actions like fact-checking and the use of VPNs.

Positive cyber peace conception will require that internet infrastructure, data, and devices are equipped with cybersecurity techniques of strong encryption. Policies and laws about encryption should ascribe to uphold human rights of people.

Bibliography

Adjin-Tettey, T. D. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities*, *9*(1), 2037229. https://doi.org/10.1080/23311983.2022.2037229

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, *58*(5), 1083–1097. https://doi.org/10.1177/0022343320964549

Amnesty International. (2017). *Protecting Human Rights on the Internet*. Amnesty International. https://www.amnesty.org/en/latest/news/2017/03/fighting-back-against-cyber-censorship/

Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, *37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

Austin, G. (2020). Introduction. In *Cybersecurity Education*. Routledge.

Baek, Y. M., Kang, H., & Kim, S. (2019). Fake News Should Be Regulated Because It Influences Both "Others" and "Me": How and Why the Influence of Presumed Influence Model Should Be Extended. *Mass Communication and Society*, *22*(3), 301–323. https://doi.org/10.1080/15205436.2018.1562076

Bambauer, D. E. (2013). Censorship v3.1. *IEEE Internet Computing*, *17*(3), 26–33. https://doi.org/10.1109/MIC.2013.23

Barolli, E., Hyra, A., & Tomco, V. (2022, July 28). *Impact of the General Data Protection Regulation (GDPR) on Cybersecurity*. Rebound, Rebuild, Reinvent, Sustainable and equitable development (3R4SED 2022). https://doi.org/10.13140/RG.2.2.28665.95843

Bazeley, P. (2009). Analysing qualitative data: More than "identifying themes." *Malaysian Journal of Qualitative Research, 2*.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Educating future multidisciplinary cybersecurity teams. In G. Austin (Ed.), *Cybersecurity Education: Principles and Policies* (1st ed., p. 13). Routledge.

Boustead, A. E., & Shackelford, S. J. (2022). Overcoming Barriers to Empirical Cyber Research. In C. Ankersen, F. Douzet, & S. J. Shackelford (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (pp. 205–211). Cambridge University Press. https://doi.org/10.1017/9781108954341.011

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. https://doi.org/10.1191/1478088706qp063oa

Brinkmann, S. (2013). *Qualitative Interviewing*. Oxford University Press. http://uml.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=e000xna&AN=603936&site=ehost-live

Buçaj, D. (2020). Cyber Conflict. In O. Richmond & G. Visoka (Eds.), *The Palgrave Encyclopedia of Peace and Conflict Studies* (pp. 1–10). Springer International Publishing. https://doi.org/10.1007/978-3-030-11795-5_76-1

Byrne, S., Matyók, T., Scott, I. M., & Senehi, J. (2020). Critical peace and conflict studies emancipated? In *Routledge Companion to Peace and Conflict Studies*. Routledge.

Byrne, S., & Thiessen, C. (2020). Foreign peacebuilding intervention and emancipatory local agency for social justice. In *Routledge Companion to Peace and Conflict Studies* (pp. 136–146). Routledge.

Caelli, W. J. (2020). History and philosophy of cybersecurity education. In *Cybersecurity Education*. Routledge.

Carnegie, A., Kertzer, J. D., & Yarhi-Milo, K. (2023). Democratic Peace and Covert Military Force: An Experimental Test. *Journal of Conflict Resolution*, *67*(2–3), 235–265. https://doi.org/10.1177/00220027221116289

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & Social Sciences Communications*, *10*(1), 71. https://doi.org/10.1057/s41599-023-01560-x

Cheng, Y., & Chen, Z. F. (2020). The Influence of Presumed Fake News Influence: Examining Public Support for Corporate Corrective Response, Media Literacy Interventions, and Governmental Regulation. *Mass Communication and Society*, *23*(5), 705–729. https://doi.org/10.1080/15205436.2020.1750656

Chenou, J.-M., & Bonilla-Aranzales, J. K. (2022). Cyber Peace and Intrastate Armed Conflicts: Toward Cyber Peacebuilding? In C. Ankersen, F. Douzet, & S. J. Shackelford (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (pp. 94–116). Cambridge University Press. https://doi.org/10.1017/9781108954341.005

Christen, M., & Bangerter, E. (2017). Is Cyberpeace Possible? In F. Demont-Biaggi (Ed.), *The Nature of Peace and the Morality of Armed Conflict* (pp. 243–263). Springer International Publishing. https://doi.org/10.1007/978-3-319-57123-2_13

Christie, K., & Hanlon, J. R. (2020). Human Security and Peacebuilding: Critical Tools for Operalizing Human Rights the post-Cold War World. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion To Peace And Conflict Studies*. Routledge.

Comeau, L. (2011). Social Exclusion, Social Justice and Racism. In A. M. Hurlbert (Ed.), *Pursuing Justice: An Introduction to Justice Studies* (pp. 100–119). Fernwood Publishing.

Cormier, P. N. (2020). *The paradox of complexity in peace and conflict studies* (S. Byrne, T. Matyók, I. M. Scott, & J. Senehi, Eds.). Routledge. https://doi.org/10.4324/9781315182070-30

Council of Europe. (n.d.-a). *Budapest Convention—Cybercrime—Www.coe.int*. Cybercrime. Retrieved May 24, 2023, from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (n.d.-b). *Types of cyberviolence—Cyberviolence—Www.coe.int*. Cyberviolence. Retrieved May 24, 2023, from https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescapé, A. (2014). Analysis of Country-Wide Internet Outages Caused by Censorship. *IEEE/ACM Transactions on Networking*, *22*(6), 1964–1977. https://doi.org/10.1109/TNET.2013.2291244

D'Angelo, G., Castiglione, A., & Palmieri, F. (2022). DNS tunnels detection via DNS-images. *Information Processing & Management*, *59*(3), 102930. https://doi.org/10.1016/j.ipm.2022.102930

Dragu, T., & Lupu, Y. (2021). Digital Authoritarianism and the Future of Human Rights. *International Organization, 75*(4), 991–1017. https://doi.org/10.1017/S0020818320000624

Duguin, S., Lewis, R., Bosco, F., & Crema, J. (2022). Bits and "Peaces": Solving the Jigsaw to Secure Cyberspace. In C. Ankersen, F. Douzet, & S. J. Shackelford (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (pp. 212–222). Cambridge University Press. https://doi.org/10.1017/9781108954341.012

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*, *4*(1), 2158244014522633. https://doi.org/10.1177/2158244014522633

Fick, N., Miscik, J., Segal, A., & Goldstein, G. M. (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet* (Independent Task Force Report No. 80). Council on Foreign Relations.

Fisher, R. J. (1990). Needs Theory, Social Identity and an Eclectic Model of Conflict. In J. Burton (Ed.), *Conflict: Human Needs Theory* (pp. 89–111). Springer.

Florek, I., & Eroglu, S. (2019). THE NEED FOR PROTECTION OF HUMAN RIGHTS IN CYBERSPACE. *Journal of Modern Science, 42*, 27–36. https://doi.org/10.13166/jms/112765

France 24. (n.d.). *Info ou intox*. France 24. Retrieved June 6, 2023, from https://www.france24.com/fr/%C3%A9missions/info-intox/

François, C., & Ankersen, C. (2022). Imagining Cyber Peace: An Interview with a Cyber Peace Pioneer. In C. Ankersen, F. Douzet, & S. J. Shackelford (Eds.), *Cyber Peace: Charting a*

Path Toward a Sustainable, Stable, and Secure Cyberspace (pp. 195–204). Cambridge University Press. https://doi.org/10.1017/9781108954341.010

Galtung, J. (1996). *Peace by Peaceful Means: Peace and Conflict, Development and Civilization*. SAGE.

Geiger, J. (2021). *The Democratic and Capitalist Peace in Cyberspace*. *8*, 5–26.

Gerlach, L., & Hurlbert, A. M. (2011). Social Justice, Stratification and Oppression. In A. M. Hurlbert (Ed.), *Pursuing Justice: An Introduction to Justice Studies* (pp. 62–82). Fernwood Publishing.

Hammersley, M. (2013). *What is Qualitative Research?* Bloomsbury Academic. https://doi.org/10.5040/9781849666084

Harrell, M. C., & Bradley, M. A. (2009). *Data Collection Methods: Semi-Structured Interviews and Focus Groups*. RAND Corporation. http://www.rand.org/pubs/technical_reports/TR718.html

Hellmeier, S. (2016). The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes. *Politics & Policy*, *44*(6), 1158–1191. https://doi.org/10.1111/polp.12189

Herr, K., & Anderson, G. L. (2015). *The Action Research Dissertation: A Guide for Students and Faculty* (2nd ed.). SAGE Publications.

Hill, J. F. (2012). A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs*, 49–58.

Hoang, N. P. (2021). *GFWatch: A Longitudinal Measurement Platform Built to Monitor China's DNS Censorship at Scale*. Citizen Lab, University of Toronto.

https://citizenlab.ca/2021/11/gfwatch-a-longitudinal-measurement-platform-built-to-monitor-chinas-dns-censorship-at-scale/

Ilunga, Y. Y. (2020). New era in global security: When peace means global complex operations. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion to Peace and Conflict Studies* (pp. 481-490.). Routledge.

Ilvonen, I., & Hellsten (formerly Virtanen), P. (2015). Preparing for Cyber Threats with Information Security Policies. *International Journal of Cyber Warfare and Terrorism*, *3*, 22–31. https://doi.org/10.4018/ijcwt.2013100103

Inversini, R. (2020). Cyber Peace: And How It Can Be Achieved. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 259–276). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_13

Irvine, S. R., & Hansen, N. (2020). Missing Discourses: Recognizing Disability and LGBTQ+ Communities in Conflict Transformation. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion To Peace And Conflict Studies*. Routledge.

Jackson, R. L., Drummond, D. K., & Camara, S. (2007). What Is Qualitative Research? *Qualitative Research Reports in Communication*, *8*(1), 21–28. https://doi.org/10.1080/17459430701617879

Janc, K. (2017). *Balkanization of the Internet – Emerging Borders in the Digital Space*. WARSAW REGIONAL FORUM 2017 Space of flows, Warsaw.

Jeong, H. W. (2020). Conflict transformation. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion to Peace and Conflict Studies* (pp. 25–34). Routledge.

Johan Galtung. (1969). Violence, Peace, and Peace Research. *Journal of Peace Research*, *6*(3), 167–191.

Kaldor, M. (2013). *In Defence of New Wars* (1). *2*(1), Article 1. https://doi.org/10.5334/sta.at

Kara, H. (2018). Democratizing Research in Practice. In R. Iphofen & M. Tolich (Eds.), *The SAGE Handbook of Qualitative Research Ethics* (pp. 103–112). SAGE Publications Ltd. https://doi.org/10.4135/9781526435446.n7

Kaur, C., & Sharma, Dr. Y. (2020). *The vital role of VPN in making secure connection over internet world*. *8*, 2336–2339. https://doi.org/10.35940/ijrte.F8335.038620

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005. https://doi.org/10.1093/cybsec/tyab005

Kroeker, W. (2020). The Peacebuilding Spaces of Local Actors. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion To Peace And Conflict Studies* (pp. 57–67). Routledge.

Lam, W. M. W., & Seifert, J. (2023). Regulating Data Privacy and Cybersecurity*. *The Journal of Industrial Economics*, *71*(1), 143–175. https://doi.org/10.1111/joie.12316

Lemley, M. A. (2021). *The Splinternet*. Stanford Law School. https://law.stanford.edu/publications/the-splinternet/

Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). *The Effect of Encryption on Lawful Access to Communications and Data* (A Report of the CSIS Technology Policy Program). Center for Strategic & International Studies.

Li, J., & Chang, X. (2022). Combating Misinformation by Sharing the Truth: A Study on the Spread of Fact-Checks on Social Media. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10296-z

Libiseller, C. (2023). ‘Hybrid warfare’ as an academic fashion. *Journal of Strategic Studies*, 1–23. https://doi.org/10.1080/01402390.2023.2177987

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly*, *6*(3), 46–70.

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, *1986*(30), 73–84. https://doi.org/10.1002/ev.1427

Lindsay, J. R. (2015). The Impact of China on Cybersecurity. *International Security*, *39*(3), 7–3. https://doi.org/10.1162/ISEC_a_00189

López-Marcos, C., & Vicente-Fernández, P. (2021). Fact Checkers Facing Fake News and Disinformation in the Digital Age: A Comparative Analysis between Spain and United Kingdom. *Publications*, *9*(3), Article 3. https://doi.org/10.3390/publications9030036

Lounsbery, M. O., & Pearson, F. S. (2020). Assessing peace and conflict studies theory and practice in reconciling agency and structural sources of severe sociopolitical polarization. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion to Peace and Conflict Studies* (pp. 81–92). Routledge.

MacKinnon, R. (2008). Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China. *Public Choice*, *134*(1/2), 31–46.

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*, 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Mani, R. (2007). *Beyond Retribution: Seeking Justice in the Shadows of War* (2nd ed.). Polity Press.

Mantelero, A., Vaciago, G., Samantha Esposito, M., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, *28*(4), 297–328. https://doi.org/10.1093/ijlit/eaaa021

Marczak, B., Scott-Railton, J., Anstis, S., Razzak, B. A., & Deibert, R. (2021). *Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts* (Citizen Lab Research Report No. 145). University of Toronto. https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., & Paxson, V. (2015). *China's Great Cannon* (Citizen Lab Research Report No. 52). University of Toronto. https://citizenlab.ca/2015/04/chinas-great-cannon/

Marlin-Bennett, R. (2022). Cyber Peace: Is That a Thing? In C. Ankersen, F. Douzet, & S. J. Shackelford (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace* (pp. 3–21). Cambridge University Press. https://doi.org/10.1017/9781108954341.001

Meel, P., & Vishwakarma, D. K. (2020). Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. *Expert Systems with Applications*, *153*, 112986. https://doi.org/10.1016/j.eswa.2019.112986

Mills, G. E. (2011). *Action Research: A Guide for the Teacher Researcher* (4th ed.). Pearson.

Mingo, A. (2018). Just Laws, Unjust Laws, and Theo-Moral Responsibility in Traditional and Contemporary Civil Rights Activism. *Journal of Religious Ethics*, *46*(4), 683–717. https://doi.org/10.1111/jore.12241

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), Article 2. https://doi.org/10.3390/s22020538

O'Connell, E. M. (2012). Cybersecurity without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209. https://doi.org/10.1093/jcsl/krs017

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review*, *44*, 105653. https://doi.org/10.1016/j.clsr.2022.105653

PolitiFact. (n.d.). *PolitiFact*. Retrieved June 6, 2023, from https://www.politifact.com/

Qureshi, W. A. (2018). STEMMING THE BIAS OF CIVIL AND POLITICAL RIGHTS OVER ECONOMIC, SOCIAL, AND CULTURAL RIGHTS. *Denver Journal of International Law and Policy*, *46*(4), 289-.

Rid, T. (2013). Cyberwar and Peace. *Foreign Affairs*, *92*(6), 77–87.

Sandole, D. J. D. (2013). Extending the Reach of Basic Human needs: A comprehensive theory for the twenty-first century. In K. Avruch & C. Mitchell (Eds.), *Conflict Resolution and Human Needs: Linking Theory and Practice* (pp. 21–39). Taylor & Francis Group. http://ebookcentral.proquest.com/lib/umanitoba/detail.action?docID=1181009

Schulz, W., & Hoboken, J. van. (2016). *Human rights and encryption*. United Nations Educational, Scientific and Cultural Organization.

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, *40*(7), 898–926. https://doi.org/10.1080/01402390.2017.1307741

Shoemaker, D., Kohnke, A., & Sigler, K. (2020). What the profession of cybersecurity needs to know and do. In G. Austin (Ed.), *Cybersecurity Education: Principles and Policies* (1st ed.). Routledge.

Spence, A. M. (2018). *Preventing the Balkanization of the Internet*. Council on Foreign Relations. https://www.cfr.org/blog/preventing-balkanization-internet

Syropoulos, S., Puschett, E., & Leidner, B. (2021). Positive and Negative Peace as Predictors of Pandemic Preparedness: Evidence from a Micro- and Macro-Level Investigation During the Onset of the COVID-19 Pandemic. *Political Psychology*, *42*(5), 729–745. https://doi.org/10.1111/pops.12773

Talwar, S., Dhir, A., Singh, D., Virk, G. S., & Salo, J. (2020). Sharing of fake news on social media: Application of the honeycomb framework and the third-person effect hypothesis. *Journal of Retailing and Consumer Services*, *57*, 102197. https://doi.org/10.1016/j.jretconser.2020.102197

Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "Fake News." *Digital Journalism*, *6*(2), 137–153. https://doi.org/10.1080/21670811.2017.1360143

the Citizen Lab. (n.d.). *An information booklet on the Citizen Lab* (18033-Citizen-Lab-booklet-p-E.pdf).

The United Nations Office on Drugs and Crimes. (n.d.). *Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms*. E4J University Module Series: Cybercrime. Retrieved June 20, 2023, from //www.unodc.org

Tschirgi, N. (2020). Rethinking International Peacebuilding. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion To Peace And Conflict Studies*. Routledge.

Turner, S. (2014). Transport Layer Security. *IEEE Internet Computing*, *18*(6), 60–63. https://doi.org/10.1109/MIC.2014.126

U.S. Chief Information Officers Council. (n.d.). *Policies & Priorities*. Retrieved June 20, 2023, from https://www.cio.gov/policies-and-priorities/FISMA/

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4). https://policyreview.info/concepts/cybersecurity

Ververis, V., Marguel, S., & Fabian, B. (2020). Cross-Country Comparison of Internet Censorship: A Literature Review. *Policy & Internet*, *12*(4), 450–473. https://doi.org/10.1002/poi3.228

Withers, G., & Austin, G. (2020). Creating social cyber value as the broader goal. In G. Austin (Ed.), *Cybersecurity Education: Principles and Policies* (1st ed.). Routledge.

Žagar, M. (2020). Transforming ethnic conflict: Building peace and diversity management in divided societies. In S. Byrne, T. Matyók, I. M. Scott, & J. Senehi (Eds.), *Routledge Companion to Peace and Conflict Studies* (pp. 414–422). Routledge.

Zarras, A. (2016). Leveraging Internet Services to Evade Censorship. In M. Bishop & A. C. A. Nascimento (Eds.), *Information Security* (pp. 253–270). Springer International Publishing.

Appendix A – Ethics Approval

University of Manitoba | Research Ethics and Compliance

Human Ethics - Fort Garry
208-194 Dafoe Road
Winnipeg, MB R3T 2N2
T: 204 474 8872
humanethics@umanitoba.ca

PROTOCOL APPROVAL

Effective: August 29, 2022 Expiry: August 28, 2023

Principal Investigator:	Joshua Dogbey
Advisor:	Maureen Flaherty
Protocol Number:	HE2022-0197
Protocol Title:	*A research study towards improvement of Human Security and Peace in Cyberspace*

Andrea L Szwajcer, Chair, REB2

Research Ethics Board 2 has reviewed and approved the above research. The Human Ethics Office (HEO) is constituted and operates in accordance with the current *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*- TCPS 2 (2018).

This approval is subject to the following conditions:

i. Approval is granted for the research and purposes described in the protocol only.

ii. Any changes to the protocol or research materials must be approved by the HEO before implementation.

iii. Any deviations to the research or adverse events must be reported to the HEO immediately through an REB Event.

iv. This approval is valid for one year only. A Renewal Request must be submitted and approved prior to the above expiry date.

v. A Protocol Closure must be submitted to the HEO when the research is complete or if the research is terminated.

vi. The University of Manitoba may request to audit your research documentation to confirm compliance with this approved protocol, and with the UM *Ethics of Research Involving Humans*Ethics of Research Involving Humans policies and procedures.

Appendix B – Sample Consent Form

Peace and Conflict Studies
Graduate Programs

252 St. Paul's College
70 Dysart Road, University of Manitoba
Winnipeg, MB R3T 2N2 Canada
Phone: 204.474-8894 Fax: 204.474.8828

Research Consent Form (to be on UM letterhead)

Research Project Title: A research study towards Improvement of Human Security and Peace in Cyberspace

Principal Investigator and contact information:

Name: Joshua Dogbey
E-mail:

Research Supervisor:

Name: Dr. Maureen Flaherty
E-mail:

This consent form, a copy of which will be left with you for your records and reference, is only part of the process of informed consent. It should give you the basic idea of what the research is about and what your participation will involve. If you would like more detail about something mentioned here, or information not included here, you should feel free to ask. Please take the time to read this carefully and to understand any accompanying information.

Thank you for agreeing to participate in this research project. The focus of the research is to gain an understanding of cyber violence and cyber peace from the perspective of people who work in the area of cyber security. This is a kind of pilot study as we try to think about violence and peace in different ways. We are interested in the perspectives of people who work directly in the area of cyber-security. By participating in this research, you are helping to integrate cyber dimensions into the broader academic literature on violence and peace.

For this study, I would like to interview 4 to 6 cyber security professionals who have worked in the sector for at least two years. There will be a one-time interview session with each participant, which will last about 45 minutes on Zoom. Fundamentally, participants will be asked about how their jobs are related to cyber security; their understanding of cyber violence and cyber peace; and what reforms they think are required to protect people in cyberspace. The audio and video versions of the interview will be recorded on the University of Manitoba licensed Zoom telephony app. The video recording will be permanently deleted after the interview. The audio recording will be deleted by November 2022. No personally identifiable data will be collected, analyzed, or reported. The audio recordings will be transcribed by the Principal Investigator manually. The entire dataset will be treated confidentially.

There is minimal risk in participating in this research. The Principal Investigator (PI) will not pass any judgment on the participant. Measures have been put in place to ensure that the research does not hinder the career of participants. In addition, an interview transcript will be sent to the participant for verification. If a month passes after the transcript has been sent to a participant and no response has been provided by the participant, the PI will assume that the participant approves of the content of the transcript. Meanwhile, you can decide to withdraw from the research at any moment. A participant can alert the principal investigator of the intention to withdraw through e-mail. Withdrawal from the research will not be possible by November 2022, when the research report would have been disseminated. The research report will be disseminated to the wider University of Manitoba community via MSpace. Excerpts of the research report may be published in other academic journals. About a three-page summary of the final research report will be shared with you by November 2022 through your e-mail address.

Will you like to receive a summary of the research results? Yes ☐ No ☐

If yes, kindly indicate the medium through which you would like to receive the research results.

.....

.....

Please do you consent that the interview should be recorded in audio and video format? Yes☐ No ☐

Your signature on this form indicates that you have understood to your satisfaction the information regarding participation in the research project and agree to participate as a subject. In no way does this waive your legal rights nor release the researchers, sponsors, or involved institutions from their legal and professional responsibilities. You are free to withdraw from the study at any time, and /or refrain from answering any questions you prefer to omit, without prejudice or consequence. Your continued participation should be as informed as your initial consent, so you should feel free to ask for clarification or new information throughout your participation. The University of Manitoba may look at your research records to see that the research is being done in a safe and proper way. This research has been approved by the Research Ethics Board at the University of Manitoba, Fort Garry campus. If you have any concerns or complaints about this project you may contact any of the above-named persons or the Human Ethics Officer at 204-474-7122 or HumanEthics@umanitoba.ca.
A copy of this consent form has been given to you to keep for your records and reference.

Participant's Signature: Date:

Researcher's Signature: Date:

Appendix C – Interview Questions

Preamble:	Thank you for agreeing to participate in this research project. The focus of the research is to gain an understanding of cyber violence and cyber peace from the perspective of people who work in the area of cybersecurity. This is a kind of pilot study as we try to think about violence and peace in different ways. We are interested in the perspectives of people who work directly in the area of cyber-security. You agreed to participate in this research voluntarily, and you can withdraw from this research at any moment up until the withdrawing deadline of November 30, 2022. You can communicate your intention to withdraw by word of mouth at any moment, during this interview session. You can also communicate your intention to withdraw through e-mail.
Theme	Questions
Job Description	Please, can you talk about what your current job entails and how long have you been working in this role? What aspects of your job are related to cyber-security?
Understanding Cyber Violence	In your view, what constitutes cyber violence? Sub-questions/prompts: a. How can a company's handling of customers' digital data constitute violence? b. How can and does cyber violence affect human rights? c. How would you describe cyber-espionage? d. How does cyber-espionage affect human security? e. What do you consider to be state-sponsored internet censorship? To what extent could state-sponsored internet censorship be allowed? f. Where does the sharing of fake news fall in the debates about freedom of expression in cyberspace?
Exploring Cyber Peace	What is cyber peace, in your view? Sub-questions/prompts: a. In your opinion, how does your work as cyber expert contribute towards peace? b. What roles could countries and private entities like NSO Group, Facebook play to sustain cyber peace? c. How does the existing global internet governance structure help to build peace? d. How does technological advancement help to improve freedom of expression and the right to privacy?
Towards Change	Can you please share your views on what reforms would be required to protect people online?