Tampere University

Alhassan Issah

ACHIEVING CYBER PEACE THROUGH AN EFFECTIVE CYBERSECURITY GOVERNANCE:

Analysis of the European Union Cybersecurity Strategy

Faculty of Management and Business
Master's thesis
November 2021

ABSTRACT

Alhassan Issah: Achieving Cyber Peace through an Effective Cybersecurity Strategy: Analysis of the European Union Cybersecurity Strategy
Master's thesis
Tampere University
Masters Degree Programme in Safety and Security Management: Security Governance
November, 2021

Cybersecurity and cybersecurity governance in the EU region has been the focus of political stakeholders at the national and regional level since the early 21st century. The EU in partnership with member countries have attempted to build cybersecurity defence and resilience strategies primarily through the promulgation of Cybersecurity policies and legislations that focus on enhancing cyber infrastructures among EU countries. Beginning with the Budapest Convention in 2002, and more recently the 2013 Cyber Security Strategy, there has been annual cybersecurity reviews of existing policies to address emerging issues. These efforts have however not sufficiently addressed the growing cybersecurity threats facing EU nations and citizens so that existing statistics still puts EU organisations, governments, security infrastructures and citizens at high risks of cyber-attacks, threats and insecurity. Therefore an evaluation of the strategies adopted by the EU to enhance cyber governance within the EU cyberspace is engaged by this study to discover existing loopholes in the strategies adopted by the EU and her member countries.

The aim of the study is primarily to investigate the challenges of the EU Cyber Security Strategies that tends to hinder her from achieving her stated cyber resilience goals. The Nodal Security Governance framework served as theoretical framework and analysis tool for the study. The study was essentially a qualitative study and thus engaged a critical review of extant literatures on cybersecurity governance and cybersecurity strategy in the EU. Twenty-one (21) literatures were reviewed for the study to provide answers to the following research questions; what is the conceptualisation of cybersecurity within the EU; what are the strategies adopted by the EU to achieve cyber peace within the EU; and lastly what are the challenges of cybersecurity governance within the EU? The study discovered that while the EU and her member countries have been essentially active in providing the policy frameworks necessary for addressing cybersecurity governance within the region, enough efforts have not been deployed towards addressing the regional cohesion and diplomatic relations among member countries. Essentially, it was discovered that the nature of hostile and suspicious interactions within member countries provides grounds for non-implementation of the cybersecurity strategies across the region. This suspicious atmosphere among EU countries also works negatively against cybersecurity governance in the region. As such the study recommends that efforts must be directed towards enhancing healthy diplomacy and engendering trust among member countries if the EU Cyber Security Strategies will ultimately achieve her goals of effective cyber governance within the region.

Keywords: Cybersecurity, Cyber-peace, Cybersecurity governance, Cyber-terrorism, EU Cyber Security Strategy, Nodal security governance.

Table of Contents

List of Symbols and Abbreviations

ACS	Australia Computer Society
APCO	Association of Public-Safety Communications Officials
CIA	Central Intelligence Agency
CoE	Council of Europe
CPI	Cyber Peace Institute
CSIRT	Computer Security Incident Response Team
DCAF	Democratic Control of Armed Forces
ECA	European Court of Auditors
ECC	European Cybercrime Centre
ECPAT	End Child Prostitution, Child Pornography, Trafficking of Children for Sexual Purposes
ECSO	European Cyber Security Organisation
EEAS	European External Action Service
ENISA	European Union Information and Security Agency
EU	European Union
Eurojust	European Justice
Europol	European Police
FBI	Federal Bureau of Investigation
GDP	Gross Domestic Profit
GDPR	General Data Protection Regulation
ICANN	Internet Cooperation for Assigned Names and Numbers
ICS	Industrial Control Systems
IDA	Inter-American Development Bank
IT	Information Technology
ITU	International Telecommunication Union
JCAT	Joint Cybercrime Action Taskforce
NATO	North Atlantic Treaty Organisation
NIS Directive	Directive on Security of Network and Information Systems
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation in Europe
SME	Small and Medium Enterprises
UK	United Kingdom
UN	United Nations
WGIG	Working Group on Internet Governance

1. CHAPTER ONE: INTRODUCTION

1.1. Background of the Study

Cybersecurity is a growing field of interest in technology and the entire cyberspace primarily due to the activities of criminally minded individuals and numerous loopholes that are constantly being revealed by advancements in technology (Berg & Keymolen, 2017; Lehto, 2013; Gogwim, n.d). Cyber users and especially governments worldwide have begun to show interest in cybersecurity both as a profession and field of study due to its vulnerabilities and opportunities to the cyber world. Growing concerns on the safety of the internet space for both individual and corporate users are reflective of the activities of expert and skilled computer and internet users who employ highly in-depth knowledge of the internet technology to violate the privacy and confidentiality of the internet space for their various purposes (Australian Computer Society, 2016). World over, the activities of hackers and computer attackers have therefore been the concern governments, global institutions, private organisations and individual computer users (Myers, 2020; Harjanne, Muilu, Pääkkönen & Smith, 2018; European Commission, 2017). The various strategies adopted to combat and enhance cybersecurity across the globe range from policy frameworks, legislations, law enforcement partnerships, prosecution, development of cybersecurity awareness strategies, trainings in cybersecurity and vulnerabilities etc. (Myers, 2020; Berg & Keymolen, 2017; EU, 2017).

The growing insecurity and the inability to contain the multi-variant threats in the cyberspace have led to the emergence of the concept of cyber-peace. Although sometimes used interchangeably, it is a socio-political term that refers to a state of political peace among nations in the cyberspace especially arising from the cyber dominance and cyber arms race among superpowers (Craig & Valeriano, 2016). The concept has thus been incorporated to designate a category of cyber threats obtainable in the cyberspace. As an emerging term however, there are divergent views expressed by scholars and experts as to the extent and scope of the term and how it affects individuals, nations, and international peace at large. Hence there have been strategies, as those outlined above, engaged by both individual and corporate bodies to protect the cyberspace within their

jurisdiction and areas of operation. However, while these tactics and strategies are developed, the activities of computer hackers and other threats in the cyberspace have been noted to continue to be on the rise (Myers, 2020; Inter-American Development Bank, 2020; Porrúa & Contreras, 2020). For example, the EU Court of Auditor (2019) report noted in a study that irrespective of the actions of governments and government institutions, computer-related threats have continued to increase across the world even to the extent of threatening national security because technology has continued to and continues to evolve, revealing loopholes and vulnerabilities in former computer systems and software. Furthermore, growing concerns on cybersecurity were heightened by the infamous interference of the Russian government into the 2016 United States Presidential elections which created international rancour (Fidler, 2016). Apart from revealing the long political ideological dispute between the two world powers, it also showed the extent of cyber insecurity and vulnerability and its implication on national and global security when left unattended. In the thoughts of Craig & Valeriano (2016), it substantiates the growing thesis that arms race and security has entered a whole new cyber phase captured in the theme, 'cyber-arms race'.

This case and others relating to national security has therefore extended the scope of cybersecurity to involve national and international security issues with huge budgetary allocations by the international community (Myers, 2020; IDB, 2020; EU, 2017; Craig & Valeriano, 2016). The European Union has also been an active player in this pursuit to secure the cyberspace within the EU territory so that the use of the internet space is safe and secure as indicated in the EU cybersecurity policy (EU, 2017; EU, 2013). Nations in the EU have also established laws and policies in line with the overall aim of the EU to achieve safe and secure cyberspace by updating and revising obsolete cyber and digital laws to apply to modern information technology realities (EU Court of Auditors, 2019; EU, 2017). The United Kingdom for example has such policies as the 2018 EU General Data Protection Regulation which is a revision of the UK's 1998 Data Protection Act that protects the rights and ownership of personal data from unauthorised access and usage by intruders (Barmpaliou, 2020; ECA, 2019). There is also the 1990 Computer Misuse Act, the 2003 Communications Act, the 2003 Privacy and Electronic Communications (EC Directive) Regulations, the 2018 Network and Information Systems Regulation and several other legislations that seeks to enhance the safety of the cyberspace (Nigel & Nathan, 2020).

Governing the cyberspace however with the establishment of the above legislations has been rather difficult as global reports on cybersecurity have continued to indicate growing insecurity in the cyberspace (Myers, 2020; Harjanne et al, 2018). Worthy of note is the fact that the various attacks and vulnerabilities on the cyberspace have resulted in massive economic and financial losses for governments, institutions and individuals making it a priority for all groups of people (Myers, 2020; ECA, 2019; Gogwim, n.d). Also the growing migration and adoption of internet technologies for economic and business transactions and services has also made the cyberspace attract several unscrupulous elements and unregulated usage of the technology. As studies have also indicated, some other aiding factors of cybercrimes and attacks are the advantage of anonymity, the belief that such attacks have no physical harm, the ease to carry out, the ubiquity of the internet and digital devices, the economic value and financial gains (Snowden, 2019; Suleman, 2018; Ojetayo, 2017, Adesina, 2017). These factors and several other salient advantages that the internet presents to users make such privacy-threatening activities lucrative and common among computer users.

There is also the growing concern on the economic disadvantage of many developing and under-developing countries whose young citizens engage in many cyber financial crimes across Europe. According to statistics, young computer and internet fraudsters from third world nations such as Nigeria, Ghana, Brazil etc. engage in internet fraudsters and cyber activities that make the smooth usage of the internet impossible (Whitty, 2018; Suleman, 2018; Ibrahim, 2016; Armstrong, 2011). This is heightened by the fact that the internet is somewhat of a global community that connects and links several groups and nations across the globe in a universal community of continual interaction and communications (Chetty & Alathur, 2018; Newman & Bell, 2012; Storck, 2011). This system of interactions give room for the exploitation of data and information as it encourages storing sensitive data and information on the internet and computer devices which can be accessed by third parties with the right access combinations. Therefore, actions and activities to safeguard the internet space across countries and continents have been aimed primarily at eliminating existing threats and promoting safety and security for internet users.

The EU community consists of one of the world's most developed regions in the world with several countries blazing the trail as global leaders in information and communications technology. The EU countries have over the years developed strategies and policies for promoting the use and applicability of the internet for daily activities and

business activities (ECA, 2019; EU, 2017). However, the growing threat of the cyberspace occasioned by the activities of internet fraudsters and hackers has underscored the need for more active and direct approaches to protect the use of the cyberspace in the EU region (World Bank Group, 2019). The need for an active and effective policy approach in the EU region have become pertinent following the development of criminal and terrorist networks across European countries who engage the use of the internet to both recruit and carry out prospective threats (ECA, 2019; Harjanne et al, 2018; EU, 2017). Indeed recent developments have shown that global terrorist groups have adopted and continue to adopt cyber strategies to carry out their fundamentalist agenda in the EU utilising such internet platforms as the dark web and other secure communications platforms to further their initiatives (ECA, 2019). In a bid to tackle and prevent human casualties and escalation of these criminal online activities from assuming a physical implication and danger to not only EU citizens but the rest of the world at large, the global campaign against terrorism has therefore incorporated a cyber-dimension (World Bank Group, 2019; EU, 2017; Craig & Valeriano, 2016; Australian Computer Society, 2016).

The EU's strategy for actualising a secure cyber space while also preventing the proliferation of terrorist threats and other internet criminalities across region have evolved over time with the adoption of the recent 'Cybersecurity Strategy for the European Union' composed by the commission in Brussels in 2013 but adopted in 2017 (ECA, 2019; EU, 2017; EU, 2013). The main highlights of the policy document are to achieve cybersecurity by reducing cybercrimes; develop cyber defence policies and capabilities; develop industrial and technological resources for cybersecurity and lastly to establish international cyberspace policy for the EU (ECA, 2019; EU, 2017; EU, 2013). These objectives are all aimed at enhancing the safety and security obtainable in the EU cyberspace. There have however been challenges with this policy framework as identified by scholars and studies (ECA, 2019). Primarily, one of the challenges confronting the attainment of a secure cyberspace in the EU region as well as globally according to EU Court of Auditors report (2020) is the sophistication of internet fraudsters and hackers. According to the report, cyber attackers and hackers globally are dedicated to developing strategies and sophisticated means of carrying out their attacks and menace against computer networks and systems. On the other hand, while the EU commission and member countries are similarly dedicated to eliminating these threats from the region's

cyberspace, the technical and technological capability is largely missing in public institutions and cybersecurity policing agencies (Herczynski, 2020; ECA, 2019).

Furthermore, studies have also identified other challenges facing the attainment of cybersecurity in the EU as arising from funding and spending on cybersecurity (ECA, 2019, Harjanne et al, 2018; Craig & Valeriano, 2016). According to this view, governments such as the United States, China and Russia have maintained a trend of allocating considerable parts of their national budgets on security to building cyber infrastructure and cyber defence over the years (Craig & Valeriano, 2016). The results of these investments have been the sophistication and continual development of the cyberspace in the US and Russia than in other parts of the world. China is also a growing participant in cybersecurity which in combination with these two nations have maintained consistent development and growth overtime due to the level of funding and investment in the cybersecurity sector (Myers, 2020). Inadvertently some of the world's most famous hackers have also been associated with these three countries either as citizens or beneficiaries of the cybersecurity institutions and infrastructures. The crux here however is that cybersecurity funding and investment which has been identified as lacking in the EU countries are considered to be fundamental parts of achieving the cybersecurity and security objective of the EU strategy.

In light of the consistently dynamic challenges and vulnerabilities associated with the evolving cyberspace around the world and in the EU region therefore, the continuous scrutiny and evaluation of the various strategies adopted and established by the EU is important for the attainment of optimal results. A brief discourse however on the nature of global cyber-threats and prevention strategies is discussed in the next section.

1.2. Aims and Objectives of this research

While there remain setbacks to the establishment of a coordinated global strategy against cybercrime, various regional governments and organisations as previously indicated have adopted regional strategies to address the threats and insecurities prevalent in such region's cyberspace. Several of these strategies have been spearheaded in Americas and the EU countries. One of the major strategies adopted for this task in these regions is the development of policy documents and coordinated regional cybersecurity strategies that cuts across the member countries in such regional organisation. The European Union commission with twenty-eight (28) member countries in 2013 adopted the

EU Cybersecurity Strategy in Brussels, Belgium to tackle various threats and attacks on the effective use of the cyber space in the EU region. The main highlights of the EU Cybersecurity Strategy are;

i. Achieving cybersecurity, reducing cybercrime;
ii. Developing cyber defences policies and capabilities.
iii. Developing industrial and technologies resources for cybersecurity; and
iv. Establishing international cyberspace policy for the EU.

The broad aim of the EU Cybersecurity Strategy is to become the world's safest cyber environment through those objectives stated above. In 2017, the EU Cybersecurity Strategy was updated to include the protection of the EU's critical infrastructure and boost the EU's digital assertiveness towards other regions. For the past 11 and 4 years since the establishment of the cybersecurity strategies however, the EU cyberspace still seems far from being the safest cyberspace in the world even though there are strategies and policies that aim for this laudable feat. In light of the above therefore, the current study aims to look into the challenges of the EU Cybersecurity Strategy to determine what factors hinders it from achieving her stated aims. This study aims to do this by providing answers to three critical research questions, viz;

i. What is the conceptualisation of cybersecurity as it concerns the EU?
ii. What efforts have the EU commission put in place to achieve cyber-peace?
iii. What are the challenges faced by the EU commission to ensure cyber-peace in the EU region?

It is hoped that the answers to the above questions will provide answers to the overall aim of the study which is to interrogate the challenges faced by the EU commission from achieving cyber-peace in the region as stated by the 2013 EU Cybersecurity Strategy.

1.3. Research Method

This study adopts the theoretical analysis method to analyse the various data retrieved for the study. Research documents and policy documents within the EU on cybersecurity and cyber-peace and specifically on the 2013 and 2017 Cybersecurity Strategy are retrieved and studied to provide answers to the research questions as well as provide data for analysis. In the next section of this thesis, a detailed review of literature is conducted to review key concepts of this study such as cyber-peace, cyber-security,

cyber-threats, cyber-attacks, cybersecurity governance and cybersecurity policies. There is also a review of extant literatures on the attempts to achieve cybersecurity by various EU countries and the EU commission before the establishment of the 2013 and 2017 EU Cybersecurity Strategy to understand the trend of cyber threats and efforts by member-countries and the commission as a whole in achieving cyber-peace. The third section discusses the research methodology. Theoretical analysis is adopted to discuss extant research documents and literatures with focus on the EU cybersecurity policy strategy while the fourth section discusses the findings of the study. The fifth section analyses the findings in line with the objectives of the study and the sixth section concludes the study with policy recommendations and implications for the EU. This study hopes to contribute to the extant literature on achieving cybersecurity in the EU region by focusing on the vital policy tool of the EU to understand the gaps and loopholes that must be addressed to achieve cyber-peace and security in the EU region. This study also hopes to enhance cybersecurity research in the EU region as it is an important aspect of achieving overall cyber-peace in the EU. The findings of this study are therefore important to policy makers and cyberspace users as it shows the practical implications of loopholes in the EU Cybersecurity Strategy.

2. CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

This section broadly discusses relevant concepts and literatures on the subject of cybersecurity, cyber-peace and cyber-governance. This section also discusses extant literatures and studies on cybersecurity and cyber-governance globally and in the EU region.

2.2. Approaches to Cybersecurity

The use of the terms 'levels' or 'categories' designate the multi-variant approaches by several key actors and interested parties in the attempt to achieve national and global cybersecurity. The categories will be discussed at the technological and policy levels.

i. Technological Approach to Cybersecurity

The technological approach to cybersecurity essentially deals with the use of technical know-how and cyber skills to build cybersecurity. As Carlton & Levy (2017) puts it, the attempt to achieve cybersecurity across the world essentially involves the use of cyber knowledge to develop strategic frameworks to protect the data and information as well as the safety of working on the internet. This approach requires a level of technological skills and knowledge to execute and as Kremer et al (2019) and Stallings (2019) rationalises, achieving cybersecurity is essentially building the skills and knowledge to identify threats, and enhance resilience in computer users. This technological approach is necessary because as Carlton & Levy (2017) reasons, the threats that are obtainable in the cyberspace are essentially the products of highly skilled and knowledgeable computer users therefore outwitting these categories of mal-users must necessarily involve an investment in technological and technical know-how. According to Reddy & Reddy (2013), this approach to cybersecurity involves the use of technologies like creation of passwords, authentication of data, firewalls, malware scanners, anti-virus software etc. These approaches require purely technical and computer skills and knowledge to develop and enforce. As stated in the APCO Cybersecurity Guide, developing cybersecurity for organisations and public institutions require the use of security audits for cyber networks, thorough vendor screening, and development of password systems (APCO, 2016). These solutions and recommendations are strategies for defending the cyber in-

frastructure and structures of private and public users using purely technological approach.

The importance of this approach to attaining cybersecurity has been noted by Craig & Valeriano (2016) when he noted that superpowers like the United States, Russia and China invest millions of dollars into developing cybersecurity infrastructures. A large chunk of this goes into cyber research and innovations which are targeted at raising a generation of cyber intelligent and knowledgeable internet users (Myers, 2020; Tsakanyan, 2017; Australian Computer Society, 2016). These investments have also resulted in the creation of hackers and malware creators who constitute threats to the internet space and cyber infrastructure of nations and public institutions (Myers, 2020). The need for technological and technical know-how in combating cybersecurity has been noted by Bodeau, Boyle, Fabius-Greene & Graubart (2010) when they opined that "cyber risk mitigation approach reflects its relative priorities regarding compliance with standards of good practice versus proactive investment in new mitigation techniques". The idea reflected here is that development of cybersecurity techniques will be relatively useless in the lack of an informed audience to perpetuate or enforce these technologies in their daily use of the internet space. Therefore, the Australian Computer Society (2016) reason that as opportunities for cyber threats and violence grows with the continual expansion of users, so also must cyber defence approaches grow by focusing on research and education of cyber users.

This human perspective to the adoption of cyber technologies and development of software technologies to enhance cybersecurity is still much debated among scholars and experts in the light of artificial intelligence and robotics technologies (Christen et al, 2020; Fuster & Jasmontaite, 2020; Schlehahn, 2020). While some scholars ultimately hold the view that human resource and education on the constantly evolving cyber space and security technologies is a necessity to implement and monitor the oversee the activities in the cyberspace thereby restating the need for continual investments on technological education and research among human users (Schlehahn, 2020; Craig & Levy, 2017), others align more with the use of robotic technology to implement complex cyber and internet operations without necessarily bothering the human users (ACS, 2016). The question raised by these scholars in light of recent technologies is how useful the human input will be in the nearest future since there is the possibility of human-like robots enforcing and even developing technologies to guard the cyberspace. This has led to questions of ethics and debates on the possibility of robots to be trusted allies

in the development of cybersecurity and at the same time 'loyal servants' to the human race (Loi & Christen, 2020; Vallor & Rewak, 2017). These debates according to Poel (2020) are an attempt to guarantee not only the safety of the cyberspace for networking activities but also the security of the human race that make use of such technologies. Therefore, the technological and scientific approach to cybersecurity has continued to raise debates among scholars.

Human errors and vulnerabilities in enhancing and promoting cyber threats and attacks have also being noted as vital loopholes that make the acquisition and deployment of cyber technologies difficult (Kremer, Mé, Rémy & Roca, 2019). As Kremer et al (2019) reasons, the lack of awareness on technological knowledge and cyber threat schemes and manipulation of hackers compounds the use of sensitive data and information but for personal and organisational reasons, worrisome. Computers according to Kremer et al (2019) are only as productive, and in this case, defensive, as the person operating them so that while technologies may be developed that protects access and utility of data, the lack of know-how of human agents may be the opening hackers need to penetrate a network and cause untold havoc. Therefore scholars note that governments and organisations have focused on not just the accumulation of cyber technologies to enhance corporate cybersecurity but also the development of human resources and cyber skills (Carlton & Levy, 2017). Carlton & Levy further reasoned that most threats in the cyberspace are only as effective as the defensive mechanism against them. This defensive mechanism involves both technological human factors as well as institutional frameworks that may protect the company's critical infrastructure at all costs (Vallor & Rewak, 2017; ACS, 2016; Meushaw, 2012). This factor Myers (2020) notes has been the challenge for developing countries as although there is the availability of cybersecurity software to relatively manage the activities of malwares and hackers, the lack of technical know-how and ability to deploy these technologies in public institutions of governance has subjected critical infrastructures to incessant attacks and penetration. Hence private hackers and skilled cyber users have continued to constitute source of threats to corporate and organisational usage of the cyberspace in the region by exploiting the dearth of cybersecurity knowledge of government agencies (Myers, 2020; World Bank, 2019).

The importance of the technological education in cybersecurity gains more weight in light of the complexity in developing security software and frameworks against cyberattacks. As Schlehahn (2020) puts it, developing cybersecurity software like firewalls,

defensive software against malwares and other threats on the internet space require highly technical and cyber skills. Even so, deploying these technologies after developing them also require a certain level of cyber skills which may not be available to the average user (Carlton & Levy, 2017). This makes cybersecurity initiatives all the more complex and drives the need for cyber education and research especially in companies and public organisations where the use of cyber technologies are a sine qua non for achieving organisational goals (Morgan & Gordijn, 2020). While these approaches are primarily the vital instruments for building cybersecurity across nations and regions, it is vital to note that they do not necessarily guarantee the safety of the cyberspace for the mere fact that hackers and other categories of internet threats are constantly evolving in their schemes. This puts a limitation on the extent to which technological approaches such as the development of software and cyber-defence programmes can address cyber insecurity. Perhaps this is the reason behind the attempt by scholars and government agencies to achieve cybersecurity by not only the development and implementation of security software but also the initiation of policies at various levels to address the menace (Myers, 2020; Craigen et al, 2014). The idea is that such policies at all levels of governance may serve as a deterrent to careless online users. This is discussed in more details in the next section.

ii. Policy Approach

Another vital approach to achieving cybersecurity as revealed by the literature is the adoption of cybersecurity-based policies to strengthen the response of governments and law enforcement agencies to cyber insecurity and threats. Vishik et al (2016) observed that the policy approach to cybersecurity is a necessary step towards providing a response platform for public and private actors to build effective cybersecurity. In the thoughts of Fischer (2014), without the development of a policy that adequately defines what constitutes cyber threats, terror and insecurity, attempting to combat or build cybersecurity strategies may not be possible as it would then be difficult to classify any online action or activity as a potential threat to cyber users. For Kosutic (2012), policy involves not only the definition of cyber threats, attacks and security concerns but it also prescribes the line of action for private and public users. Essentially the idea of cybersecurity policy is to define the limits within which the freedom of cyber activities should be exercised (Gilligan & Pardo, 2020; Stallings, 2019; Kosutic, 2012). This is because as Schlehahn (2020) rightly observes, some cyber activities that constitute insecurity to

other cyberspace users do not necessarily begin or have the intention of an attack but are only an unforeseen reaction to a combination of some computer commands and codes. This is evident in the creation of the first set of malware and virus software (Kaspersky, 2020). While the intention was to secure an identified loophole the emerging computer network system, the result of such actions have resulted in the development of computer malware programs that can be used to attack unsuspecting and unprotected computers. Therefore as rightly observed by Gilligan & Pardo (2020), without clearly defining the limits and context of what constitutes cybercrime, there is likely to be an uncoordinated approach to building cybersecurity and prosecuting cyber terrorists and attackers.

Cyber policies according to the World Bank (2019) are also important aspects of organisational and government response to the growing cyber threats in view of the dynamic nature and peculiarity of threats across territories and regions. Gilligan & Pardo (2020) and Tiirma-Klaar (2011) have noted that cyber threats and attacks occur at different levels that necessitates policy actions at such levels. For instance, cyber-attacks may target personal computers, organisational or corporate computer networks, government computer networks, or law enforcement cyber network. These attacks could also result from another country in clear disregard of the authority and autonomy of the attacked country thus necessitating an international code to prescribe a series of response in such scenario (Craig & Valeriano, 2016; 2018; Tsakanyan, 2017). These different levels of cyber-attacks and threats to computer networks have occurred at different times and places that reveal that ordinary software approach to cybersecurity may be myopic and not nearly enough to combat such threats. The importance of policy development in cybersecurity according to Stallings (2019) is the clear statement of the organisational goals and the definition of a clear path to follow to attain such goals as it concerns information security technology. Therefore cybersecurity policies are a sort of description that reflects what kind of activities is allowable on the internet space for healthy interaction, communication and usage. While such activity is targeted at enhancing protection of data and information, it describes how such protection should take place. Therefore Stallings (2019) defines it as an aggregate of all directives, rules and practices that prescribes how an organisation manages, protects and distributes information including the behaviours and necessary actions aimed at protecting data and IT assets.

Among its many advantages, scholars note that such policies also help to educate computer users on the existing threats on the cyberspace and the actions to prevent such

threats from manifesting (Stallings, 2019; Vishik et al, 2016). These policies at the global, national, corporate and personal levels according to Tiirma-Klaar (2011) helps not only to provide a broad framework for the pursuit of cybersecurity but also educates users at all levels on the accepted policy-based actions, as well as threats toward cyber threats and cybersecurity. For corporate policies for instance, Carlton & Levy (2017) observed that the specific actions and decisions leading to the protection of organisational and corporate data are spelt out to employees hence they are trained in both corporate policy documents and national legislations that back their actions. Following the thoughts of Kremer et al (2019) which reflected the view that cybersecurity strategies are subject to the flaws of human operators and initiators, such policy education approach as well as training on the response to cyber threats makes employees and corporate users of the internet space less prone to threats, errors and attacks. Except in cases of dissidents, corporate bodies are known to employ cybersecurity policies that build resilience to the computer network and cyber infrastructures continually. This is exemplified by the policies of Facebook, Google and other global corporations whose policies allows for both employees and users of their technologies to identify loopholes in their networks for rewards.

The importance of a policy approach to cybersecurity is all the more important in light of the recent development of what has been tagged, ‘cyber warfare’ between nations. This is understood by Craig & Valeriano (2016) to be the clash of nations using cyber technologies in promotion of political and philosophical differences. This has been specifically spearheaded by world powers that have developed sophisticated cyber technologies in security and warfare in an attempt to reduce the physical loss of troops in the case of war (Shackelford, 2017). Such clashes has therefore being restricted to cyber-attacks against state-controlled security networks for the purpose of acquiring sensitive national security data that could empower the attacking party over the victim. Actions like this do not go unnoticed hence nations have repeatedly reached out to global bodies like the United Nations and the World Bank to develop strategies for curbing the excesses of nations in relation to cyber warfare to prevent such actions and activities (Myers, 2020). Therefore scholars like Tsakanyan (2017), Craig & Valeriano (2018; 2016) and Shackelford (2017) reason that since cybersecurity is becoming more of a political and national security concept, necessary policy framework to regulate the interaction between nations on the cyberspace is important especially to define such emerging terms as cyber terrorism, espionage, warfare etc. Through adequate policy de-

velopment, the acts and actions that constitute each of these actions can be clearly defined with a proportionate sanction to defaulters. Also Schneider (2012) notes that prohibited actions by states, corporations, organisations and private computer networks are stated by cybersecurity policies to help promote a safer use of the cyberspace to protect the confidentiality, integrity and availability of data.

By virtue of the dynamic nature of cyber threats and technologies, the Malla Reddy College of Engineering and Technology (2021) notes that cybersecurity policies are living documents which means that they are never conclusively finished but are continuously updated to reflect the existing conditions. Thus by 'living document', they show that threats evolve as cyber technology also evolves. This character of cybersecurity policies was exemplified by the Obama government in the United States of America when in 2015, he declared a national emergency on malicious cyber activities in view of the threats it constituted to national security, foreign policy and the economy of the country (ACS, 2016). This response indicated the growth of the menace overtime to the American cyberspace and has since necessitated an array of policies by various nations and in the region and globally too to enhance resilience and protection of information data among cyber users. The growing concerns on cybersecurity policies as noted by Christensen et al (2020) is that although it ultimately seeks to protect personal data from third parties, such policies may necessarily involve giving cyber experts access to these personal files to detect the maliciousness or not.

This feature is particularly contradictory and has resulted in various data protection legislations both in the EU and other nations. There is the dilemma of wanting to pursue a truly data protection policy among nations while at the same playing a 'big brother' role by accessing personal files of computer users to make sure such files do not constitute insecurity or threat to other computer users. This has been the concerns of the ethical debate by scholars and experts on the role of government secret agencies who purportedly aim to pursue a national security policy by violating the very contents and components of cybersecurity policies of nations, corporations, and organisations (Loi & Christen, 2020; Vallor & Rewak, 2017). The question this presents to the general public therefore is which of these actions constitutes a greater threat and a greater good, access to data for malicious reasons or access to data for security reasons. While these opinions are not conclusive and continues to engender debates among cyber tech experts, spying on personal and personal corporate data continues among nations in supposed pursuance of cybersecurity and national security policies (Muhammad, 2017).

While the development of cybersecurity policies are generally aimed at protecting data and information, national, organisational and corporate policies however do have specific nationalistic and organisational goals. For instance, the Malla Reddy College of Engineering and Technology (2021) noted that the national cybersecurity policy of nations like India and other smaller countries are essentially aimed at protecting their information database in light of the discovery that technologically advanced nations like the United States were spying on Indian cyber users. The crux therefore is not only the protection of data from malicious hackers and threats, but even the protection of data from those who are supposedly in the business of securing the cyberspace from malicious activities. Of course, by attempting to protect national data and critical infrastructures from major world powers through cyber policies, countries are pursuing a nationalistic agenda that protects the confidentiality, integrity and availability of sensitive data that could be used against them (Westby, Wegener & Barletta, 2010).

The question according to scholars like Poel (2020) and Shackelford (2017a) is how much can guarantee can be given to other nations across the globe that the unethical and illegal break into the cyber architecture of these nations is to pursue a global cybersecurity policy that protects them and other nations from pervading threats. The antecedent of the US spy agencies have not undermined the fact that access to national confidential files and data could be used against these nations in a supposed global effort to combating insecurity. Therefore, there seems to be a clash of security policies in relation to cybersecurity. While some nations pursue a system of cybersecurity policies that are essentially concerned with protecting their national data archives from incursion by unauthorised cyber users, some others have as their policies, the protection of their national and cybersecurity by violating the cyber integrity of these nations. Such a conflict of interests in policy developments can only result to clashes in the global scene as is evident in the attempt to establish a global cybersecurity policy across in the United Nations (Homburger, 2019).

In summary, the concept of cybersecurity continues to expand, and this expansion has made a simple concise definition impossible as several aspects of what the concept entails are difficult to capture in a single sentence. Another difficulty with defining the term is the divergent perspectives expressed by various scholars, experts, corporate bodies, organisations, governments and regions on what constitutes the term. As the array of literature has indicated, there are no single or similar perceptions to the idea of cybersecurity. While bigger nations may equate it with national and global security, other na-

tions may see it as protecting their growing cyber infrastructure from unauthorised access by bigger nation and the policies that follows from this perception reflects these views (Muhammad, 2017). Therefore, only a conceptualisation of cybersecurity may be possible but not a specific definition as a definition portrays the idea of capturing the precise meaning and extent of the term which is impossible in view of practical realities. Importantly, the conceptualisation of cybersecurity has led to newer concepts like cyber-peace, cyber governance, cyber-terror, and cyber-warfare, all in an attempt to grasp what it is cybersecurity really is. The next section discusses the concept of cyber-peace.

2.1. Concept of Cyber-Peace

Cyber-peace and cybersecurity have been used interchangeably by scholars to refer to the same condition or state of affairs in the cyberspace. However as rightly observed by scholars like Shackelford (2014), Shackelford (2017), Craig & Valeriano (2016), the idea of cyber-peace immediately connotes a cyber-warfare which is not necessarily captured in the conceptualisation of cybersecurity. This provides a basis for more interrogation of the term cyber-peace. According to former director of the NSA and CIA, General Michael Hayden, the use of the term cyber-peace connotes warfare whereas warfare requires rules to prosecute while the cyberspace is simply lawless, the national legislations notwithstanding (Shackelford, 2014; Medeiros & Goldoni, 2020). Therefore, scholars like Inversini (2020) and Shackelford (2017; 2014) would rather view cyber-peace as the construction of a network of multilevel regimes that promote global, just and sustainable cybersecurity by clarifying the rules for companies and countries to help reduce threats of cyber conflict, crime and espionage. His use of the term here sounds similar to cybersecurity but for the introduction ‘sustainable cybersecurity’. The idea of sustainable here connotes a perpetual state of stability in the use of the cyberspace without posing threats to categories of users. Therefore, cyber peace can be viewed from this perspective as the state of relative tranquillity in the cyberspace among all categories of users engendered by adherence to global cyber code of conduct that prevents conflict, crime, and attacks on the cyberspace (Inversini, 2020; Muhammad, 2017; Roff, 2016). The question however is whether such a cyber-utopian state can be achieved or can there really be a global adherence to a body of laws that could improve cybersecurity and result in a state of peace? Further still, could there be a body of laws that would ad-

dress all forms of cyber threats and eliminate vulnerabilities in the cyberspace? (Homburger, 2019) At the head of these questions is the notion of espionage and conflict between nations on the cyberspace. By the use of the term espionage and conflict, Shackelford portrays the idea that there is an existing conflict among nations on the cyberspace which is the basis of cyber-warfare and the calls for cyber-peace.

The concept of cyber-peace has been used by healthcare institutions and security experts to also designate the series of attacks that have flooded the internet space in the last couple of years. Relating the experience of healthcare workers, the CyberPeace Institute (2021) reported that the healthcare institution and her workers have repeatedly become victims of malicious attacks on the internet space with attacks in the form of data breaches (from theft to cyberespionage), disinformation of public (erosion of trust) and disruptive attacks (deploying ransomware threat to healthcare). These activities and actions have particularly thrived in recent time with severe consequences for patients, and the healthcare workers' psychological health (Gisel & Olejnik, 2018). Therefore, the CPI report noted the need for peace in the internet space due to its physical implications on the health essential workers and patients whose treatments and wellbeing depend on the sustenance of medical technology and IT systems (CPI, 2021). As Robinson et al (2018) puts it more broadly, any cyber warfare which causes blackouts, cuts off supplies, makes traveling dangerous or destabilises a national economy is clearly a threat to the stability of that nation and hence a threat to international peace and security. Therefore, such actions as reported by the Cyber Peace Institute may be regarded as a threat to the peace and security of not only the healthcare workers and their patients but also the nation at large (CPI, 2021; Inversini, 2020; Robinson et al, 2018).

What this connotes is that any cyber action the consequences of which results in the disruption of stability and order in the state of affairs may be regarded as a threat to peace and social order that must be prevented (Shackelford, 2017; Gisel & Olejnik, 2018; Muhammad, 2017; Westby, 2011). Cyber-peace therefore may refer to the attempt to prevent the various threats and attacks that characterise the cyberspace from escalating to social disruptions and physical conflicts (Robinson, Jones & Janicke, 2015). The current trend and development of cyber threats and espionage has necessitated Robinson et al (2018) to opine that there may be need for cyber peacekeeping in the near future to help main peace at the cyberspace. The need for maintaining peace in the cyberspace is all the more likely considering that nations are becoming more interested in developing and pursuing a cyber-warfare agenda in the effort to become global

players. Cyber-peace in the period of what Craig & Valeriano (2016) titles ‘cyber-arms race’ may not necessarily by the cessation of attacks and malicious activities on the cyberspace but a relative control over such. As Shackelford (2017) puts it, “the end of cyber-attacks, is politically and technically unlikely, at least for the foreseeable future” hence he opined that “working together through polycentric partnerships, we can mitigate the risk of cyber conflict by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration” (Shackelford, 2017; Shackelford, 2014).

The use of the concept of cyber-peace has also been noted as an attempt to change the perspective of readers and cyber users from a negative perception occasioned by such terms as cybercrime, cyber-terrorism and cyber-war (Wegener, 2011). This essentially means that the concept is a deliberate attempt to achieve what is currently absent in the cyberspace which are crimes, terrorism and war occasioned by individual, corporate and national actors (Inversini, 2020). As Wegener further notes, the use of the term cyber-peace implies a less forceful and military approach to an already bad situation on the internet space so that instead of military options, more civil strategies can be adopted by nations to achieve cyber peace (Wegener, 2011). The use of such phrases as ‘cyber-war’, ‘cyber-terrorism’, ‘cyber-espionage’ in the opinion of scholars who share this thought is that governments may likely resort to military options once an action has been tagged ‘war’, ‘terror’, ‘espionage’ or any other national security compromising term (Robinson et al, 2015). Hence there is the advocacy for a more tranquil resolution concept to achieve the same goal. The question that comes to mind with this conceptualisation however is whether this tactics changes the pervading threats or approach of countries to threats on the internet space.

This reverse conceptualisation of cyber-peace makes an attempted definition all the more difficult as most concepts and explanation of the term only end up describing an opposite situation and not what it is per se. For instance, the Erice Declaration Principles for Cyber Stability and Cyber Peace observed cyber peace in the notion that the sophisticated and pervasive risks on the internet space has presented nations and rogue actors with the capability to significantly disrupt life and society in all countries hence cybercrime and its resulting cyber conflict threatens the peaceful existence of mankind and also threatens the beneficial use of the cyberspace (Westby, Wegener & Barletta, 2010). By such indirect statements and explanations, no concrete definition of cyber peace is

essentially made. In the view of scholars like Inversini (2020) and Roff (2016) cyber peace is seen more in the negative definition of peace which understands peace as the absence of war and the maintenance of peace through unstable means as threats, deterrence or lack of capacity to engage in violent conflict at a particular point in time. He notes that current global cyber peace is in a negative state as although there are no outright wars as yet but conditions for escalation already exist. By engaging this negative peace perspective, Inversini (2020) attempts to capture the inability of current international and national efforts in preventing a cyber-war in the nearest future especially as nations continue to acquire and develop cyber-munitions (Craig & Valeriano, 2016).

An important feature to note of cyber-peace is that it is more of a political term than a technological phrase. This is because nations go to war and thereafter make peace. The existing cyber threats that threaten international peace and stability are essentially between nations and not necessarily between individual and/or global corporations (Craig & Valeriano, 2018; Robinson et al, 2015). The notion of Cyber warfare that has been used to describe the opposite condition of cyber peace do not also reflect individual actions against governments but government-backed actions against other governments (Inversini, 2020; Craig & Valeriano, 2018; Shackelford, 2013) hence the notion of internet governance which shall be examined later. In view of this obvious growing disregard for national sovereignty and autonomy in the cyberspace by both state-actors and non-state actors, scholars like Inversini (2020) have opined that the only way to ensure and guarantee cyber-peace is to prepare defensively for such a scenario. This would mean preparing the cyber infrastructure of nations to be resilient to attacks while also securing their critical infrastructures from invasion (Roscini, 2010). Important to note however is that this defensive approach to national security resulted in the accumulation of arms and weapons during the cold war that has fuelled global terrorism regimes (Robinson et al, 2015). Advocating such an agenda in the attempt to achieve cybersecurity therefore may only be a preparation for an all-out cyber war especially in the context of the realist approach to cybersecurity that the best form of defence is attack (Inversini, 2020; Craig & Valeriano, 2018; Craig & Valeriano, 2016). The facts seem to suggest that the quest of nations to gain ‘cyber power’ over others have resulted in the accumulation and deployment of national security threatening technologies that threatens global peace instead of guaranteed security.

2.2. The Concept of Cyber Governance

Cyber governance connotes the idea of governing the cyberspace for the purpose of regulating actions and activities to prevent security threatening outcomes from cyber users. The concept of cyber governance is one of the few concepts that have resulted from the discourse on cybersecurity in an attempt to present a broad definition. Cyber governance has become an important aspect on the discourse on cybersecurity due to the proliferation of actions and activities that tend to constitute threat to human existence in the real world (Medeiros & Goldoni, 2020; Cuihong, 2018; Munk, 2015; Kurbalija, 2014). According to Kouliopoulos, Vandendriessche, & Saz-Carranza (2020), global cyber-governance is defined as the institutions that guide and restrain collective global activities related to cybersecurity. Furthermore, the World Summit on the Information Society (WSIS) defined cyber governance as the development and application of shared principles, norms, values, rules, decision-making procedures and programmes that shape the evolution and use of the internet by governments, the private sector and civil societies (Cuihong, 2018; Kurbalija, 2014). The idea promoted here is 'common approach' to internet issues but as Kurbalija observed, this definition hardly solves the debate on internet or cyber governance.

Reflecting on the importance of cyber governance in recent times, Akyeşilmen (2018), observed that the concept presents two important factors; first is the growing need for a global cyber governance in view of the ever-increasing importance of the cyberspace to daily activities and secondly the question of who should govern or who is governing the cyberspace and more pressingly, can the cyber space be governed? (Akyeşilmen, 2018; Chang & Graboski, 2017) These questions follow from the definition of cyber governance as an aspect of global governance that attempts to ensure the protection of rights and properties across the globe. The Democratic Control of Armed Forces "*Guide to Good Governance in Cybersecurity*" also defined the term by applying good security governance principles as accountability, transparency, rule of law, participation, responsiveness, efficiency and effectiveness to the cyberspace (Democratic Control of Armed Forces, 2021). This way the idea of policing or ensuring global adherence to certain laws and guiding codes in the cyberspace is likely to result in good cyber governance. The question and doubts raised by Akyeşilmen (2018) however comes to mind as to the possibility of effectively controlling and managing such a massive, loose and virtual space which restricts no participants.

Still attempting a definition, cyber governance is viewed by the US Office of the Co-ordinator for Cyber Issues (2015) as a broad term that applies to all the diverse set of largely technical functions, all of which impacts the character of the internet. Yan (2019) notes that the concept and practice of cyber governance has become important not only for ensuring cybersecurity but even national and international security as several nations have taken to the cyberspace to pursue opposing political agenda. This resonates with the idea portrayed by Craig and Valeriano (2018), Karim, Bonhi & Afroze (2019) that the cyberspace has witnessed several nations pursuing global political agenda through cyber warfare and arms race. This happens obviously in the face of a lack of efficient body to regulate and control the activities of these countries from pursuing such ideals or viewed differently, the activities of these countries may have been stalled from escalating to full cyber war because of regulations by some existing bodies (Cuihong, 2018; Bradshaw, DeNardis, Hampson, Jardine & Raymond, 2016; DeNardis, 2016). Whatever the case, the importance of providing a governance and regulation body to oversee and possibly regulate cyber activities is laudable although seems more difficult in practice than it sounds.

The question surrounding definitions and conceptualisation of terms have been left unanswered while the use of the terms has continued by scholars and experts so that while there is no general agreement as to what precisely constitutes cyber governance, scholars like Shackelford & Kastelic (2015), Verhulst, Noveck, Raines & Declercq (2016), nevertheless notes that achieving cybersecurity must necessarily involve cyber governance at the national and international levels to regulate and possibly enforce legislations and policies that are established to govern the cyberspace at these levels. The concept and practice of cyber governance however has not been without much debates and considerations by scholars, experts and governments (Kurbalija, 2018; Nye, 2016; Munk, 2015; Shackelford, 2014). As Munk (2015) views it, the concept of cyber governance does not imply a state-centric definition where state policies, institutions and a command-and-control approach are adopted but a people-centred conceptualisation where the people and people-centred institutions are central.

By this is meant the debunking of a top-down approach that should be interrogated by the joint policy approaches that provides room for identifying and eliminating "contradictions, inconsistencies and inefficiencies caused by policies or regulations" (Tait et al in Munk, 2015; Munk 2015; Roff 2016). This idea is further debunked by Roff (2016) in her study "*Cyber Peace: Cybersecurity through the Lens of Positive Peace"*

that the politicisation and militarisation approach of major governments to cybersecurity in the supposed fight against national security is a falsehood approach that promotes the Westphalian quest for power. Specifically, the International Communications Union has been one of the key international organisations spearheading cybersecurity governance over the internet space by regulating the activities of member states while promoting cooperation amongst them (Shackelford, 2017; Kurbalija, 2018; Cuihong, 2018). Although these scholars identify the need for adequate governance and regulation of the internet space, there manner with which cyber threats are framed and addressed are not particularly in harmony. Ethical issues are identified in the approach of some stakeholders to matters of cybersecurity especially since the revelations of Edward Snowden on the violations of privacy rights by state actors (Loi & Christen, 2020; Yan, 2019).

The debates on who and what strategy to engage in governing the cyberspace has become more interesting following the activities of several private and public actors in the cyberspace who both act as guards and police of the internet space by monitoring the activities of cyber users (Yan, 2019; Mueller, 2018). The likes of this are the CIA, NSA, FBI, Anonymous, Spamhaus, Anti-Phishing Working Group, Virtual Global Task Force and End Child Prostitution, Child Pornography, Trafficking of Children for Sexual Purposes (ECPAT), CyberAngels and whistleblowers like Edward Snowden etc. (Chang & Grabosky, 2017). These groups of individuals and organisations have acted in their various capacities as cyber watchmen and employ different methods to gain access to data and information which are made available to the public for safety precautions on the internet space (Yan, 2019; Chang & Grabosky, 2017). While these groups abound in the internet space and obviously engage in extra-legal activities, they all seem to take pride in the difficult job description of regulating the cyberspace against practices and activities which threaten violate human rights and dignity.

Although these various groups project the idea of cybersecurity and safeguarding the cyberspace, there have been concerns as to the methods with which they achieve this aim (Chang & Grabosky, 2017). Snowden's revelation of the NSA and CIA's massive cyberspace regulation principles and strategies raised considerable concerns about the violation of human rights and privacy by the US government and law enforcement agencies in the supposed mission of protecting the cyberspace (Yan, 2019; Chang & Grabosky, 2017). Private groups like Anonymous have also characteristically violated personal privacy to release otherwise confidential data of cyberspace users in a supposed effort to protect cyber users. All these activities make the concept of cyber gov-

ernance all the more difficult as there is no monopoly of action, 'access' or 'force' by any private or public agency to ensure strict adherence to rule of law on the cyber space (Mueller, 2018).

According to the European Union 2020 report on cyber governance, the first attempts to build to global cyber governance strategy through the adoption of the World Summit on the Information Society for two years failed and the EU and US resorted to the private strategy to serve as the governing and regulation body for the internet (European Union, 2020). Thus the Internet Corporation for Assigned Names and Numbers (ICANN) was one of the first strategies for managing and regulating the internet while discussions and motions were considered for establishing an intergovernmental organisation through the ITU to take up the task of managing the internet space (EU, 2020; Yan, 2019; Bradshaw et al, 2016; Taylor, 2016; Kurbalija, 2014). Hence the UN's Working Group on Internet Governance (WGIG) established in 2005 began the process of ensuring internet governance by expanding the scope of the concept to include, "development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (EU, 2020: 9). Over the last decade since the initiation of the concept of cyber governance however, there have been numerous developments in the field of cyber technology that has necessitated deliberate considerations by nations and international organisations (Yan, 2019; Mueller, 2018; Taylor, 2016; Jayawardane, Larik & Johnson, 2015).

Since the establishment of the ITU, Homburger (2019) notes that there have been considerable progress among nations in promotion of cyber governance as the ITU has fostered "cooperation among member states regarding the use of telecommunication technologies and especially emphasize the purpose to promote and to offer technical assistance to developing countries in the field of telecommunications…by implementing 21 cybersecurity projects in different states" (Homburger, 2019:). Also the United States, European Union, Brazil, China, Russia and India have been key players in the development of a global governance strategy for the internet space (EU, 2020; Kurbalija, 2014). Specifically, these nations through their governments and government agencies have technically and politically supported the establishment of the ITU to enhance her efficiency and effectiveness as a global cyber police. Major telecommunications corporations, internet service providers, social media companies and domain name companies as well as civil society groups have all adopted a multi-track approach to

governing the internet specifically the establishment of global cyber policies and technical development (Gilligan & Pardo, 2020; Raymond, 2016; Savage & McConnell, 2015).

3. CHAPTER THREE: RESEARCH PROCESS AND METHODOLOGY

3.1. Introduction

The research process was structured according to the aims and objectives of the study which is to analyse the EU's Cybersecurity Strategy as a tool for attaining cyber-governance and cyber-peace in the EU region. The study therefore involved an outline of objectives and research questions structured according to the overall aim of the study. The research questions are

i. What is the conceptualisation of Cybersecurity in the EU?
ii. What efforts have the EU commission put in place to achieve cyber-peace; and
iii. What are the challenges faced by the EU commission to ensure cyber-peace in the EU region?

The study is structured to provide answers to these questions and literatures were retrieved according to the research questions listed above.

3.2. Research Process

The research is broken down into sections beginning with the statement of research aims and objectives/questions to guide the research. The first part of the study introduces the subject of cybersecurity and cyber governance as a global concern and concludes with a statement of the research aim and objectives. The second section of the research contains an in-depth and critical review of literature on the subject of cybersecurity and cybersecurity governance. A conceptual clarification to clearly define the use of terms and concepts adopted for the study is also presented in the second section. The third section presents the methodology of the research and the various steps and processes engaged in the conducting the research. The research findings are presented in the fourth section and chapter of the thesis as revealed from the review of relevant literatures using the theoretical research approach. The fifth section and chapter of the study presents a detailed evaluation of the research findings as discovered from the reviewed document and these are compared with the research questions to provide answers to the

questions. The sixth and final section of the thesis concludes the study with recommendations for addressing the challenges identified in the study.

3.3. Research Design and Method

The research design for the study is qualitative and theoretical. This methodology entails a qualitative study and analysis of a phenomenon or experience with the goal attaining a greater understanding of the behavioural patterns or characteristics of the phenomenon. This is done by studying the evidences and extant researches of scholars on the subject with the aim of understanding and possibly improving the current mode of expression. The qualitative and theoretical method is applied to this study to enable the researcher gain an in-depth understanding of the European Union's Cybersecurity Strategy and how this document has enabled cyber-governance and cyber-peace in the EU region. This is done by studying the manifestations of cyber-threats in the region, the efforts of the EU commission in building cybersecurity and the challenges of the commission's Cybersecurity Strategy. Extant literatures and researches on the EU Cybersecurity Strategy are retrieved and studied to create a balanced discussion on the subject as well as to reveal some of the challenges hindering the successful implementation of the document in the region.

3.4. Conceptual Clarification and Review of Literature

Following the outlining of the research aim and questions, the clarification of key concepts as cybersecurity, cyber-threats, cyber-governance, and cyber-peace is done to indicate exactly how the terms are applied in this study. This is done by conducting a broad review of literature on the various concepts and terms and also reviewing previous works of scholars on the stated research questions. The review of relevant literature gave the advantage of examining existing researches to reveal research gaps so that the research questions can be structured appropriately. Also the review of relevant literatures was instrumental in clarifying the various key terms employed in the research and also revealed the gaps this current study is intended to fill which is a critical study of the EU Cybersecurity Strategy for the purpose of identifying and proffering solutions to the challenges of implementation.

3.5. Sources of Data for the Study

Literatures and documents were retrieved from the internet space using search engines as Google, and other bibliography sites. Several documents relevant to the study

were retrieved by engaging key words and concepts as “cybersecurity”, “cyber-attacks”, “cyber-governance”, “cyber-peace”, “cyber-threats in the EU”, “cybersecurity in EU countries”, “EU Cybersecurity Strategy” etc. on the search engines. This method was used to download extant researches, policy documents and articles on the EU Cybersecurity Strategy and Cyber-threats in the EU generally. These documents were retrieved according to the research questions and aims as the study progressed. Also these documents served as sources of data for analysis in the study.

The literatures retrieved for the study include Munk’s (2015) study on “Cybersecurity in the European Region: Anticipatory Governance and Practices”, Franco-Fabio’s “Analysis of the European Union Research and Development priorities in cybersecurity: Strategic priorities in cybersecurity for a safer Europe”, Dewar’s “Cybersecurity in the European Union; An historical institutionalist analysis of a 21st security concern”, Lukaševičiūtė’s “EU and NATO Cybersecurity Policy”, Backman’s “The Institutionalisation of Cybersecurity Management at the EU-level”, Fuster and Jasmontaite’s “Cybersecurity Regulation in the European Union: The Digital, Critical and Fundamental rights”, Chappell, Mawdsley and Petrov’s “Strategy in European Security and Defense Strategy policy: does it matter?”, Bendiek’s “European Cyber security Policy”, Kovács’s “Cyber Security Policy and Strategy in the European Union and NATO”, Liveri & Sarri’s “An Evaluation Framework for National Cyber Security Strategies”, Markopoulou, Papakonstantinou & Hert’s “The New EU Cybersecurity Framework: The NIS directive, ENISA’s role and the General Data Protection Regulation”, Kouliopoulos, Vandendriessche, & Saz-Carranza (2020) “GLOBE Report: Case study of Cyber Governance”.

Others include, Sliwinski’s “Moving beyond the European Union’s weakness as a cybersecurity agent”, the “**European Union’s Cybersecurity Strategy for the Digital Decade**” 2020 document of the European Union, the EU’s “**Challenge to Effective EU Cybersecurity Policy**”, the European Union’s (2019) “**Challenges to effective EU Cybersecurity policy**”, Lanon’s (2019) “EU Cybersecurity Capacity Building in the Mediterranean and the Middle East”, Bendiek, Bossong & Schulze (2017) “The EU Revised Cybersecurity Strategy”, Cappalletti & Martino’s (2021) “Achieving robust European cybersecurity through public-private partnerships: Approaches and Development”, Giantas’s (2019) “Cybersecurity in the EU: Threats, Frameworks and Future Perspectives”, Sterlini, Massacci, Kadenko, Fiebig & Eeten’s (2019) “Governance Challenges for European Cybersecurity Policy: Stakeholders Views”, Pâris (2021) “Guardian of the

Galaxy? Assessing the European Union's International Actorness in Cyberspace", Griffith's (2018) "Strengthening the EU's Cyber Defence Capacities: Report of the CEPS Task Force", the EU's (2019) document on "Regulation (EU) 2019/881 Of The European Parliament And Of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", Eurosmart's (n.d) "European Cyber Security Act", Maravić (2021) "Cybersecurity Policy Development and Capacity Building – Increasing Regional Cooperation in the Western Balkans", Bendiek & Kettemann (2021) "Revisiting the EU Cyber Security Strategy: A Call for EU Cyber Diplomacy", Christen, Gordijn & Loi (2020) "Ethics of Cybersecurity", Veale & Brown's (2020) "Cybersecurity", Krüger & Brauchle's (2021) "The European Union, Cybersecurity and the Financial Sector: A Primer", Bendiek & Maat's (2019) "The EU's Regulatory Approach to Cybersecurity", the EU's (2020) December Press Release titled "New EU Cybersecurity Strategy and the new rules to make physical and digital critical entities more cyber resilient", the EU's (2018) "EU Cyber Defence Framework as Updated in 2018", Hernández-Ramos, Matheu & Skarmeta's (2021) "The Challenges of Cybersecurity Software Certification", Efthymiopoulos (2017) "A Cyber-security Framework for Development, Defence and Innovation at NATO", Kadlecová, Meyer, Cos & Ravinet (2020) "Cyber Security: Mapping the Role of Science Diplomacy in the Cyber Field".

In all, 37 documents were reviewed for the study and selection was based on the relationship of the title and abstract to the theme of study. The twenty-one documents selected above treated the EU's cybersecurity strategy from different angles such challenges, evaluation, analysis, prospects and gaps making them relevant for the study. The findings and analysis of this study was based on the in-depth study of these documents. Another criterion for including literatures was the year of publication which is restricted to literatures published not more than 6 years ago for the reason of relevance to current realities on the EU. Hence documents selected are essentially those between 2015 and 2021. Older literatures are also mentioned when necessary.

3.6. Method of Data Analysis

Theoretical analysis method is adopted for analysing the findings of the study from the in-depth study of the various literatures consulted for the research. The Nodal security governance framework was used as analytical tool. This method was used to criti-

cally analyse the findings from the study while necessary conclusion and recommendations were given after analysis. The nodal security governance pioneered by Shearing Christopher in the 1980s (Nøkleberg, 2016) was adopted to discuss how the EU engages the nodal framework in driving cybersecurity within the EU as well as how this framework can be used to address the challenges bedevilling the effectiveness of the region's Cyber Security Strategy.

3.7. Theoretical Framework: Nodal Security Governance

The Nodal Security Governance framework arises from the notion of thought that security concerns have experienced a global departure from traditional State systems and governments to include other non-State actors and stakeholders (Munk, 2015). It thrives on the fact that more individual and corporate interests have come to dominate the discourse on security at different levels. As a result, security has garnered interests from stakeholders at the transnational level to regional and even local level with the formation of bodies and institutions in these different spheres but with little interference with government structure to enhance equitable collaboration and deployment of resources for the actualisation of security goals. Consequently the hierarchical model of ensuring and driving security typical of national governments and State institutions is giving way for a more heterogeneous structure where collaboration rather than commands are the strategic approaches that enhance security governance. According to Munk (2015) the fundamental understanding of the nodal security framework is the thought that in contemporary society unlike the classical times, when security matters and decisions are made from the centre, the government must necessarily rely on the resources of the constituent elements to provide resources and tools that may otherwise not be readily available to the government. With such collaboration and resources committed to security concerns, it is only normal that security governance incorporates not only the financial resources but the interests and intellectual resources of these broad networks of stakeholders.

Nøkleberg (2016) recognised also that the traditional system of approaching security matters according to the Hobbesian theorisation necessarily saw security governance as the sole responsibility of the State which means it emerged from a top-down approach. The concept of the Leviathan very well captures the role of the State in essentially driving security through a command structure with little inputs and negotiations from other non-State actors. Indeed this view gave legitimacy to governments globally and also

helped build the solid government structure that drives global security. This system according to scholars is also reflected in the definitions given by scholars of what a State necessarily is in relations to the provision of security. In other words, nations were readily defined in relation to their ability to provide security for the territories and citizens. Nøkleberg (2016) notes that this conceptualisation of State enhanced the perspective that it "was the use of legitimate force to establish and maintain order that was sought monopolized" and Weber following the Hobbesian perspective similarly defined "States in terms of a legitimate monopoly over use of physical force to impose social order within its spatial boundaries" (Nøkleberg (2016:55).

The emergence of the Nodal security governance thought can also be readily traceable to the recognition and incorporation of civilian actors to global security concerns and the eventually modification of global national security discourse to human centred security. This system focuses not only on the government's deployment and enhancement of military measures in an attempt enhance human security but in the diversification of essential services and resources that constitute human security. Hence security concerns expanded from the predominantly military consideration to involving health, food, economic, communal, environmental, national and other strategic stakeholders that make humans relatively secure. The UN spearheaded this modification and hence promoted security sector reforms among nations. The Nodal security governance system is a necessary implication of the UN structure that drive security concerns from the perspective of this broad base of concerned actors. The Nodal framework according to Shearing et al (in Munk, 2015; 65) considered that "nodal governance is based on a special way of thinking about matters, such as governing nodes, methods for executing the influence over the events, resources to support the management, management of a given problem, and institutional structures".

The Nodal Security Governance is a security governance framework where external institutions of authority are formed to ensure regulation and control of particular security concerns (Burris, Drahos & Shearing, 2004). Traditionally the State and her institutions of governance are tasked with providing security especially as it concerns combating crimes and other similar security threats (Holley & Shearing, 2017; Nøkleberg, 2016). But current trends and observation of transnational crimes has revealed the limitations of government apparatuses from effectively curbing and tackling these security concerns especially when they involve other nations and continents. This particular difficulty and limitation informs the development of the nodal framework. According to

Munk (2015), nodes are private institutions formed outside the traditional government structure with specific needs and aims for which resources are gathered and mobilised to meet. These nodes can cut across different sphere and levels of society with little or no interference from the government (Burris, Drahos & Shearing, 2004). As such nodes could be created at the local, national or regional level to address specific security and policing concerns. Boutellier & Steden (2011) rightly observed that nodal security governance is not necessarily adopted to relegate the value of States and State security institution, rather they act as complements to existing State institution and more importantly so that States can focus more essentially on governing and effective steering of internal affairs.

The nodal system was pioneered by scholars as Shearing C., Stenning P, Johnston, L. amongst others. Shearing & Stenning (Holley & Shearing, 2017) raised concerns about the traditional forms of security governance exerted by the State which was essentially hierarchical and command-control shaped. While this system was mostly successful and engaged by the larger world in enhancing national security, growing political and technological realities necessitated a distinct approach that required a less unitary and command-control structure. Debates on the theoretical framework to address the increasingly complex security concerns especially as it extends beyond the physical space to outer space thus resulted in the proposition of nodal security governance by Shearing and other scholars (Holley & Shearing, 2017; Nøkleberg, 2016; Boutellier & Steden, 2011). The idea was to promote a less complex and narrow form of ensuring security governance across a vast territory. Hence the nodal governance system proposed is defined by Shearing & Wood (2007 in Holley & Shearing, 2017) as;

> …organisational sites (institutional settings that bring together and harness ways of thinking and acting) where attempts are made to intentionally shape the flow of events. Nodes govern under a variety of circumstances, operate in a variety of ways, are subject to a variety of objectives and concerns, and engage in a variety of different actions to shape the flow of events. Nodes relate to one another, and attempt to mobilise and resist one another, in a variety of ways so as to shape matters in ways that promote their objectives and concerns. Nodal governance is diverse and complex. (Shearing & Wood, 2007: 149)

Boutellier & Steden (2011:465) further noted that "Within assorted nodes, security is shaped by complex arrangements of agents and agencies (ranging from the public police to private security companies and active citizens) that constantly interact and struggle with each other". This implies that the partnerships and collaborations that result in a nodal security system are not necessarily free from internal clashes of ideologies and modus operandi but are constantly interacting and seeking ways to foster cordial collaborations for general security concerns. This approach to security according to Munk (2015) makes the nodal security governance framework essential and fit for addressing contemporary security concerns. This is because more permanent and pursuance of political or any other leanings that make collaborations difficult as experienced in the traditional State structure ultimately works against attaining security at whatever level. But the nodal framework encourages collaboration even in the midst of several differences and ideologies. The strength of this collaboration is the focus on the ultimate goal which is security governance. As long as parties are aligned with the main objective of collaboration, behavioural modification and complex arrangements can be easily negotiated for the common good.

An essential characteristic of the nodal approach to security governance is the fact that there is no centre which controls the affairs of the network as is visible in the State hence the value and priority of constituting members of the nodes are protected and essential in security decisions (Boutellier & Steden, 2011). Since the success of the network is dependent on the resources and contribution of the nodes, every member is therefore essential and important in the decision making process especially as it concerns security governance. This system of security governance cuts across both public and private institutions and organisations so that it presents a robust and interactive form of convergence to existing security stakeholders in an attempt to decentralise security governance. Another risk this form of security governance helps to address is the possibility of abusive security governance from State-actors (Holley & Shearing, 2017). Whereas some States would have adopted security governance and policing strategies that may have been detrimental to the organisational frames and interests of private organisations, the nodal system addresses this by incorporating both private and public institutions in an objective-driven alliance (Nøkleberg, 2016; Munk, 2015). This alliance draws on the common aspiration of security needs and mobilises resources from these sources as well to see goals achieved.

There are four risk based approaches and steps taken by the nodal security governance to ensure effective security governance; the first is reactive strategies based on punishment, reaction and retribution of crimes related to the criminal justice system; the second is nodal technologies which refers to the tools used for exerting influence over a course of events; the third is nodal resources which determines to a large extent the level of implementation of technologies for enhancing security governance; and lastly is the nodal institutional structure that determines the mobilisation of resources, mentalities and technologies for the common goal (Nøkleberg, 2016). Any Nodal system must therefore necessarily incorporate these concerns and structure to orderly and effectively enhance security governance. This system of security governance has increasingly become popular in the Western sphere and even global politics as nations at various levels are increasingly forming nodal governance systems to drive common policies and agenda that affect them on different levels. Although the Nodal security governance was formed and basically used in the security and policing sector, the success and prospects of the framework has enhanced its extension to other global sectors.

In relation to this study, the nodal security governance model saddles the question of cybersecurity with the European Union and not just the separate nations within the EU. This is because due to national limitations based on narrow nationalistic policies, regional interests and alliances may not be effectively captured by the separate nations (Wilson & Laidlaw, 2017; Nøkleberg, 2016; Munk, 2015). Meanwhile the growing concerns of cybersecurity and cyber-threats have attained regional proportion such that big corporations and government institutions are increasingly becoming threatened by outsider and insider threats. Hence the EU serves as a nodal security framework for addressing these issues. Within this broader nodal framework however, the study investigates the other nodal systems such as mentalities, political ideologies, strategies, institutions and practices that create smaller nodes in the pursuit of cybersecurity governance in the EU. Addressing these cyber concerns however necessarily involves establishing reactive and retribution strategies for cybercriminals and other threat actors, establishing the necessary methods, technologies and agencies for ensuring and extending cybersecurity governance over the EU, the mobilisation of resources from constituent members to ensure effective deployment of the technologies and lastly the establishment of the institutional structure within the EU cybersecurity agency to ensure the mobilisation of resources, mentalities and technologies (Wilson & Laidlaw, 2017). The success of the cybersecurity agenda of the EU however is closely tied to the effectiveness and align-

ment of thoughts of the various nodal structures within the EU with the overall aim of the EU nodal structures as well as the strength of the various strategies identified above. This study however investigates the various nodal structures within the EU using the Nodal security governance framework to understand the challenges presented by these nodes.

4. CHAPTER FOUR:PRESENTATION OF FINDINGS

4.1. Context of Study

The findings presented in this section of the research were retrieved from the review of selected literature on the EU cybersecurity framework in the EU countries. Hence data were retrieved from contexts where the EU cybersecurity laws and mechanism have operational jurisdiction. This was in an attempt to answer the RQ1, which focuses on the conceptualisation of Cybersecurity in the EU and among her member countries? Also, the selected documents were reviewed to determine the strategies and efforts put in place by the EU to combat and enhance cybersecurity in the EU (RQ2). The last research question RQ3 was further engaged to determine the existing challenges of the EU cybersecurity strategy. Therefore, the qualitative research design was adopted to comprehensively consider the findings in this regard and critically discuss the findings from the existing studies.

4.2. Data Collection and Analysis

Data was collected from existing research not more than six (6) years old so that information could be relatively recent and related to current realities in the EU. However, references will be to the earliest cases of cyber-attacks in the last 20years representing the beginning of the 21st-century cyber-attacks. This is done to roughly capture the trend and proliferation of such cyber-attacks and threats from the beginning of the first years in the current century to date as it relates to EU countries. Thus, research and literature on the EU Cybersecurity Strategy between 2007 (when the first case of cyber-attacks was recorded) and 2021 were retrieved for the study. The sorting of the literature and their relevance to the current study was done within two months to determine which contained relevant information. Therefore, studies outside the scope of the current research both in time frame and context were excluded, and only relevant documents within the scope of the study were retained. The findings of the study are presented in headings according to the overall aim of the study. These findings were also analysed

using theoretical analysis which critically discussed the findings and allowed for comprehensive consideration of the various research findings.

4.3. Findings: Cyber-threats and Cyber-attacks in EU Countries (Cases)

According to the literature, the threats and attacks on the cyberspace in EU countries has grown exponentially in the last couple of years. In the estimation of some scholars, cybercrimes constitute half of crimes in some EU countries and majority of EU citizens are beginning to see the possibility of being victims of one form of cybercrime or the other more than ever before (Mortera-Martinez, 2018). Several incidents and events have been identified as awaking the consciousness of the EU to the dangers and vulnerabilities of the cyberspace. For example the studies of Pâris (2021), Giantas (2019), and Meer (2015) observed that the attack of Estonia in 2007 was one of the earliest incidents of cyber threats that awakened the need for a response mechanism to the numerous threats on the cyberspace.

In 2007, the Presidency, parliament, government ministries, political parties, media, banks, and communication structures were attacked by cyber-attackers from Russia. This was an extension of the political brawl between two countries over the removal of the Bronze Soldier of Tallinn statue in Estonia (Giantas, 2019). The Estonians in furtherance of their political agenda to rid the country of the oppressive tendencies of Russia removed the statue from the Estonian city of Tallinn while the Russian government saw this as an affront on the cultural heritage and disrespect for the Red Army which fought Nazi Germans during the Second World War. After efforts by the Russian government to stop the removal proved abortive, the cyber infrastructure of the Estonia was attacked that manages and ensures the smooth running of the country as the whole country was covered in WIFI. The DDoS attack on the nation was possible because Estonia was operating an e-government system as virtually all government services were available online and 86% of the population did online banking hence internet technology accounted for voting, education, security, banking and economy (Giantas, 2019; Meer, 2015; Kozlowski, 2014).

As a result of this attack, parliamentary email servers were disabled, credit cards and automation machines were disabled, along other online activities. The attack had lasted for a month but was only noticed after several disruptions and damages had been caused. Although perpetrated by Russia, there were no much damages and the idea is

generally aired that the Russian government used the attack to prove her political superiority over Estonia on the issue of dispute but for the quick response of Estonia and other allies in overcoming the attacks (Pâris, 2021; Giantas, 2019). While the country relied heavily on infrastructure however, there was no strategy for protecting the critical technology from possible attacks as later occurred. Although the failure to ensure this cyber-protection strategy has been attributed by Pernik & Tuohy (2013 in Giantas 2019) to the lack of awareness since prior to this time there had not been any case of such magnitude of attack against a country's cyber infrastructure. Also this opened a new level of possibilities in the cyberspace for EU nations as warfare was taken to a new level. The attack originating from a major country increased the awareness of the vulnerability of EU countries to such threats and attacks on the cyberspace not only by thrill seekers or black hackers but by also governments.

Countries aspiring to join the EU have also witnessed similar attacks from Russia in what is believed to be a political game of power against the EU commission showing obvious supports for the political aspirations of these previously Russian territories (Pâris, 2021). Georgia and Ukraine have been victims of the cyber prowess and attacks originating from Russian sponsored hackers. In the case of Ukraine, the attacks were aimed at the power grid system. The Ukrainian power grid attack in 2015 caused a major damage to the energy sector of the country. The attack caused power outage that resulted in severe consequences for the country as the nation's power grid was essential to the daily activities in the state. Amongst other effects, this attack also revealed that these critical infrastructures needed protection and resilience to guide against such interruptive attacks on a mass scale. According to Lété & Pernik (2017), the Ukrainian attack was "Europe's next big shock" after major cyber-attacks on Estonia and Georgia. The growing vulnerability of nations in the EU was thus implicated in the various attacks that targeted critical national infrastructures. Although there were cases of individual and corporate cyber-attacks, the attacks on the critical infrastructure of nations underscored the need for greater attention to EU cybersecurity.

In the case of Georgia, similar to the Estonian attack, the cyber-attack here was a part of a full scale war between Russia and Georgia on political domination grounds in 2008 (Meer, 2015). At a time when the nation was aspiring to belong to the EU and NATO, Russia launched attacks aimed at stalling this integration. This involved land, air, sea and cyber conflict with the nation of Georgia. Russia was rather successful in the cyber DDOS attacks that shut the Georgian government's access to the outside world using

her cyber infrastructure (Mortera-Martinez, 2018; Kozlowski, 2014). While physical combat was prosecuted, cyber war was used to handicap the government's ability to control the narratives on the web which had been hacked and manipulated by Russian-sponsored hackers (Gianatas, 2019). The DDoS cyber-attack was presented in two phases: the first attack targeted news and government sites using botnets to conduct the attacks while the second phase of attacks blocked access to financial institutions, education, businesses, western media and a Georgian hackers website (Kozlowski, 2014). This resulted in the country's inability to communicate with the outside world and also helped Russia propagate political propaganda against the Georgian government that stirred up cyber activism against the government. This attack is adjudged the most successful attacks against a national government as it completely shut out the government and controlled the information disseminated from the country's news media stirring up ill sentiments against the sitting government. According to Giantas (2019), this attack by Russia was not only aimed to testing the cybersecurity architecture of the State but also aimed at testing the cyber-defence of the NATO and EU which were close allies to Georgia. The country was however able to recover from the attacks with help from allies.

The possibility of these attacks as findings indicate from the study has since increased from that perpetrated by Russia to include other nations and individuals who engage in these attacks for monetary and ideological reasons. The Estonian cyber-attacks also had the implication of associating and aligning national security with cyber infrastructure so that both are treated with equal attention not only by EU countries but globally. The vulnerability of relying on the internet technologies without requisite security backgrounds and strategies was revealed by the Estonian attacks to be highly against the interest of the government and citizens making use of internet technology. The fact that the attack originated from within the EU region also revealed the level of hostility and aggression some countries in the region were willing to engage in pursuit of national interests and political agenda over other smaller nations in the region. Thus countries within the EU pursued national cybersecurity frameworks. Indeed Germany before the Estonian attacks had passed her cybersecurity policy in 2005 under the "National Plan for Information Infrastructure Protection" which was aimed at protecting the IT infrastructure in the State. Sweden also passed the "Strategy to Improve Internet Security in Sweden" after the Estonian attacks and became the first EU nation to adopt and

implement a broad national cyber policy governing and protecting the use of internet against the various attacks (Giantas, 2019).

The investment of the German government in cybersecurity infrastructure is also traced to the pervading threats and attacks directed at the nation's infrastructure. This was reported in the study of Bendiek when during the 2011 Munich Security Conference, the then-German Minister of interior had revealed that the country's network was constantly attacked at least four or five times a day by foreign intelligence (Bendiek, 2012). Although in the argument of Lété & Pernik (2017) and Bendiek (2012), this is not a new phenomenon in national security as nations including Germany may have also tried to gain access to other nation's cyber infrastructure for intelligence purposes. Cyber investigations had revealed that the German Federal Intelligence Service had engaged in similar operations infiltrating 90 computers in the Democratic Republic of Congo and Afghanistan (Bendiek, 2012). The idea however is that Germany and other member countries in the EU are continually faced with the possibility and vulnerability of attacks on political and economic grounds. Demertzis & Wolff (2019) also observes that nations engaging in cyber-espionage or cyber-attacks employ the services of hackers and hackers' groups to perpetrate these online activities. This generally creates an air of suspicion and vulnerability among EU countries and international relations by extensions. The goal of political cybersecurity attacks as discovered from the study is to most times to cause a regime change and disrupt national economies by creating a system of distrust in the capacity of the government to manage the affairs of state. This is done by crippling the smooth running of daily activities of the nation by attacking critical infrastructures as power, internet, communication, and misinformation, etc. which are strong pillars for national and economic development. This strategy can be noticed from the records of attacks aimed at nations in the EU from 2007 especially by Russian government-aided hackers.

The cyber threats and vulnerabilities of the EU region also have economic as well as political implications. For instance, in 2008, the German Police reported that 38,000 criminal cases of and online financial fraud and identity theft was reported. In 2010, the statistics indicated that such threats and practices had risen to 60,000 with a record loss of 6million euros within two years (Bendiek, 2012). Major European companies and corporations have also become possible targets of numerous hackers and cyber-attackers who are constantly seeking ways of financially exploiting the rich EU countries. According to Bendiek's study, there were over 30,000 vulnerability analysts willing to sell

their expertise to organised crime syndicates and even governments as at 2012. This statistics have risen in recent times as investments by nations and corporations have considerably increased technical knowledge and skills among young persons both within and beyond the EU countries (Myers, 2020). In the study of Demertzis & Wolff (2019), findings showed that there is a considerable increase in cyber-threats and attacks to EU nations and companies. For instance the study findings showed that between the years 2016-2017, German companies recorded a damage of €43billion from data espionage and sabotage. The study also revealed that seven out of ten companies have been subject to cyber-attack in the country. Similarly, reports in the UK indicated 32percent of companies recorded cybersecurity attacks in the 2019 which was lower than the previous year with 43percent.

The threats of cybersecurity in the EU have escalated and continue to grow due to the growing ambitions and political behaviours of aggressive nations with high expansionist agenda (Bendiek, 2012). Powerful countries like the US, Russia and China are typical examples of such countries that have employed technological and cyber resources to pursue their global political expansionist agenda so that while nations in pursuit of national security are concerned with protecting cyber infrastructures, these countries have repeatedly engaged in cyber-espionage (Pâris, 2021; Giantas, 2019; Lété & Pernik, 2017). As Kavanagh (2017) reasons, while cyber technologies contains several vulnerabilities that can be utilised for personal, corporate or national purposes, the real threats to cybersecurity are the personalities engaging the vulnerabilities and loopholes of these technologies and not necessarily the technologies themselves. As such the aggression of Russia against EU countries typified in the cyber-attacks against Estonia, Georgia, Ukraine and other countries in the West are direct results of the political ambitions of Russia. As such, an important variable in the discourse of cybersecurity as discovered from the study is the diplomatic relations and interrelation between countries. This is important because politically hostile countries could engage cyber and technological resources to pursue or prosecute political disputes and conflicts. Therefore the level of threats against EU member countries can be estimated in light of the growing aggression of countries like Russia and China against the EU (Bendiek, 2012).

International trade wars and disputes between China and the EU on standards of manufacturing and labour terms within the EU and beyond have resurfaced in recent times due to the nonchalance of the Chinese government to adhere and implement international labour standards (Bošković, 2020; Yilmaz, 2020). This and other factors that

have increased tensions between States has made the use of cyber technologies to influence political and economic policies in other States have made the cyberspace within the EU more prone to attacks by other States and non-State actors (Brady & Heinl, 2020). Although economic and financial crimes and attacks are more common to EU nations and companies, Kavanagh (2017) opines that such attacks may not be totally eliminated from occurring from State actors in pursuit of economic gains and agenda. While there are no proofs to back this claim however, the trade and economic disputes between the global economic standards championed by the EU and disputed by other nations could be regarded as some of the likely reasons for the increasing vulnerability of EU countries to cyber-threats and attacks. This only goes to prove the point that political actors as well as State and non-State actors are sources of cyber-threats in the EU region especially when such actions are results of differing political and economic views with either the EU or EU member states. Just like internal security therefore, the state of cyber insecurity in the EU as findings indicate is a reflection of the diplomatic relations with other nations.

The WannaCry and notPetya attacks on the cyber infrastructure of 150 countries across the world, Europe inclusive, are cases of cyber-threats and attacks that necessitated the cooperation of the EU countries to combat these cyber concerns. In 2017, multiple variants of ransomware with the name WannaCry spread on the internet globally across 150 countries affecting thousands of individual and organisational users in the EU and beyond (Pâris, 2021; Giantas, 2019). The ransomware locked users out of computer networks and essential services and demanded a ransom for access to be logged back in (Mortera-Martinez, 2018). The ransomware spread affected several sectors across nations including telecommunications, healthcare, gas and government with about $1billion loss recorded in a week. The WannaCry attack succeeded in crippling activities in the EU region with the healthcare sector of the UK particularly affected. Several data and files in the healthcare sector were lost to the attack with the effects that people's health records and appointments for operations including emergency units of the sector were distorted (Giantas, 2019). The magnitude of this attack across the globe and the effects recorded in several countries including the EU, indicated the volatility of modern technology and the dire need for cybersecurity measures to protect the internet data especially cloud technology.

The NotPeya attack followed immediately after the WannaCry ransomware. This attack similarly affected many countries across the globe and is traceable to the Ukrainian

accounting software M.E.Doc (Giantas, 2019). Hackers were noted to have used sophisticated software backdoor to access this software and spread the infection to other countries in Europe and beyond, a total of 64 countries in all. The NotPetya attack like the WannaCry also locked users out of their computers and demanded a ransom for access. However while payments were made for the restoration of the network by users, the hackers did not restore services as the confirmation mail for the payments were shut down and over 2000 users were affected with a recorded loss of $1.2billion (Mortera-Martinez, 2018). The attack has also been traceable to the Russian government by other countries following investigations and style of attacks but as Pâris (2021) observes, the EU has not openly acknowledged this for want of conclusive evidence and only publicly condemned this attack whereas member countries of the EU has directly accused Russia of perpetrating this attack. According to Pâris (2021), the EU in an attempt to prevent wrong attribution is only protecting her integrity and credibility as a major global cyber actor. However rationalisations for the deployment of the NotPetya ransomware have been traced to the ill political and historical relations between Russia and EU countries. The NotPetya and the WannaCry attacks according to Giantas (2019) had the implication of rallying the EU member countries to seek ways to protect the cyber infrastructure in the region as the vulnerability of the cybersecurity framework was revealed in the two consecutive attacks.

In their studies on cyber threats assessment in Europe, Kertysova, Frinking, Dool, Maričić, & Bhattacharyya (2018) outlined the various types of cyber-threats prevalent across Europe and European countries. The study identified malware and phishing, distributed denial of service (DDOS), and data breaches attacks. Findings showed that malwares such as ransomware, Trojans, worms, viruses and backdoors were prevalent forms of attacks on companies and individual computer network system in the EU. The EUROPOL reported in 2016 that ransomware was a dominant concern in the EU with such ransomware as CryptoWall, CTB-Locker, TeslaCrypt and Locky (Kertysova et al, 2018). Also in 2017, the European Union Network and Information Security Agency (ENISA) identified ransomware as one of the main areas of malware innovations inotherwords, considerable attention was being invested into the creation of sophisticated ransomware by hackers. Several other private sector reports indicated similar development of interests in ransomware creation has made it a multimillion dollar business generating a profit of $25million. Bulgaria and Romania are however the two nations in the EU region that have suffered considerably from the ransomware attacks in comparison

to the other member countries which have recorded below average statistics in such attacks. Although other nations in the regions have suffered harms from such attacks, findings indicate that Russia and Iran have recorded more harms than any EU country.

DDoS attacks have also been recorded in recent times in the EU region increasing with time according to the technological advancement of the nation involved. According to Kertysova et al, (2018), the DDoS attacks prevalent in the EU region originates majorly from five EU countries, Romania, Netherlands, Germany, France and UK while the targets are usually the UK, Netherlands and Germany. Some of the DDoS attacks that have affected EU countries and companies are the 2014/15 New year eve's DDoS attack on the Finnish bank, OP-Pohjola Group that denied customers money withdrawal services and other online services from the bank, the January 2016 DDoS attack on the HSBC bank in London that disrupted customer banking services although no recorded loss was incurred, and the 2016 DDoS attack on DNS-services by Dyn that affected and shut down web access to internet companies as Facebook, Netflix, Twitter, and Amazon in the UK and US (Kertysova et al, 2018; Mortera-Martinez, 2018).

This attack is engaged for different purposes ranging from attempt to disrupt online network of competitors to politically motivated attacks aimed at crippling governance as in the Estonia cyber-attack case or it could also be a part of a sequence of attacks aimed at penetrating and installing a malware in a network system (Kertysova et al, 2018). Whatever the case, this system of attacks has been used against nations and corporations in the EU and findings indicate that the trend continues to be increase with hackers and creators inventing more sophisticated ways of planting these attacks with the use of 'BoTs' or 'zombies' to maintain access and prevent early detection. These attacks pose threats to financial institutions within the EU and to governments engaging the internet for vital services as findings show that 98% of DDoS attacks in the region are targeted at large corporations (Brady & Heinl, 2020; Kertysova et al, 2018). As witnessed in the Estonia attack, an extended distributed denial of service attack may have severe national security implications in the coming years due to the growing sophistication of the tools for attacks.

Data breaches, according to findings by Kertysova et al (2018), is an emerging cyber-threat for the EU targeting the health sector amongst other sectors. The infamous WannaCry ransomware deployed against the UK National Health Service is one of the instances of data breaches that grossly affected the healthcare sector and service. As a result of the attacks, 6,912 appointments (including operations) were cancelled and

19,000 appointments were affected with ambulances diverted from emergency centres with test results delayed among other disruptions and elimination of data. This threat is dangerous to the EU because as observed by Pâris (2021), Giantas (2019) and Kertysova et al (2018), healthcare services can be equated to life and health of EU citizens, therefore attempts to breach sensitive data as health services records more than anything directly impacts the life and health of individuals hence the magnitude of the threats cannot be overemphasised. Data breaches according to Giantas (2019) is further complicated by the cloud technology adopted by many countries in the EU which makes storage of much vital data possible with less physical facilities and devices. While this is advantageous to large corporations and nations with large quantity of data, the risk is however high because as findings indicate, more information could be lost in fewer attacks than previously. Any successful attacks on the cloud storage technology or the contracting cloud technology data storage company could result in loss of large files. Hence although his findings indicate that such attacks are decreasing in comparison with other forms of cyber-attacks against EU countries, data breaches are nonetheless more devastating.

In the same vein, studies by Brady & Heinl (2020) identified Spear-phishing as one of the growing threats in the EU especially in Ireland. In their studies although they observed a great threat arising from this threat, they however reasoned that not all phishing attempts are successful in the region especially due to the level of public awareness on the phenomenon on the internet space. Their study also noted that two-thirds of Irish businesses and internet users have been targeted for phishing in 2018 compared to 33% percent of global internet users. Phishing, targeted spear-phishing and email spams are used by cybercriminals to target organisations and large corporations' internet websites to monitor how financial transactions are run, for weeks before engaging in spam mails and targeted attacks to either clone these websites to get their customers or employees to divulge confidential information. As a result many businesses and large corporations' employee may get hundreds of spam mails trying to get sensitive information. Brady & Heinl's studies also discovered that spear-phishing and leaks of sensitive data has increased in recent times through social media platforms as Facebook, Instagram, LinkedIn and Twitter due purposely to the lack of awareness of social media users who are mostly victims of these attacks.

Financial cybercrimes are however increasing in the EU as reports indicate. According to studies by Demertzis & Wolff (2019), countries in the EU have consistently wit-

nessed increase in financial related cybercrimes and non-financial crimes from 2011 to 2018 with a little decline in 2018. According to findings, data breaches and financial frauds are daily targeted at countries and companies within the EU. For example, Bulgaria was a victim of such attack in 2019 which resulted in the stealing of personal data of 5million Bulgarians in an attack against the Bulgarian Tax authority. This amount of data could be potential tools for massive financial fraud and attacks as financial records of companies and individuals are invaluable tools for financial criminals especially those affiliated to States and terrorist groups. Between 2018 and 2019, various public institutions, companies, international institutions, academic institutions, nongovernmental institutions, and other unspecified targets within the EU were reported in the press as victims of various cyber-attacks. While the cost and quality of these attacks were not as huge, the fact that public and private institutions alike are victims of these cyber-attacks projects an idea of accessibility to and exploitation of confidential and personal files on the internet by hackers.

Although national and regional data on the economic costs of cyber-attacks on the EU is lacking, findings from a 2015 survey for the private sector in the EU estimated a total of $62.3billion loss in revenue. In the UK, findings show that the total cost of cybercrime suffered by UK companies in 2016 is estimated at €33.billion which is 1.1% of the country's GDP for the year. For Germany within the same fiscal year as the UK, cybercrime resulted in a total loss of €22.4billion which is about 0.76% of the Germany's GDP. In the Netherlands, the loss was estimated at €10billion which was equal to 1.5% of the country's GDP. The report however noted that 75% of this was an opportunity cost as direct loss was a total of €2.5billion which represents 0.32% of the GDP (Kertysova et al, 2018). For the Irish government, 2014 data indicates that cybercrimes cost the economy a total of €630million. Furthermore, defensive costs resulting from adoption of cyber defence strategies by countries in the EU have also considerably increased over the years. According to available data, business across Western Europe spent a total of 19.5billion dollars on cybersecurity tools to improve cyber resilience and security in 2016. Generally, the European Cybersecurity market was estimated at 22billion dollars as at 2016 with prospects for increase as projections estimated an increase of 8% per annum on cyber services. The UK had also invested a total of £1.9billion on cybersecurity between 2016 and 2021 (Michel et al in Kertysova et al, 2018).

Similarly, studies by the European Court of Auditors discovered that the cyber-threats phenomenon in the EU region is quite alarming than most EU member states were willing to acknowledge or address. According to their findings, the economic impact of cybercrime raised fivefold between 2013 and 2017, with serious economic effects on large and small companies as well as governments (European Court of Auditors, 2019). Reflecting this, the report observed that the fact that between 2018 and 2020, cyber insurance premiums rose from €3billion to €8.9billion reflects the level of threats and seriousness of cyber-attacks on the region's economy. The report also noted that although in 2016 alone, 80% of businesses in the EU had experienced one form of cybersecurity incident, 69% of businesses in the EU had no basic understanding of their exposures or vulnerability to cyber-threats and attacks. Another 60% had never estimated their potential financial losses. The ECA also noted the huge financial disparity between the cost of launching a cyber-attack and the cost of prevention, investigation and reparation. They noted that a DDoS cyber-attack could cost less than €15 to launch in a month but result in huge financial and reputational losses for the target (ECA, 2019).

The findings on the level of vulnerability and attacks on Small and Medium Enterprises in the EU indicate a growing trend of attacks on these businesses for several reasons. According to findings by Giantas (2019), the SMEs are very vulnerable targets in the EU as they adopt little or no cybersecurity strategies to safeguard their data for the reason that they are not big enough to attract cyber-criminals. Also although SMEs constitute 99.8% of businesses in Europe, they are ill-equipped for cyber-attacks and threats hence they are mostly targeted by cybercriminals according to findings by Brady & Heinl (2020), European Court of Auditors (2019) Giantas (2019). Giantas's studies further showed that while larger businesses may record higher costs in nominal terms, the financial impacts for smaller enterprises in some EU nations are disproportionately high. The threats to SMEs in the EU are further compounded by the lack of adequate awareness and appreciation of these cyber threats to business stability and progress by small business owners.

The flexibility and rapidity with which businesses expand and meet social needs in the EU region makes them very vital part of the regional economy therefore the growing threats to the financial stability and growth of these businesses makes them a major threat to regional economic stability and development especially as reports have shown that these SMEs constitute the major percentage of businesses in the region. The focus of hackers on businesses has also extended to medical manufacturing companies so that

SMEs businesses across the various sectors are possible targets of cyber-attacks. This puts businesses of all scale around the EU with cyber technology on high alert especially in a time when physical interaction and transaction are giving way for virtual business transactions even among SMEs around the world.

Findings from the study also reveal that cyber-terrorism threats are sources of threat in the EU as records show that there have been several attempts to attack countries in the EU by individuals and groups sympathetic to terrorist groups (Mortera-Martinez, 2018). The case of Junaid Hussain Abu Hussain al-Britani who founded "Team Poison" and launched cyber-attacks against the NATO and British Ministry of Defence are examples of hacktivist and cyber-terror attack (Jayakumar, 2020). Although a citizen of the UK, he got radicalised and travelled to Syria where his hacktivism led to his being an ISIS member and a strong social media (Twitter) influencer for the terrorist group. He was also a key member of ISIS cyber offensive team that launched attempted several cyber-attacks against the Western government. Although these attacks did not amount to much because of the sophistication and preparedness of the US and UK government to clamp down on Junaid Hussain, his was nonetheless a cause of concern to the EU's cybersecurity especially in light of the growing solidarity and sympathy of EU citizens with pro-ISIS and other terrorist groups. This was also witnessed in the Tunisian Fallaga Team that launched an attack the UK's National Health Service in protest of the Syrian Civil War and the role of some EU countries. The attack involved defacing the NHS websites with photos from the Syrian civil war in protest of the plight of the citizens.

While the threats of cyber-terrorists and hacktivists persist in the EU region, Pâris (2021) observed that nations constitute more threats cybersecurity than terrorist groups even though they may always engage in open propaganda than nations. According to his findings, whereas hacktivists and cyber-terrorism is a growing trend and threat among the EU, more cyber-attacks have been recorded as originating from nations within and without the EU than from terrorist groups (Jayakumar, 2020). This has been attributed to the fact that while terrorist groups may possess daring and anti-government ideals and express the same on the internet, nation-states actually possess the cyber technologies and wherewithal to perform or undertake these attacks and more often than not they have engaged in these peace threatening cyber activities that has made cyber-peace difficult (Jayakumar, 2020). Although nations may not own up to these attacks, reports and investigations also show that attacks by private hackers and hacker groups could be in-

fluenced and induced by nations who hire the services and technologies of these black hackers for political purposes. Also nations rather than terrorist groups possess the funds and resources to easily purchase and deploy cyber-threatening technologies than most terrorist groups. While reports have indicated the desire and attempts of ISIS, AL-Qaeda and pro-terrorist individuals and groups to acquire cyber-technologies to pursue their anti-West ideals, they have not succeeded much in this endeavour.

Findings however indicate that these threats are continually present among the cyber and national security architecture in the EU (Jayakumar, 2020; Brady & Heinl, 2020; Giantas, 2019; Meer, 2015). As a result there are approaches and attempts to contain and control the internet space in the EU region by particularly pursing and spearheading innovative research and developments in the internet space to prevent unpleasant surprises from the numerous terrorist groups threatening peace and social order in the region (Brady & Heinl, 2020). While the cases of past and potential threats facing the EU as identified above have been noted to be recent developments and cause for concerns, Brady & Heinl (2020) in their study have made a distinction between old and recent cyber-threats. According to them, hacking which is pervasive threat in the EU region and beyond cannot be classified as a recent crime or threat as it has been a phenomenon recorded for over 20years. In their study, they relate that while some of these threats have become sophisticated over the years, they are not actually recent threats. As such, tackling and engaging them must identify the rate and scale of developments they have attained over the years to adequately tackle and address their current disposition in recent times. The major threats to the cybersecurity infrastructure of the EU and her member nations in their view is actually the level of comprehension and capacity of computer and internet users to identify and mitigate the ever growing sophisticated threats on the internet space.

Furthermore they reason that the vulnerability of the EU region to cyber threats and attacks is not necessarily a function of the pervasive threats of cybercriminal activities prevalent in the internet space. In their view, the opportunities presented by internet users to cybercriminals even where there is no active threat as a result of the gap in technological knowhow also presents a serious challenge and vulnerability to the EU's cybersecurity. This vulnerability extends beyond individual capacity to identify threats and securely utilise the internet to involve the capacity of organisations, institutions and national security agencies to ably engage the internet space while eliminating threats. Therefore cyber-threats in the EU region over the years according to this view have not

only been the malicious activities of hackers and anti-State actors but also the vulnerability presented by all categories of internet users ranging from individual to state actors. As in the case of the Estonian cyber-attack in 2007/2008, Brady & Heinl (2020) would thus reason that the inability of the Estonian government and cybersecurity infrastructure to identify secure the nation's cyber technology against the attacks is directly responsible for the success of the attacks against the state. This also resonates with Myers's (2020) and Pernik & Tuohy's (2013 in Giantas, 2019) view that far from being an issue of computer programmes and malicious hackers alone, cybersecurity also has a lot to do with the skilfulness and capability of the computer user to not only identify potential threats but prevent the same.

4.3.1. Summary of Findings

In summary, the findings from the study suggest a relative severity in the occurrence and possibility of cyber-attacks and threats among EU nations. European companies, businesses and government institutions are increasingly becoming targets of hackers and malicious cyber users hence there is a growing interest in the field and skills of cybersecurity in the EU. However findings also suggest majority of the cyber-threats facing the EU since the beginning of the century are more often than not, politically motivated. The cyber-attacks on Estonia, Georgia, Ukraine, and numerous others on the EU nations according to findings have maintained a pattern of political disputes and conflict. Indeed they have been extensions of political and ideological conflicts among EU countries hence political threats seem to arise more from European countries against their European neighbours. This is instructive because although other kinds of threats exist in the region, political cyber-threats and attacks over the years have shown to be very devastating in its occurrence due in part to the availability of State resources that may not be readily available to the individual user. On this premise therefore, the level of seriousness of cyber-threats and attacks on the EU may very well be reliant on the healthy political relations and interactions between the EU member countries. This is because contrary to the global anti-terrorist campaigns and fears of cyber-terrorism in the EU, findings indicate that cyber-terrorism have been relatively scarce in comparison with State-motivated cyber-attacks. Therefore while there is obvious need to improve cybersecurity and awareness to mitigate other kinds of cyber-attacks in the EU, there is need for improved diplomatic relations among nations within the region especially to

contain the excesses of aggressive nations like Russia which is notoriously linked with virtually every political cyber-attack in the region.

4.4. Strategies adopted by the EU to enhance Cyber-Peace and Cybersecurity in the EU

This section discusses the efforts and strategies adopted by the EU to mitigate and address the growing seriousness of cyber-threats and attacks against the cyber infrastructure of the EU and member countries. Findings from the study conducted are related below. Studies and scholars have expressed mixed views on the mitigation strategy of the EU in curbing cyber-threats and enhancing cybersecurity. While scholars like Jayakumar (2020) believe the EU and her member countries have been active in the fight against cyber-threats, others like Pâris (2021), Mortera-Martinez (2018) and Bendiek, Bossong & Schulze (2017) believe the EU and member countries have been rather slow and not efficient enough in action. However there is the consensus that there is a growing acknowledgement and response by EU member countries to the pervading threats. These responses have been basically in the form of policy actions, investment in cybersecurity, attempts at regional and global cyber-governance.

One of the earliest instruments and approaches to improving cybersecurity in the EU was the Council of Europe Convention on Cybercrime in 2001 also known as the Budapest Convention with the mandate to pursue a common criminal policy aimed at the protection of society against cybercrime especially by adopting appropriate legislation and fostering international cooperation (Brady & Heinl, 2020; Veale & Brown, 2020). Although this legal document which is regarded as the first EU policy approach to address cybercrimes and attacks against information systems was however brought into force in 2011 and have countries within and beyond the EU as parties (Brady & Heinl, 2020). The Convention outlines the following objectives as her goals;

i. Foster cooperation with the other State parties to this convention;
ii. Pursue a common criminal policy aimed at the protection of society against cybercrime, by adopting appropriate legislation;
iii. Foster international cooperation;
iv. Recognising the need for cooperation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

v. Effective fight against cybercrime by fostering increased, rapid and well-functioning international cooperation in criminal matters (Brady & Heinl, 2020).

Subsequent protocols, conventions and strategies on cybercrimes in the EU region have built on this foundation to promote and expand the mandate on cybersecurity among member-countries and beyond. In 2013, a Directive was issued by the EU to member States to the end of harmonising national laws and penalties for cybercrime by criminalising attacks against information systems such as identity theft or illegally accessing banking records and networks (Sterlini, Massacci, Kadenko, Fiebig, & Eeten, 2019). According to Mortera-Martinez (2018), this directive created a new category of cybercrimes in the EU and also boosted the cooperation between the Police and the judiciary in the various countries region as it outlined and determined which country's agency is responsible for certain lines of actions in the case of cross-border cybercrimes. The directive also mandated member countries to implement a penalty of up to 5years and above for cybercrimes with allowance for increasing this sentence in aggravating cases as in identity theft. All the EU countries except Denmark ratified this directive and have made it national laws. The idea according to findings is to promote an integrated and coordinated approach to tackling cybercrimes in the EU region to prevent legislative and bureaucratic gaps among the different countries. Also the European Police (EUROPOL) set up its Cybercrime Centre in 2013 which serves as a central hub for coordinating operations, sharing intelligence reports and supporting member States' operations and investigations on cybercrime (Giantas, 2019). One of the successes of the Europol's efforts was the investigation and dismantling of the online criminal network, 'Avalanche' which was notorious for attacking online banking systems worldwide. The Europol was also instrumental in the arrests of 193 persons involved in online air ticket fraud.

The EU Cybersecurity Strategy was however launched in 2013, years after the cyber-attacks on Estonia, Georgia and other EU members and neighbours. This strategy according to Sterlini et al (2019) was the first document to take into consideration the modern threats and vulnerabilities in the cyberspace of the region. The 2013 Cyber Strategy had five objectives and priorities within the EU; cyber resilience, drastically reducing cybercrime, developing cyber defence policies and capabilities, developing industrial and technological resources for cybersecurity and establishing a coherent international cyberspace policy for the EU to promote EU values among member-States

(Lukaševičiūtė, 2019). However as at the time of ratification in 2013, Mortera-Martinez (2018) observed that about 11 member-countries of the EU were yet to have neither an emergency computer response team nor a national cybersecurity strategy. Hence there were institutional and practical challenges at the national and regional level in the successful implementation of the EU Cybersecurity Strategy. The EU subsequently partnered with the private sector under the auspices of the European Cyber Security Organisation (ECSO) to enhance and cover for the lapses of member-States especially as statistics for the year indicated an all-time high for cyber-attacks in the year (Mortera-Martinez, 2018).

Findings also reveal that the EU has adopted a number of policies since the 2013 framework was established to tackle and combat cyber-insecurity. Some of these policies are the EU Cyber Defence Policy Framework in 2014 (which was updated in 2018), the 2015 European Agenda on Security, and the 2015 Digital Single Market Strategy, the 2016 NIS Directive and Global Strategy, and the 2016 EU Joint Framework on Countering Hybrid Threats. In 2017, the EU also presented the Cybersecurity Package under the Cyber Diplomacy Toolbox 2017 which was aimed at strengthening the mandate of the European Union Information and Security Agency (ENISA) which was established in 2004 to address concerns on information security (Lukaševičiūtė, 2019; Sterlini et al, 2019). The 2017 Cyber Security Package however aimed to make ENISA a permanent agency with a doubled budget amounting to €23million to help EU member-States, businesses and institutions in intelligence sharing and other mitigation efforts in the case of a cyber-attack (Mortera-Martinez, 2018). The EU Cybersecurity Strategy was also renewed in 2017, the EU Cyber Defence Policy Framework was updated in 2018 and in 2019 the EU Cybersecurity Act was passed which made gave ENISA the full mandate as a permanent agency notably for cybersecurity certification. In 2020, the New Cybersecurity Strategy was formulated and a decade-long policy for cybersecurity is envisaged from 2021 forward (European Commission, 2020).

ENISA was founded as a centre for expertise on cybersecurity according to Giantas (2019) with the aim of understanding the dynamics of cybersecurity culture. The Agency through her cyber experts thus provides useful step-by-step information and guidance to both public and private institutions within the EU on how to beef up cybersecurity and enhance cyber-governance by the EU. The Agency has also facilitated information and intelligence sharing between governments in the EU through active NIS field agents which works together to prevent cybercrimes and attacks through adequate cyber-

governance. ENISA thus in the view of Giantas (2019) has become somewhat of a cybersecurity knowledge and information broker for the EU and her member-States whose duty is limited to preventive technology and not operational responsibilities as the NATO and Europol even with the level of expertise and resources at her disposal. ENISA is therefore supportive in nature to other more active and operational policies and agencies in the cybersecurity field in the EU. The Directive on the Security of Network and Information Systems (NIS) is another legal document established by the EU to check cybersecurity and cyber-governance standards among member countries in the EU. It is basically a set of minimum standards for EU member-states to implement and achieve in their various efforts to enhance cyber resilience in their nations and in the EU at large. In the thoughts of Giantas (2019) this law can result in upscaling cyber capabilities, preparedness and effective risk management, enhance cooperation and exchange of information and good practices for cybersecurity among nations and businesses in the region.

The 2013 EU Cybersecurity Strategy according to scholars (Pâris, 2021; ECA, 2019; Giantas, 2019) is regarded as the chief policy on cybersecurity in the EU to which all other policies and legal frameworks either draw support or aims to support and strengthen. The EU Cybersecurity Strategy has five core objectives as previously stated above which are;

i. increasing cyber resilience;
ii. reducing cybercrime;
iii. developing cyber defence policies and capabilities;
iv. developing industrial and technological cybersecurity resources; and
v. establishing an international cyberspace policy aligned with core EU values.

According to Pâris (2021), the 2013 EU Cybersecurity Strategy framework linked with the Budapest Convention by using the terms ‘cybercrimes’ and ‘cybersecurity’ interchangeably so that actions and provisions in the Convention relating to cybercrime could be adopted in the Cybersecurity Strategy. As Backman (2019) and Kovács (2018) observes in their findings, the Cybersecurity Strategy was an important achievement and step towards cybersecurity at the EU level at the time as there was no prior comprehensive regional document for the purpose. Findings also reveal that though the 2013 Strategy was not binding, it however provided a framework for member-States of the

EU to work towards. As such there was a regional goal that EU countries could aim to achieve in the attempt to enhance cyber-governance and build cybersecurity. However the document was non-binding on the member-States hence there were lapses in the implementation process which affected the actualisation of the goals of the Strategy. The Strategy explicitly stated that for it to be effective among member States there was need for legislative processes across the states to properly implement the recommendations of the Strategy.

The document also outlined awareness for cyber users on the risks and threats available on the internet space as one of the approaches towards achieving cyber resilience hence Member States were advised to adopt the various cyber awareness campaigns and education to promote awareness. This objective here was to encourage cyber resilience through broad cyber awareness and education campaign that involved orienting all sectors of society by partnering with key stakeholders in the EU such as ENISA, Europol, Eurojust and the European Cybercrime Centre (EC3) (Kovács, 2018). The idea however as stated by Giantas (2019) was to harmonise the instruments and strategies for combating cybercrimes and cyber-threats at local, nation and regional levels within the EU. Thus the 2013 Cybersecurity Strategy was updated in 2017 to further strengthen collaboration and implementation among member-States so as to enable adequate regional cyber-governance and cybersecurity within the EU.

Part of the provisions of the 2013 Strategy was the encouragement of technological innovations through investment in research and development by member countries and Commission. Through the Research and Development funding for technological resources and innovations, foundations were laid for the realisation of the “Horizon 2020” programme of the EU which is focused on innovative research in cybersecurity. Also the 2013 Strategy laid the foundations for the creation of a single market for existing and emerging products to enhance manufacturers’ adherence to the NIS Directive (Kovács, 2018). Furthermore the Strategy also called for the formation and adoption of a foreign policy by the EU and EU member States that enhanced capacity building, maintenance and adherence to cybersecurity strategies/initiatives and ensured cyber-governance in other states outside the EU. This move was necessary according to the 2013 Strategy document to regulate and enhance cyber-governance beyond the EU and her member states to other States and regions where the EU has strategic partnership especially in third world countries where capacity for such cyber initiatives was grossly lacking and inadequate (Bendiek & Maat, 2019). The policy development by the EU

from 2013 till data have therefore being in furtherance of the ideals outlined by the 2013 Cybersecurity Strategy.

Pursuant to the 2013 Strategy, the 2014 EU Cyber Defence Policy Framework updated in 2018 was enacted in response to the cybersecurity challenges that resulted from implementation (Sterlini et al, 2019). The 2014 Cyber Defence policy document was aimed at conflict prevention and greater cooperation among stakeholders in the cyberspace in furtherance of cybersecurity governance in the EU region. Some of the other areas listed as the areas of priorities in the 2014 policy document include, development of cyber defence capabilities, training and exercises, research and technology, civil-military cooperation and international cooperation. This was in response to the growing need for collaboration and information sharing between the various national defence agencies in the cyberspace. As Lété and Pernik (2017) puts it, there was challenge arising from the need of the specific roles and responsibilities of the various EU security stakeholders especially the military intelligence agencies in matters relating to operational and intelligence. The 2014 framework therefore outlined the roles and mandates of the various EU agencies involved in the partnership. The 2018 updated Cyber Defence Policy Framework however outlines six priority areas;

i. development of cyber defence capabilities;
ii. protection of the EU Common Security and Defence Policy communications network;
iii. training and exercises
iv. research and technology;
v. civil-military cooperation; and
vi. international cooperation (Council of the European Union, 2018)

The 2015 European Agenda on Security in the same vein focuses on a coordinated approach at the regional level in enhancing cybersecurity by implementing existing policies and adjusting existing legislations. The 2015 Digital Single Market Strategy is another policy initiative by the European Union which focuses on incorporating the private sector in the war against cybercrimes and cyber-attacks. The programme was slated to run for five years between 2015 and 2020 with the aim of overcoming fragmentation of the European cybersecurity market by innovation, researches and trust-building among between member-States and industrial actors. The idea of this policy according

to Cappelletti (2021) is to invest in novel technologies and small SMEs that are necessary for combating cybercrimes across Europe. As the 2020 report of the Council of Europe observes, this became imperative as a result of the failure of solely national strategies to adequately tackle the increasing rate of cyber-attacks and threats against businesses in the EU. This policy led to the formation of a partnership between the EU and the European Cybersecurity Organisation (ECSO) comprising over 200 stakeholders including SMEs and start-ups, large cybersecurity companies, universities, research centres, end-users, operators, clusters, and public authorities (Kertysova et al, 2018). The EU thus committed €450million to the partnership over the period of 5years while the partnering Cybersecurity market players were outlined to invest three times the amount (Kertysova et al, 2018).

The 2016 Directive on Security of Network and Information Systems (NIS Directive) further consolidated efforts on improving cybersecurity in the EU. Passed by the European Parliament in July, 2016, the directive was aimed at improving the national and regional capacities of member-countries to address cyber-threats and enhance cyber-governance (Kertysova et al, 2018). Cross-border information sharing and cooperation among EU countries was also outlined by this policy as an important strategy for enhancing cyber-governance in the region. The Directive amongst other aims therefore sought the development and improvement of the national cybersecurity frameworks and agencies by stipulating a benchmark for EU member-States to meet in order to attain and maintain cyber-resilience (Brady & Heinl, 2020). Member States were also required to have a national cybersecurity strategy, a national cybersecurity authority and a national cybersecurity response team in place in times of emergency. The Directive also mandated private companies with ties to EU member States to adopt serious security measures to protect cyber infrastructures and data and to report incidents of cyber breach or attacks to the appropriate authority. The overall aim is to improve cybersecurity consciousness in both private and public institutions within the EU while also promoting cordial relations and interactions among stakeholders necessary for enhancing cyber-governance and cybersecurity. According to Brady & Heinl (2020), the Directive is lauded by the 2017 EU Cyber Strategy as a progressive step towards improving the region's criminal law response to cybercrimes. Since her implementation, it is noted that there is considerable progress in criminalising cyber-attacks across member-states at a level that necessitates and facilitate cross-border cooperation among law enforcement agencies of various States within the EU.

However, more needs were identified in the collaborative efforts of the EU as the existing policies were limited in addressing the traffic of attacks arising from nation/s outside the EU. This and several challenges identified in the existing policies led to the 2017 Cyber Diplomacy Toolbox (CDT) in June 2017, which focused diplomatic relations and policies with nations beyond the EU with records of aggressive cyber-attacks against EU nations. As Sterlini et al (2019) puts it, the idea of the policy framework was to influence the behaviour of aggressors and potential aggressors in the long run. In other words, the Cyber Diplomacy framework was an attempt at cyber-governance that focused on managing and controlling the actions of cyber aggressors as well as potential cyber aggressors. Part of the Cyber Diplomacy Mandate is the coordination of response directed to malicious cyber activities directed at EU member states including sanctions for perpetrators and accomplices (Lațici, 2019).

To enhance international diplomacy that fosters and helps this coordinated response to cyber-attacks from other nations outside the EU, the Commission has entered into partnerships and collaborations with several international committees and bodies including the Council of Europe (CoE), the North Atlantic Treaty Organisation (NATO), the Organisation for Economic Cooperation and Development (OECD), Organisation for Security and Cooperation in Europe (OSCE), and the United Nations (Kertysova et al, 2018). Strategic partnerships have also been established with nations as Brazil, China, India, Japan, Republic of Korea and the United States of America. The Commission also commissioned the G7 Cyber Expert Group to address the increasing sophistication of cyber-attacks and threats in the financial sector and develop strategic techniques for improving the cybersecurity initiatives of the region's financial sector. The assignment was to conduct a non-binding assessment of the fundamental components of cybersecurity in the EU's financial sector to reveal her vulnerabilities, threat levels and cybersecurity initiative for the financial sector.

Also the New Cybersecurity Regulatory Package was initiated in 2017 to further strengthen the ENISA to much more than before assist nations and businesses deal with cyber threats and attacks (ECA, 2019). According to Mortera-Martinez (2018), amongst other functions given to ENISA under the 2017 repackaging framework, the agency had the task of implementing the NIS Directive and the cybersecurity certification framework. The EU-wide Cybersecurity certification scheme under this framework is another initiative under this framework that aims at increasing the security of digital products and services, improve cross-border trade and reduce market fragmentation. This certifi-

cation scheme applied to essential services sectors while a joint Commission-Industry was also designed to promote a 'duty of care' principle for reducing software and product vulnerabilities.

The 2017 Package also introduces new target sectors that the NIS Directive applies to i.e. it expands the mandate of the existing NIS Directive to a full mandate by including new sectors as public administration, the postal sector, food sector, chemical and nuclear sector, environmental sector, and civil protection within the EU based on the prerogative of member States (Lațici, 2019). This is in combination with the large-scale cybersecurity incidents and key strategic sectors the Directive already applies to. Additional steps and developments initiated by the 2017 Package include the development of a Blueprint on how best to respond to large-scale cyber-attacks (so that in the event of cross-border large-scale attack or cyber incident in any member-State, there is a system of well-rehearsed response through swift communication and coordination to address such concerns among member States), the establishment of a European Cybersecurity Research and Competence Centre along with a network of similar centres across member-States, more effective criminal law response to cybercrimes and the enhancement of international collaboration and cooperation in cybersecurity initiatives (Griffith, 2018).

The EU Cybersecurity Act was adopted in 2019 with laudable improvements on the Cybersecurity Certification Scheme. Amongst the many provisions of the Act was the empowerment of the ENISA as a permanent agency of the EU to issue cybersecurity certifications across the European single market (EU, 2019). This scheme helped to consolidate the European single market by resolving the problems related to fragmentation of certification schemes in the EU. According to Angelika Niebler, a member of the European Parliament and Rapporteur of the Cybersecurity Act, the EU Parliament had two specific focuses for adopting the Cybersecurity Act (Eurosmart, n.d). The first was to address the growing attacks on the critical infrastructures of the EU and her member countries which consist of all aspects of daily lives as electricity, water, health, communication etc. The second focus of the Cybersecurity Act was the growing number of devices to access the internet and the distrust of users over privacy and safety of their devices. To undertake these tasks, ENISA is given a broader range of activities and assignments to fulfil the mandate of the Cybersecurity Act. Some of the tasks stipulated under the new permanent mandate of ENISA include,

i. development and implementation of a regional cybersecurity law. ENISA is tasked among other duties with providing independent analysis and preparatory work on the development of cybersecurity laws and also assisting member nations implement the laws to facilitate best practices between competent authorities.
ii. capacity building initiatives for member States by organising regional cybersecurity exercises and assisting member countries with expertise and knowledge on cybersecurity initiatives.
iii. marketing cybersecurity certifications and standardisation by supporting and promoting the development of region policies on ICT products and services.
iv. providing information and knowledge. This function of the ENISA includes serving as a knowledge bank to the EU member countries such that specific knowledge and information on cybersecurity incidents are provided to members as at when needed.
v. awareness raising and education involves raising awareness and education on cybersecurity risks for the EU by engaging region-wide awareness programmes and assisting member countries in their cybersecurity awareness efforts.
vi. research and innovation for the EU by engaging in innovative researches and assisting member States with research needs and research priority areas to direct research innovations in the field of cybersecurity.
vii. facilitate international cooperation between EU member countries and third countries by providing the necessary guidance and recommendations within international frameworks (EU, 2019; Eurosmart, n.d).

In 2020, a decade programme on cybersecurity was also launched by the European Union to further check the rate of cyber-attacks and build operational capacity for preventing and deterring such attacks (European Commission, 2020). The EU Cybersecurity Strategy for the Digital Decade was launched as the primary policy for the year 2020, however other frameworks and documents were formulated to further drive the fight against cyber-attacks in the region. Some of these documents are the 2020 EU Security Union Strategy and the Screening of Digital Investment, the Digital Single Market Strategy, the EU Commission Economic Recovery Plan, and the Security Union Strategy 2020-2025 (Bendiek & Kettemann, 2021). The 2020 Cybersecurity Strategy resulted in the launching of the 'Joint Cyber Unit' that was tasked with strengthening the IT capacities in cybersecurity defence communities and law enforcement agencies in the region. This is also to strengthen cooperation ties among member countries in the region

especially between cyber defence agencies and the civilian/diplomatic community to enhance quicker and timely response to cross-border cyber-attacks (Bendiek & Kettemann, 2021). Furthermore the new strategy also focuses on partnership and supports like the European Defence Agency framework. Also the network of Security Operations Centres was established in 2020 serve as a cooperation platform between civilian and military authorities as well as EU commission members States in cybersecurity. Laws were also reviewed to address issues as growing threats in the areas of health, hospitals, utilities, and transport which is not adequately captured in the 2016 EU Network and Information Security Directive (NIS Directive) (Bendiek & Kettemann, 2021).

The 2020 Cybersecurity covers three main areas of interest, which are resilience, technological sovereignty and leadership, build operational capacity to prevent, deter and respond to cyber threats and lastly, advance a global and open cyberspace through increased cooperation. The first area outlined a set of measures to be undertaken which resulted in making internet devices within the EU more secured, resilient to attacks and amenable to mitigation of vulnerabilities. Meanwhile, the 2020 framework also aimed to make the EU attain a leadership position in the digital technologies and digital supply chain through her 'Cyber Defence Shield' project and funding in research and innovations (Warman, 2021; EC, 2020). Secondly the new cybersecurity framework also aimed to build the operational capacity of member countries through the Joint Cyber Unit initiative which a physical and virtual platform for cybersecurity communities within the EU such that members could draw from the operational capacity and capabilities made available at the regional level to address cyber threats and insecurity. Also building operational capacity also relates to adhering to technological guidelines within the EU not only build community capacity but also to resolve disputes when needed (Warman, 2021). Lastly, the 2020 framework aimed to achieve her technological aims in the EU through greater cooperation within the region and between member countries and third parties so as to perform the cybersecurity leadership role in global cybersecurity efforts. The measures of this framework were scheduled for implementation in the year 2021 as the new framework was passed in December 2020.

4.4.1. Summary of Findings

In summary, findings show that the EU has maintained a pattern of evaluation and re-evaluation of her cybersecurity policies since the year 2013 to ensure that lapses and loopholes in existing frameworks are addressed and cyber resilience is achieved in the EU. The findings also show that the EU has been particularly poised towards improving regional capacity for cyber resilience and governance by providing the necessary tools and resources to member countries needed to address the persistently growing threats of cyber insecurity. However, from the findings, indicators point to the fact that the implementation of these policies have faced not yielded the desired results as envisaged by the Commission hence cybersecurity policy aims and objectives are repeated year after year. This is particularly so in the areas of cooperation and capacity building. The policy frameworks from the year of implementation of the Budapest convention in 2011 to the recent New Cybersecurity Framework in 2020, there have been consistent mention and measures to improve cooperation among member countries. Even though the aims are targeted at international cooperation, there is considerable focus of initiatives to improve regional cooperation and information exchange. Hence it portrays the idea of lack of necessary regional cooperation needed to jointly combat cyber threats and attacks even though the member countries are appreciating the need for cybersecurity. This trend tends to be more visible among the military and law enforcement agencies especially in the areas of intelligence and information sharing. Therefore the proliferation of regional agencies to address cooperation and build regional cyber resilience and capacity of member nations to develop and implement the measures needed to enhance cyber governance. In all however, there is considerable policy evidence that shows the dedication to cybersecurity in the EU even though challenges exist that hinder the successful implementation of these frameworks.

4.5. Challenges of the Cybersecurity Strategies of the EU

This section discusses the challenges of the cybersecurity strategies outlined by scholars especially of the 2013 EU Cyber Security Strategy updated in 2017. This particular framework is chosen because it represents the beginning of active and assertive efforts by the EU to address the challenge of cyber threats and attacks targeted at her member countries. Also as reasoned by scholars, it represents the specific landmark in the fight against cyber threats and beginning of cyber-governance initiatives in the EU.

As such every other policy framework from the year 2014 has been an attempt to address the loopholes of the 2013 Cyber Security Strategy hence the need to outline the challenges of this and other policy documents to discover the loopholes and challenges that has resulted in the increase of cybercrimes and attacks over the years. Several challenges have been identified by scholars as challenges mitigating the successful implementation of the EU Cyber Security Strategy. These are discussed below.

According to findings from the study, several challenges are identified with the 2013 Cyber Security Strategy and other frameworks in furtherance of cybersecurity and cyber-governance in the EU. In summary the challenges identified from the study bothers on the following;

i. Evaluation and accountability
ii. Uneven transposition of EU laws in comparison with technological innovations
iii. Funding and spending
iv. Clear overview of EU budget spending
v. Governance and standards
vi. Skills and awareness
vii. Information exchange and coordination
viii. Detection and response
ix. Protecting critical infrastructure and societal functions

These points are discussed in details below.

Lack of Evaluation and Accountability

The first concern on the evaluation and accountability of the Cyber Security Strategy is the lack of measurable targets and objectives. According to the 2019 report by the European Court of Auditors, while the Strategy outlined objectives and targets for the regional commission and member States, these objectives were not measurable but only expressed a vision and not a measurable target hence there is the challenge of measuring the progress and otherwise of the Strategy (ECA, 2019). Also the objectives were broadly formulated with no specific targets which make specific actions aimed at measurement and evaluation of the objectives difficult (Yan, 2019; Mueller, 2018). Furthermore, findings from the study showed that although the 2018 cyber defence policy framework outlines minimum cyber defence objectives and how these are measured

overtime, the scope of measurement and evaluation is limited to cyber defence only (Brady & Heinl, 2020; ECA, 2019). This creates a loophole in the entire EU cyber resilience as measurable objectives have not been set. Findings further showed that measurement and evaluation criteria for assessing impacts of the implementation of the policies are also lacking in the Cyber Security Strategy (Bendiek & Kettemann 2021; EU, 2020; Bendiek et al, 2017). This challenge for the EU according to the ECA report is also due to the unavailability of rigorous evaluation culture for cybersecurity issues generally (Giantas, 2019; ECA, 2019; Kertysova et al, 2018). This lack of monitoring and measurement culture for cybersecurity awareness and resilience therefore plays a major role in limiting the mandate of ENISA (ECA, 2019; Eurosmart, n.d).

The issue of evaluation and accountability can also be linked with the unavailability of enough evidence-based policies and the statistical or measurable indicators to help monitor trends and developments in the cybersecurity sector (Yan, 2019; Kertysova et al, 2018; Chang & Grabosky, 2017). Also member States rarely collect such information at the national levels to aid comparative evaluation so that information and evidence-based data on the economics of cybersecurity, the impacts of cyber-failure and cybercrime, macro-statistics on cyber trends and challenges and the best solutions to these threats are lacking (Giantas, 2019; ECA, 2019). Findings also show that in light of this dearth of well-defined indicators, quantitative analysis and assessment of the Strategy has been impossible except qualitative data. Progress reports are reported thus to only make mention of the milestone achieved or the measure implemented and not on the measurement of the result of the initiative to cybersecurity in the region (Pâris, 2021; Giantas, 2019; Bendiek et al, 2017). Findings further showed that member States hardly performed auditing evaluations and the few that did, did not make such information public on the grounds of national security. The report further identified that the areas where such auditing were focused on were “information governance; protection of critical infrastructure; information exchange and coordination between key stakeholders; incident preparedness, notification and response” (ECA, 2019:18). Other areas that were hardly audited to measure the rate of success of the Strategy are awareness raising measures and digital skills gap. As such evaluation and accountability of the Strategy to adequately monitor its progress were among the key challenges identified from the study.

Uneven Transposition of EU Laws

Another challenge identified from the study was the ever increasing rate of digital technologies and the threats facing digital users so that the EU laws are outpaced in her implementation efforts to govern the cyber space through legislations and policies (Barmpaliou, 2020; Nigel & Nathan, 2020; ECA, 2019; EU, 2017). While the laws and policies like the Cyber Security Strategy are rigid and static for instance in handling cyber related threats, the realities and dynamics of cyber threats are flexible and rapidly changing hence these laws are largely inadequate as they are not framed to anticipate and shape the future (Munk, 2015; Bodeau et al, 2010). Legislative gaps are continually being identified in the framework that hampers the achievement of the objectives of the overall policy leading to inefficiencies and fragmentation of policies and legislative frameworks to make-up for identified lapses (Schlehahn, 2020). For instance, the ECA study of the Strategy found that gaps exist in the balance of responsibilities between users and providers of digital products as well as certain aspects left unaddressed by the NIS Directive (ECA, 2019). Although the Cybersecurity Act attempted to address these lapses, findings reveal that a clearly defined industrial policy and a common approach to cyber-espionage are still noticeably absent.

Some of the noticeable gaps in the existing legislations and frameworks according to the study are that at the time the Digital Single Market policy was initiated, the Consumer Sales did not cover cybersecurity although the directives on digital content addressed the lapse (Lukaševičiūtė, 2019; Sterlini et al, 2019). Also under the Digital Single Market, there are limited and diverse legal frameworks for duties of care in EU member countries so that there were issues of legal uncertainties and difficulty in enforcing legal remedies in the EU (Lukaševičiūtė, 2019; ECA, 2019; Sterlini et al, 2019). Another such gap had to do with Strengthening network information and security while member countries were free to include sectors that were omitted from the NIS Directive (Markopoulou et al, 2020; Kovács, 2018). This provided a lapse as member countries had sectors like the accommodation sector that were not included in the initiative which could be exploited for crimes as human and drug trafficking and illegal migration (ECA, 2019). Furthermore, in the areas of Fighting Cybercrimes, many member States did not review their national policies to reflect the aims and peculiarities of the EU for instance some nations did not include a definition of e-evidence in their legislations which is a necessary item in the discourse of combating cybercrimes (Veale & Brown, 2020). Also the difference in the application and implementation of laws among mem-

ber countries has also hampered policy objectives. For instance in the aftermath of the data retention judgement by the Court of Justice of the European Justice, different application of laws and impeded the enforcement of the judgement so that vital investigative leads were lost and prosecution of online criminals was impaired (ECA, 2019).

Another lapse of the Cyber Security framework is the fact that the application of some aspects of the legislation is on voluntary basis both for States and private organisations (Backman, 2019; Kovács, 2018). This is so with the application of certification for ICT products and services within the region which is on a voluntary basis which leaves huge gap for lapses and uneven cyber resilience and defence (Giantas, 2019; Kertysova et al, 2018). Also the evaluation of national strategies on the security of network and information systems and the effectiveness of CSIRTs is on a voluntary basis thus watering down the capacity and effectiveness of the cooperation of EU countries to enforce necessary cyber policies (ECA, 2019). This becomes problematic in the light of the fact that the EU and her cybersecurity agencies are mandated to work together with member nations to improve capacities and engender trust for the regional cooperation while at the same time member States are within their rights to withhold sensitive information in their national interest when such data may be useful to the regional partnership. This is possible because the legislations are mostly voluntary and nations are to participate or apply them on a voluntary basis. This creates a fundamental gap to the success of the policy frameworks which are intended to improve cybersecurity and resilience as well as protect cyber infrastructures within the EU region.

A dimension of the inconsistent transposition of legislations among EU members is the effect on operational coherence in areas where member countries have differing interpretation of a particular legislation (Muhammad, 2017; Verhulst et al, 2016; Shackelford & Kastelic, 2015). For instance, the European Parliament has raised concerns over some EU-based companies exporting technologies and services that can be used for cyber-surveillance and human rights violations through censorship or violations on the basis of dual-use exports controls (ECA, 2019). While some member countries may interpret this as engaging necessary controls for regional security, others may view it from a more nationalistic perspective and hence engage in business deals that may adversely regional cybersecurity (Thomas et al, 2018; Craigen, Diakun-Thibault & Purse, 2014). There is also the concern of balancing personal data protection and applying regional security initiatives. The GDPR for instance is one of the legislations that seek to protect and regulate access to personal and confidential data of EU citizens (Giantas, 2019;

ECA, 2019). Therefore reconciling these differences through legislations to avoid clashes between fundamental values and regional frameworks remains a gap in the Cyber Security frameworks of the EU. This lack of appropriate demarcation and distinction in application of legislations and policies may engender conflict. The findings from teh study also indicated that efforts at enhancing harmonisation and cooperation of member States must extend beyond legislations as those alone may not guarantee the needed relationship to foster cyber resilience (ECA, 2019).

Funding and Spending

One of the major issues identified by reports and scholars as impeding the successful implementation of the cyber frameworks for the region has to do with financial budgets for implementing the various legislations and frameworks (ECA, 2019; Harjanne et al, 2018; Craig & Valeriano, 2016). According to reports by the ECA, the spending on cybersecurity by the EU and in EU countries have been relatively low compared to the United States of America as well as in comparison with the desired goal of the region to enhance and build cyber resilience (Myers, 2020). Although there are no concrete figures, findings suggest that the EU spend between €1billion and €2billion per year on cybersecurity while member countries even spend lower than that as investments on cybersecurity (Giantas, 2019; ECA, 2019; Mortera-Martinez, 2018). However these figures according to reports are only about one-tenth or less of the US's annual budget on cybersecurity (Myers, 2020; Barmpaliou, 2020; Inter-American Development Bank, 2020). The fact however that there are no official documents and statistics to compare regional and national spendings also present a challenge to the funding and spending prospects of the region's cyber infrastructure as there are no ways to reveal funding gaps that should be addressed by either parties (ECA, 2019). This is especially so because some members of the EU are economically unable to fund both national and regional cybersecurity frameworks (Inversini, 2020). However the statistics to reflect the gaps in the funding and spendings of nations within the region are largely lacking.

The source of funds for the implementation of these initiatives has also been identified as a challenge especially from the private enterprises (Jayakumar, 2020; Inversini, 2020; Giantas, 2019; ECA, 2019; Mortera-Martinez, 2018). According to findings, scaling up investments in cyber initiatives by public and private firms in the EU remains a challenge due to the fact that public capital is often unavailable for growth and expansion phases of cybersecurity firms (ECA, 2019; Kertysova et al, 2018). While start-up

funds and investments initiatives may be available in the EU, there are numerous red tapes and bureaucracies that discourage members from accessing such funds (ECA, 2019). As such the growth and development of cybersecurity firms in the EU are handicapped and they perform less than their counterparts in the international scene as the average amount of funds they raise is significantly lower than their counterparts (Pâris, 2021; Myers, 2020). Therefore the challenge of adequately funding cybersecurity start-ups in the EU to considerable stages is important for the EU to achieve her cyber objectives. There is also the challenge of a clear spending budget of cybersecurity funds by the EU to adequately match spendings with priority goals. According to findings by the ECA study, spendings for cybersecurity initiatives in the EU come from the general budget of the EU and co-funding by members. This complicates the spendings and budget of the regional body as several funding bodies with their peculiar goals, rules and timetables affect the efficiency and disbursement of funds for regional cybersecurity initiatives.

Data for spending and operational costs of the several agencies operating within the field of cybersecurity in the EU has also posed relative challenge to the successful implementation of the regional frameworks and Strategy. This arises from the fact that there are no explicit framing of required budgets and spending to evaluate the impacts of such spendings on cybersecurity within the region. For instance, between 2013 and 2018, €13million was budgeted for member States to apply and to help implement the NIS Directive's requirements (Giantas, 2019; Demertzis & Wolff, 2019; ECA, 2019). In contrast however, there have not been any initiatives to study and determine the exact financial needs of the CSIRTs network and Cooperation Group to have an effect (ECA, 2019). Similarly while several budgets and financial resources have been dedicated to cover operational costs of cybersecurity agencies in the region and tackle cybercrimes, there are hardly any information on the exact figures and statistics of the spendings and impacts of these spendings in the public domain.

Resourcing the EU's Agencies

Allocating financial and human resources for the various EU cybersecurity agencies to meet with the operational and policy demands and objectives of regional frameworks has posed a challenge to successful implementation of the legislative and policy framework (Giantas, 2019; EU, 2017; Wilson & Laidlaw, 2017; EU, 2013). The request of cybersecurity agencies for adequate funding and resourcing to meet with rising demands

are not fully satisfied thus handicapping timely resources and attainment of objectives. This factor was observed to have hindered ENISA from achieving her full objectives in 2017 so that additional resources were proposed for the 2017 package to cover up the lapses (EU, 2017; ECA, 2019). The supply of experts and ICT capabilities have also not met with the required demands due to the cost burden attached in some regional initiatives (Schlehahn, 2020). For instance, the Europol's Joint Cybercrime Action Taskforce (JCAT) initiative is staffed by member-State and third countries experts to support intelligence-led investigations while the costs are largely borne by the sending State thus discouraging the deployment of larger number of skilled experts (ECA, 2019). In some other cases, the inability to procure necessary staff and labour necessitated the investment in contract staff and outsourcing of labour (ECA, 2019; Kertysova et al, 2018). Findings indicate that many CERT-EU and ENISA staff are contract agents with the result that much of ENISA's works between the years 2014 and 2016 were outsourced (ECA, 2019). Also other initiatives for retaining labour such as attracting and retaining talents stem from the agency's inability to compete with the private sector's salary structure or poor career progression prospects.

This feature is particularly vulnerable and dangerous to the EU's cybersecurity framework as loopholes are created by the lack of adequately qualified labour to handle the numerous tasks and labour associated with online data as well as necessary for mitigating the threats of cyber-attacks. As findings also indicate, the lack of capable technologies and tools needed to secure and successfully integrate and interconnect threat data cannot help to intercept and share timely information about such threats to member nations in cases of attacks thus presenting a fundamental vulnerability to cyber-threats and attacks. With delay in dissemination of such vital intelligence, the legislations and frameworks cannot translate to any useful piece of information.

Governance and Standards of EU Member countries

There is also the challenge of strengthening governance and maintaining standards in the policy frameworks. Governance structures for cybersecurity among member States and within the EU assume different structures such that cooperation between the various bodies regulating cybersecurity initiatives across the borders becomes difficult (EU, 2020; Craig & Valeriano, 2018). According to findings, the responsibility for addressing cybersecurity issues between and within member countries in the EU are split into entities so that there are several governance structures for various different levels of responsibilities (Giantas, 2019; ECA, 2019; Shackelford, 2017; Eurosmart, n.d). The im-

plication of this is that series of cooperation and collaboration are required to respond to cyber threats at the national and regional levels (ECA, 2019). The problem however is that these governance structures adopt different models of engaging cyber-governance, as such collaborative and cooperative efforts in times of attacks and threats that require rapid response may be hindered by the differences and obstructions of cyber-governance at the different levels. This is particularly likely because the structure of governance in public authorities among member States in the EU have been noted to be considerably weak in risk managements thus projecting high possibility of vulnerability (Brady & Heinl, 2020; Giantas, 2019). Survey findings indicate in this regard that in the private sector, nearly 9 out of 10 organisations report that cybersecurity functions does not fully meet their needs nor does cybersecurity officials deeply involved in board decisions (ECA, 2019). As such cybersecurity governance still assumes a weak structure across the private and public sectors.

Furthermore, findings relate the fact that EU's company law directives relate no specific requirements on the disclosure of cyber risks like the Securities and Exchange Commission in the United States (Myers, 2020; Giantas, 2019). Although the Joint Committee of the European Supervisory Authorities (ESAs) issued warnings on the increasing rate of cybercrimes and encouraged financial institutions to improve fragile IT systems and to explore internal risks to information security, connectivity and outsourcing, the lack of proper cybersecurity governance framework in the EU hinders the implementation of such directives (ECA, 2019). For instance, SMEs in EU according to the findings from the ECA survey lack the necessary guidelines to apply the information security and piracy requirements to mitigate technological risks. The lack of a coherent cybersecurity governance framework in the international community also presents a challenge that can be advantageous to the EU community by setting up a cyber-governance structure that best reflects the values and interests of the EU. Even though the EU has made attempts to strengthen her agenda on cyberspace governance by formalising partnerships with six cyber partners to establish regular policy dialogues for the purpose of building trust and cooperation in key areas, findings still suggest that the EU is yet to be considered a major actor in cybersecurity even though it has increased its profile (Pâris, 2021; World Bank, 2019; Shackelford, 2017).

Standard approach for classifying and mapping risk assessments to harmonise response mechanism to threats are also lacking in the frameworks and policies (Kertysova et al, 2018). Findings indicate that there are no similar or standard assessments of

threats and attacks among member countries so that a coherent EU-wide approach to addressing cybersecurity issues is impossible (Evan et al, 2017; Jeffray, 2014). As such no single or standard measures are used by member countries to address similar threats or attacks which pose a problem to the EU-wide cybersecurity framework (ECA, 2019). This is escalated by the reluctance of nations and national agencies to share necessary information or under-report incidents of attacks (Giantas, 2019; Mortera-Martinez, 2018). Instead findings indicate that EU countries tend to rely on other threat assessment standards at the risk of giving inadequate attention to other primary threats (ECA, 2019). Thus cybersecurity frameworks face the challenge of divergent views and standards of mapping and assessing threats within the region. Although the Hybrid Fusion Cell of the EEAS was established to improve situational awareness and support decision-making through analysis sharing, the ECA report however underscores the need to broaden her expertise in cybersecurity.

Another challenge on the maintenance and sustenance of standards among EU countries on cybersecurity has to do with incentives. According to findings, there are too few economic and legal incentives to notify and share information about incidents (Giantas, 2019; ECA, 2019; Mortera-Martinez, 2018). In an attempt to avoid the reputational damage such reports and information may cause to an organisation, they tend to withhold or underreport incident and cases of attacks. In cases of direct attacks, organisations may decide to pay off attackers rather than access or engage any of the regional response mechanism to save her reputation and clients. Therefore strict maintenance of standard and governance structure in the cybersecurity framework of the EU region remains a challenge that works to hinder the successful attainment of a cyber-attack resilient territory due to the numerous openings and loopholes presented by lack of a strong governance and standard structure for the cyber initiatives adopted in the region (ECA, 2019). These loopholes according to findings do more to strengthen perpetrators of cyber-attacks in their attempts to penetrate the cyber defensive infrastructure of the EU than it helps the economic and public reputation of organisations and companies who intentionally discard regional mechanisms in response tactics.

Cyber Skills and Awareness of Citizens

The challenge of skills and awareness bothers on the fact that defending cyber infrastructures or else raising the necessary skills and awareness required to build a cyber-literate population is also the skills required to attack cyber infrastructures (Kremer et

al, 2019; Stallings, 2019). As such there is the challenge of improving the standards, awareness and skill set of young persons to make them resilient to cyber-attacks while also considering the possibility of this young population engaging in cyber-attacks and threats (Carlton and Levy, 2018). This is fast becoming an issue of concern to the cyber skills and awareness policy in light of the crime-as-a-service model that seeks to get more internet literate persons into criminal tendencies online by lowering or reducing the barriers of entry to the criminal market such that individuals without technical knowledge to build technical software programmes can rent botnets, exploit kits and ransomware packages to perpetrate attacks (ECA, 2019). This possibility and the inability to adequately regulate the activities of these cyber-criminal elements present a challenge to the EU-wide cybersecurity structure.

The above phenomenon is compounded by the fact that there is a global shortfall in the availability of skilled computer or cybersecurity skilled labour. According to reports by the ECA, the workforce gap has widened by 20% since 2015 hence there is a growing demand on the limited labour while efforts are geared towards enhancing and increasing this number (ECA, 2019). However efforts at raising and balancing the population of skilled cybersecurity labour are hampered by the fact that cyber-related subjects are under-represented in non-technical programmes in universities. Furthermore for the successful implementation of the cyber initiatives in the EU region, there is need for cyber literate workforce as well as a workforce with the necessary skillset among the various national and regional agencies and institutions of cybersecurity. However findings show that there are currently no EU-wide standards for training and awareness on cybersecurity and cyber-resilience curricula (Costigan and Hennessy, 2016). As such although cyber education and awareness is needed among law enforcement, civil servants, judiciary officials, armed forces and educators, there are no EU standards on cyber education to help educate this population of people so as to build cyber resilience. Rather these classes of people are schooled in varying aspects of cybersecurity with little or no emphasis on the security of EU cyber infrastructure which is the basis for such education and awareness in the first place (Morgan & Gordijn, 2020).

And as report findings indicate, without these necessary custom-structured cyber education and awareness skills, institutions may not be able to properly define the scope, identify the right partners and security needs, neither will they be able to possess the capacity to manage cybersecurity programmes (Pâris, 2021; ECA, 2019). This is in turn only further negates and adversely affects the effective implementation of the EU's

cyber policies and frameworks. As Giantas (2019) puts it, the workability of the various legislations and frameworks at the regional and national levels relies considerably on the ability to institutions and individuals to considerably engage recent technologies to identify threats, engage defensive actions and protect critical information from corruption. This however is at the mercy of deliberate cyber educational efforts by the EU and her member countries which are currently largely lacking and absent. As the EU law enforcement training agency notes, more than two-third of EU member States do not provide regular cyber training for law enforcement officials even though they are constantly faced with the possibilities of cyber-attacks (ECA, 2019). Similarly, ENISA noted training in critical sectors in the EU do not sufficiently target the resilience of critical infrastructures even though they are extensive (Eurosmart, n.d). This challenge is also compounded by the fact that the task of establishing training policies, curriculum and activities are the Member countries and not the regional institution. This creates issues of maintenance of standards as there are no EU standards to guide such educational policy formulation and training. And this is important in vital sectors as digital forensics where certain standards are required to admit evidences for investigations.

Another dimension of the fight against cybersecurity is the raising of awareness among the populace and internet users who majorly use the internet and are mostly victims of social engineering and other forms of cyber-attacks. Majority of EU citizens who are active cyber users are vectors for attacking and spreading disinformation as they are unprotectedly exposed to cyber vulnerabilities distributed by cybercriminals across the internet space. As such awareness of vulnerabilities for cyber-active citizens is a challenge in the implementation of cyber resilience initiatives and attainment of the EU frameworks. The need for increased awareness is also deepened by the fact that the number of internet users continues to grow by the day with the result that more and more young and cyber-inexperienced or unaware population are continually registered in the internet space. The result of this is in the face of lacking cyber education and awareness initiatives are that more populations in the EU are susceptible to attacks and become victims. The EU commission had noted that the cybersecurity strategy had only been partially effective in raising individual and business awareness.

Information Exchange and Coordination

One of the major aims of the Cybersecurity Strategy and other subsequent policies has been to foster cooperation among member countries and the Commission while also

promoting information exchange and coordination at all levels (EU, 2020; Homburger, 2019; Kurbalija, 2018). The NIS Directive has also focused on strengthening trust among members (Markopoulou et al, 2020). While these and other initiatives have focused on regional partnership and coordination, findings have indicated that such moves by the EU have been largely insufficient in engendering operational cooperation and coordination. The main aim of these cooperation and coordination initiatives have been to foster relatively easy access to information and information exchange between member countries with a common understanding based on a common goal. However findings indicate that the partnerships and cooperation between member countries have seldom resulted in such synergies especially among the various agencies and stakeholders in the EU (ECA, 2019).

According to an evaluative study by ENISA, it was observed that the EU's approach to cybersecurity was not sufficiently coordinated so that there was a lack of synergy between ENISA's activities and other stakeholders in the region (Eurosmart, n.d; Pâris 2021; Jayakumar, 2020). Cooperation mechanisms in the assessment of the ECA are still immature and unable to bring about the needed synergy for developmental projects. However although the policy frameworks for the various years have repeatedly identified and outlined guidelines for cooperation and coordination, the differing policy initiatives, needs and investment programmes among member nations have worked to fragment and hinder synergies among member nations. And this is important for adequate regional cybersecurity.

Another perspective of the coordination of information exchange concerns sharing information with the private sector (ECA, 2019). This is another major pillar of partnership projected by the EU to assist in spreading and developing the cybersecurity policies and frameworks of the region. Findings however shows that a 2017 assessment of the relationship between the private and public sector by the Commission discovered that information exchange between both parties were not optimal due to lack of trusted reporting mechanisms and incentives to share information (Giantas, 2019; Mortera-Martinez, 2018). This lapse is also observed among member nations so that strategic partnerships necessary for enhancing lasting industrial capabilities are missing. While these strategic partnerships are important for tracking criminals and combating complex cybercrimes, the level of efficiency is determined not just by the level of legislative policies and documents but also by the level of trust between both parties. Findings however show that this ingredient is largely missing among EU countries hence the implemen-

tation and coordination of partnerships including information sharing are mostly mechanical and do not reflect the spirit of common goals and interests as stated by the Cybersecurity frameworks. While several initiatives comprising collaborations between advisory groups, private sector operators, EU institutions and agencies, and other international organisations to improve information sharing and cooperation, there are still loopholes identified in the partnerships.

Detection and Response

Early detection and response to cyber-threats is vital for detecting and resisting cyber-attacks and this is quite easy with detection tools. However as findings show, detecting attacks have become considerably difficult than it used to be because technologies evolve into sophisticated forms by the day, hence detecting crimes and preventing or responding to them may take a longer time (Christensen et al, 2020). Sophisticated improvements in criminal technologies has made early detection of such crimes difficult so that automated machines and other technological options for detecting and responding to cyber-attacks are increasingly focused on (Kertysova et al, 2018). However there are technical but vital issues with these systems in that they are rigidly programmed such that they may flag non-threatening activities as malicious when they are really not (ECA, 2019; Kertysova et al, 2018). This feature according to findings has made such technologies suffer low patronage from businesses. The crux however is that while early detection of cybercrimes and attacks on critical infrastructures in the EU is necessary for mitigating such attacks, certain factors tend to hinder effective detection of attacks and early response. One of these factors bothers on the reluctance of organisations to acknowledge and alert other organisations about an attack or incident on their cyber infrastructure thus exposing other organisations to potential vulnerabilities and dangers (Christensen et al, 2020; ECA, 2019). The reluctance as identified in previous sections results from the fear of negative public reputations of companies and organisations. Hence in an attempt to protect organisational image, some companies and organisations may resort to hiding useful information that may be required to access or else detect a potential cyber threat.

Also, findings indicate that prior to the establishment of the NIS Directive, there was the lack of regional institutional framework and requirements to address or respond to breaches hence there were risks of delays in incident notifications (Markopoulou et al, 2020; Lukaševičiūtė, 2019; Sterlini et al, 2019). While the NIS Directive was an attempt

to address the reluctance in reporting incidents of breaches, evidences and findings reflect the fact that there are still issues bothering on early detection and response to the owner. For instance, operators of essential services within the EU still face the issue of multiple notification and response mechanism under EU regulations such that an efficient response to a case of attack or breach is delayed or inefficient (ECA, 2019). Also, operators in the financial sectors are subject to different notification criteria, standards, thresholds and time under the GDPR, the NIS Directive, Payment Services Directive, ECB/SSM, and the eIDAS regulation (Demertzis & Wolff, 2019; ECA, 2019). In the event of such a scenario, adhering to all the legislations and guidelines at the same time will only resulted to fragmented reporting. As findings indicate, the EU's capacity to respond to attacks on a large and small scale cross-border event has been labelled limited due to the fact that cybersecurity is not yet incorporated into existing EU –level crisis coordination mechanism.

Another challenge posed by the lack of effective response mechanism to cyber threats and attacks is the fact that exchange of information between EU member countries and regional agencies still remain a concern even though several policies and frameworks for cooperation have been identified. With reluctance of State and organisations to share necessary information, responding to cyber-attacks will be difficult. Secondly, there is the issue of difference in criminal justice among member countries in the EU, as such, legal and procedural differences may impede rapid criminal investigations and prosecution of suspects especially when the crime is transnational and involves two nations with different criminal justice system. Furthermore with growing sophistication of cyber-attackers, there is need for more collaborative and cooperative efforts to adequately identify cyber threats and respond accordingly especially in these times of anonymisation. Hence findings from the study suggest that a coordinated response mechanism championed by Europol and Eurojust's European Judicial Cybercrime Network is needed to coordinate a regional response system to attacks and cases of incidents within the EU.

Protecting Critical Infrastructure and Societal Functions

A final challenge identified with the EU Cyber Security policies is the fact that protecting critical infrastructures in the EU and among member countries may face challenges arising from the fact that the EU's critical infrastructure are operated through industrial control systems (ICS) that were custom-made to work within the region (Myers,

2020; Saxena et al, 2020; ECA, 2019; World Bank, 2019). However the connectivity to the internet of some components of the ICS has presented vulnerability concerns for the critical infrastructures such that there is need for protecting these infrastructure against foreign influence and attacks. One of the ways to do this however is by constantly upgrading the systems which is a costly and time-consuming process (Saxena et al, 2020). Furthermore the protection of critical infrastructures faces the challenges of interconnectivity of devices that may have chain effects in the event of an attack. While the Cyber Security frameworks deals with protecting critical infrastructures, the connectivity and interdependence to the internet and other digital devices ultimately makes this possibility a threat to the protection of critical infrastructure (EU, 2020; ECA, 2019). As long as critical infrastructures are connected to other devices, the growing digitalisation and interconnectivity of the technical and technological world makes attacks on cyber infrastructures a possibility with constant need to monitor and protect these infrastructures against attacks. A constant threat therefore to the EU's cybersecurity infrastructure is how to engage and protect critical infrastructures from manipulation and interference from external interests for the purpose of maintaining and protecting the integrity of her infrastructure especially in the areas of politics and elections.

There is also the concern of raising readiness and response mechanism of critical sectors to large scale incidents with the aim of protecting the EU's critical infrastructure. This is important because the EU is an importer of cyber products and services which increases the risks of technological dependence and vulnerability to non-EU operators. This reliance on foreign technology and expertise fundamentally undermines the cybersecurity infrastructure of the EU region because it increases chances of non-EU operators accessing critical technologies and information of the EU.

4.5.1. Summary of Findings

In summary therefore the challenges identified above are some of the challenges discovered from the study as hindering the successful implementation of the EU cybersecurity frameworks in the region. While some of the challenges are related to the activities and ability of individuals to implement and activate these possibilities, others are related to the social and political interactions between the member countries in the region. For instance, on the challenges of skills and awareness and information exchange and coordination, there seems to be the problem of interpersonal and inter-group relation-

ships and diplomacy. On the other hand, the other challenges such as evaluation and accountability, gaps in the EU law and its uneven transposition, funding and spending, clear overview of EU budget spending, governance and standards, effective detection and response and protecting critical infrastructure and societal functions tend towards the failure of systems and structures. As such addressing these challenges must of necessity deal with not only structural and institutional capacities of organisations in an attempt to address these loopholes but must also involve improve interpersonal and intergroup relationships among other things.

4.6. Summary of Chapter

This chapter has presented the findings from the studies and researches reviewed for the current study. Findings have revealed the level of seriousness of cyber-threats and attacks to the EU region, her member countries and organisations as well as individual cyber users. While there have been unprecedented levels of attacks against the cyber infrastructure of the region, findings reveal that these threats are likely to continue escalating as the EU remains one of the most attractive destinations for cyber-attacks to all categories of malicious cyber users. Major attacks on the EU and EU member countries have however been more of politically motivated than otherwise which indicates unhealthy political relations. The findings therefore indicate that cyber-threats and attacks to EU member nations and corporations can only be better mitigated by building resilience and enhancing cyber-governance initiatives as these threats cannot be totally eradicated from the cyberspace. Also findings revealed that the EU and her member countries have taken several active steps to build cyber resilience and cyber-governance aimed at achieving cyber-peace in the region beginning from the Budapest Convention in 2001. More cybersecurity focused frameworks began from 2013 with the Cyber Security Strategic Framework. Several policy documents have been initiated by the EU since the 2013 document in an attempt to improve cyber resilience in the region. Also findings indicated that several regional cybersecurity agencies have been established by the EU in an attempt to promote the implementation of the necessary policies and legislations on cybersecurity in the region. Lastly, this section revealed the challenges associated with the cyber security frameworks especially since the initiation of the 2013 Strategy and how these loopholes affect the stated goals and objectives of the EU. Among the various challenges identified was the inability of a purely legislative or poli-

cy tool to foster cooperation among EU nations which has been a recurrent them in the various cybersecurity policies since 2013. The next section therefore attempts a critical discussion of these findings.

5. CHAPTER FIVE: DISCUSSION AND ANALYSIS

5.1. Analysis of Findings

The discussion and analysis of findings from the study conducted will be done according to the themes of the research question. The first section discusses the conceptual difficulty in the consideration of Cybersecurity in the EU, while the second section discusses the efforts of the EU and the challenges identified from the findings of the study. The challenges of Cyber Security in the EU region and the Cyber Security Strategy as discovered from the study is traceable to the following factors which are discussed in detail; conceptual diversification and perception of cybersecurity, difference in approach to tackling the menace, political relations between and beyond EU members, funding and implementation of the Cyber Security Strategy across various nations, exploitation of existing political and technical loopholes by hackers and other ill cyber users, political and technical limitations of the Cyber Security Strategy, and less awareness and skills on cybersecurity strategies by overwhelming population of cyberspace users. These challenges identified are discussed and analysed according to their implications on cybersecurity governance in the EU region and how it affects the cybersecurity efforts of the EU.

5.2. Conceptual Difficulty and Perception of Cybersecurity

As indicated from the study, there is a general conceptual difficulty relating the conceptualisation, perception and appreciation of Cybersecurity by the various EU member countries and institutions. Although this may not be an issue for national and organisational concerns, it presents serious issues for regional security and more so regional cybersecurity which is increasingly becoming the foundation and basis of Europe's economy. Cybersecurity is used to denote the protection and safety of the cyber/internet space from the various threats and harms obtainable therein. Although this is the basic conceptualisation of the term, it has been viewed and conceptualised differently by scholars, experts and institutions so that a single definition is impossible in light of the

several definitions and conceptualisations. Fischer (2014) attempts to capture the precise meanings of cybersecurity in three sentences; i) "A set of activities intended to protect- from attack, disruption and other threats- computer, computer networks, related hardware and devices software, and the information they contain and communicate including software and data as well as other elements of cyberspace"; ii) "the state or quality of being protected from such threats" and iii) "the broad field of endeavour aimed at implementing those activities and quality" (Fischer, 2014:1). This broad conceptualisation tends to classify as cybersecurity every act that protects ICT. The conceptualisation by Vishik, Matsubara & Plonk (2016) however goes a step further to include not just the actions to protect but the 'capability' to ensure the protection of the cyberspace. According to them, cybersecurity is essentially the activity or process, ability or capability, and state whereby information and communications systems and the information store therein are protected from damage, unauthorised access, modification or exploitation. These definitions generally reflect the perspectives of most scholars (Wilson & Kiy, 2014; Meushaw, 2012; Landwehr, 2012).

The literature on cybersecurity however has included more contemporary definitions that incorporate not only the technical and technological ability and capability to improve or develop cybersecurity technologies but the political and legislative capability. In light of this, the International Telecommunications Union (2011) conceptualised the cybersecurity to be the collection of tools, policies, security concepts, security safeguards, guidelines, risks management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and users' assets. This definition tries to incorporate all the activities and actions taken by public and private institutions to protect their cyber assets. Resonating this idea, the Malla Reddy College of Engineering and Technology (2021) defined cybersecurity as all the approaches incorporating people, processes, and technologies aimed at reducing vulnerability, improving resilience and deterrence, projecting incidents, establishing recovery policies and activities, law enforcement initiatives and computer network operations for building cyber infrastructure.

Carlton & Levy (2018) in their study and consideration of the concept of cybersecurity underscored the need for technological skills and knowledge in enhancing cybersecurity. In view of this position, they conceptualised cybersecurity skills as a necessary part of building cybersecurity. For them, building a framework or structure against cyber threats must necessarily involve building technical know-how and skills in indi-

vidual computer users. Without an interest and investment in the skills and knowledge of people, cybersecurity may only remain a concept that would be difficult to achieve. The emphasis therefore in this conceptualisation is on the acquisition and development of people skills in cybersecurity and related threats. For Thomas et al (2018) the concept of cybersecurity has suffered several misconceptions from application by various computer users. According to their study, they identified themes as overgeneralisation, conflation, biases and incorrect assumptions, as some misconceptions that colour the appropriate use of the term in academic circles. For instance, their study carried out in India found that students assumed that cybersecurity do not include malware that can attack keyboards and other physical components of the computer system due to the perceived idea that cyber threats do not affect or include threats against keyboards (Thomas et al, 2018).

Such misconceptions of the term affects not just the universality of grasping the concept of the term but if not properly curtailed, the practical implication resulting from such a difficulty in understanding or narrow/short-sighted conceptualisation may only lead to a limited approach in enforcing the concept (Thomas et al, 2018; Craigen, Diakun-Thibault & Purse, 2014; Bodeau et al, 2010). This is also reflective of the limited conceptualisation of the term which associates cybersecurity only with the need for technological and technical approaches to building cyber resilience and protection against criminal elements (Sleeman, Finin & Halem, 2020; Craigen et al, 2014; Kosutic, 2012). However as relatively recent developments as indicated, cybersecurity is not merely a technical and technological concept but also a political concern having to do with national security (Stallings, 2019; Craig & Valeriano, 2016), and even health security as indicated by the CyberPeace Institute (2021) and the National Association of County and City Health Officials (2017). Thus the misconceptions and definitions of cybersecurity that tend to ignore the evolving nature of technology and cyberspace are only workable within a limited period of time (Craigen et al, 2014). Reddy and Reddy (2013) similarly in their studies noted that the use of the term cybersecurity immediately brings the concept of ‘cybercrime’ to mind because cybersecurity as a concept can be said to be an attempt to eliminate all forms of cyber threats from the internet. Cybercrime however can be considered as a form of cyber insecurity and a growing menace across the globe, the manifestations of which varies across the globe in proportions and nature. Therefore conceptualising and equating cybersecurity with the narrow conceptual of cybercrimes may inadvertently promote the picture of a certain type of cyber relat-

ed crime prevalent in a region while non-recognised in another, hence cybersecurity which is a more broader concept is favoured in conceptualising the various threats on the internet.

As stated above, the evolving nature of the term has made a static and definite definition and conceptualisation of the term impossible so that while there are certain limits to defining the term today, new boundaries are likely to occur in the nearest future to make such definitions inadequate (Stallings, 2019; Costigan & Hennessy, 2016). One of the core additions and indications of the evolution of the concept of cybersecurity is the expansion into the global political and security sectors (Tsakayan, 2017; Maurer & Morgus, 2014). Politically, cybersecurity is regarded as a critical infrastructure as global and international political relations and dynamics have revealed that cybersecurity plays a major role in maintaining global order, peace and security (Myers, 2020; Robinson, Jones, Janicke & Maglaras, 2018; Tsakayan, 2017). In light of this, the conceptualisation of cybersecurity as a political concept and idea has gained traction. Defining the concept from a political viewpoint, Maurer & Morgus (2014) sees the term as a global regime concerned with making the internet space stable for legal contents and prosecuting illegal contents for the sake of maintaining national security and healthy interactions amongst nations. They further reason that essentially, cybersecurity has to do with the security of national information and digital assets from unauthorised access, so as to maintain confidentiality, integrity and availability whenever it is needed (Morgan & Gordijn, 2020; Maurer & Morgus, 2014). This political conceptualisation becomes important in view of the encroachment of nationally sponsored hackers to gain unauthorised access to national archives to retrieve sensitive information (CRS, 2020; Sadowsky et al, 2003).

The political conceptualisation according to scholars and the literature is closely associated with the adoption of cyber technologies by nations and governments to pursue the philosophical and ideological agendas as well as enhance national security (Craig & Valeriano, 2018). As Tsakayan (2017) puts it, the concept of cyber-war and cyber-conflict was initiated by the tendencies of world powers like the USA, China, Japan and Russia who engaged technological knowledge to pursue their political agenda in the 1970s. This was heightened by the incursion of Russia in the 2016 United States election using the internet platform and several other cases of cyber-attacks on the national cyber infrastructure and frameworks of security organisations in the US, China, Russia, and other countries (Myers, 2020; Fidler, 2016). This race to gain global supremacy and

promote national agenda in international diplomacy using cyber technological resources has helped to strengthen the political conceptualisation of the term so that a purely technological definition of cybersecurity in recent times is inadequate to grasp the entire significance of the term (Gilligan & Pardo, 2020; Sleeman et al, 2020; Morten, 2016; Craigen et al, 2014). As Tsakayan (2017) and Medeiros & Goldoni (2020) contend, the concept of cybersecurity has gone further to include not only the political space but virtually every other sector of a nation so that an attack on the cyber infrastructure is likened to an attack on the nation. This is because every sector of the economy is virtually dependent on the access to information on the cyberspace (ACS, 2016). Protecting this critical infrastructure therefore is an important aspect of national security in most nations.

The use of cybersecurity in various conceptualisations and studies involves the notion of identifying and eliminating threats in the cyberspace (Carlton & Levy, 2017; European Commission, 2017). Cybersecurity according to this view essentially seeks to eliminate pervading threats on the cyberspace which according to the European Court of Auditors (2019) have continued to grow exponentially. The idea of threats on the internet space as cybersecurity scholars have noted, affects all category of users. Even in the health sector, there have been cases of cyber related threats and attacks that target health information of institutions and individuals for harmful purposes (CyberPeace Institute, 2021; Koeppe, 2020). This has influenced the increasing interest of healthcare institutions in research on cybersecurity measures and strategies typified by the National Association of County and City Health Officials report (2017). Relating the threats on the economic sector of nations, Antunes et al (2021) noted that trades and business information of national and international bodies and organisations are constantly faced with the threats of unauthorised access and manipulation and exploitation of sensitive data. The threat to these data with huge financial and economic implication has necessitated the development and interest of these institutions to cybersecurity.

In summary therefore, the attempt to conceptualise cybersecurity and give a definite definition with its multifaceted dimensions and sectors as it has continued to widen in scope and understanding has proved difficult for scholars and experts. What is however obtainable is that various countries, institutions, sectors and experts from the various fields attempt to give a definition as it relates to them since a universally accepted definition may be impossible in view of the continual evolution and expansion of the term. The implication of this on the EU Cybersecurity Strategy and Cyber governance attempt

as realised from the literature is that there are several approaches to attaining cybersecurity across the numerous sectors. While the central aim and goal is making the internet space safe and stable for use for all categories of users, the approaches are largely dependent on the capability and ability as well as the necessity of the skills and tools at the disposal of the various categories of users. For instance, due to the perception of Cyber Security as a political strategy and conflict between bigger nations, smaller nations within the EU have gained a posture of allowing bigger nations engage cybersecurity strategies (Giantas, 2019).

This is reflected in the amount of funding and technical investment in Cybersecurity strategies by smaller nations within the EU. While it may considered that these nations would not be able to invest as much as bigger nations within the region, the fact that these nations are more vulnerable to cyber-attacks and cyber insecurity should be enough bolster to aggressively engage and support cyber governance strategies within the region. However, as findings indicate, there is a growing fear that the technological and economically bigger EU countries through these global and regional cybersecurity initiatives are attempting to extend their political and technological influence over smaller regions especially through cyber governance. In such an atmosphere as related above, concerted efforts at implementing and tackling identified challenges is difficult because a consensual perception of the problem is grossly missing among member countries. Flawed by national and institutional interests, there is no generally agreeable definition and designation of what constitutes security in the cyberspace. As such while a regional initiative as the EU Cyber Security Strategy may have been developed to provide regional governance to the cyberspace and promote cyber peace within the EU, the differing perspectives grossly affect the implementation of this document among member countries. The commitment level based on these differing perspectives is at best intermittent and not consistent so that in the course of implementation, institutions and organisations within member nations are better aligned towards engaging different, false and flawed implementation of the regional strategies better suited to their perception of the cyber insecurity.

Even among scholars, the differing perspectives and definitions of the concept presents a challenge to identifying and understanding the nature of cyber threats and the necessary cybersecurity approach to engage within the region. Although a general agreeable conceptual consensus is rare amongst scholars, in matters of security (national, regional and global), the implications may be more devastating and adversarial than

mere dialogues. Actualising cyber peace and instituting cyber governance strategies within the EU is definitely at the mercy of a consensual understanding and definition of what constitutes cybersecurity. This lays the platform upon which the whole cybersecurity structure is built and sustained. Hence the inability for scholars and experts to agree beyond nationalistic and political biases on what cybersecurity would mean to the EU has made thorough implementation of the EU Cyber Security Strategies difficult. What this means for the EU is that the threat level of the cyberspace is viewed differently by member countries, institutions and business organisations even though they all believe there are threats in the cyberspace. For technologically and economically smaller nations, cyber threats are actually posed by bigger nations than by an inherent threat in the cyberspace hence cybersecurity from this perspective is enhancing national security against regional and political incursion. This is especially evident in the cases of Russia versus Ukraine, Russia versus Estonia and other nations that have been confronted with the Russia hegemony in the recent past.

On the other hand, nations who understand cyber threats as arising from the activities of smaller countries perpetrating financial scams and hacking government institutions for financial reasons, perceive cybersecurity as building sophisticated firewalls and cyber resilient strategies against this class of threats. Still for others, the perception and mitigation strategy may be different, hence while series of funds and budget are allocated annually for enhancing and implementing regional cyber governance and cybersecurity strategies, several businesses, organisations and institutions as well as nations are still more aligned towards engaging domestic cybersecurity strategies. The proof of this is the finding by the European Court of Auditors (2019) that some institutions and organisations within the EU in defiance of approved cyber strategies engage false and flawed implementation of several EU Cyber Security Strategies out of concern for profit, customers and sustainability in business. In other words, the various regional strategy is not trusted enough to provide the required protection or better still not perceived to be in the overall interest of the organisation hence implementation is not total or thorough. Meanwhile achieving the full intention of cyber governance and cyber peace in the EU is only possible when nations committedly implement the several strategies outlined by the EU. Furthermore, the fact that several institutions and countries do not engage total commitment to the established cyber security codes may also be an indication that the perception of cyber threats and the required strategy for tackling these threats are different. For such organisations and even member nations that believe that the interests of

their businesses and profits are not taken into consideration by these strategies, there will be obvious flaw in the implementation process as long as differing perspectives and appreciation of the cyber threats and cybersecurity persist. Efforts therefore at arriving a consensual conceptualisation of the definition of cybersecurity and the specific strategies to achieve this state are important. While it may be difficult to arrive at such an agreeable conceptualisation especially among scholars and experts, as long as political biases and nationalistic considerations influence regional initiatives as the EU Cyber Security Strategy, achieving cybersecurity governance may be farfetched. In essence, there is need for establishing cyber peace as it relates to the conflict of perception, conceptualisation and ideas of cybersecurity among EU member countries and experts before it can be translated to actual peace in the cyberspace. While this conflict of ideas and perceptions persists however, there may not be effective cyber governance within the EU cyberspace.

In summary therefore, the difficulty in perception and definition of cybersecurity and the threats of the cyberspace by EU member countries and institutions presents a specific challenge to understanding and engaging necessary steps in tackling these threats. At the conceptual and pragmatic levels, there is need to adopt a regional definition that reflects the realities and threats of the various member countries of the EU and the necessary strategies to eliminating these threats. While other necessary steps may follow from this, the task of adopting a regional and relatable definition is important for laying the platform for establishing cyber governance within the EU cyberspace. More importantly, the political dialogues and intrigues that inform the difference in the perception and definition of cybersecurity must also be addressed to make room for a balanced interpretation and appreciation of cyber threats. This is because, the presence of cyber threats is not the basis of disagreement or dispute among members but the source of this threats and the medium for eliminating this threats. Therefore not only a technical definition of the term but also a political dialogue is important to eliminate the various suspicions surrounding cyber threats in the discourse of cybersecurity within the EU region.

5.3. Discourse on the Efforts of the EU in enhancing Cybersecurity

Evidences from the study has indicated that the EU since 2001 has taken efforts to address cybercrimes in the region although more active efforts towards addressing cybersecurity were generally initiated in 2013 beginning with the Cyber Security Strategy. From the Budapest Convention on Cybercrimes, to the various regional cybersecurity policies, indications from the study indicate a steady responsiveness to cyber and technological realities (Brady & Heinl, 2020; Veale & Brown, 2020; Council of Europe, 2020). Perhaps an indication of the responsiveness of the Commission to cyber realities and developments is the update from focusing on combating cybercrimes to generally addressing cyber insecurity which is a broader categorisation encompassing other forms of cyber threats. Also the efforts of the EU have yielded several positive results and initiatives such the establishment of the ENISA, a regional cybersecurity agency and other similar agencies and institutions at the national levels for combating crimes. Similarly, efforts of the EU have resulted in the adoption of cybersecurity policies and legislations across various countries in the region enhancing collaborations in the investigation and prosecution of cyber based crimes and threats (Pâris 2021; Jayakumar, 2020; Bendiek & Maat, 2019). Due to the efforts of the Commission, significant funds and partnerships between and beyond member nations of EU have also been facilitated in recent times (Giantas, 2019; ECA, 2019; Kertysova et al, 2018) making cyber governance and global cybersecurity initiatives possible.

These efforts have also set the pace for global cybersecurity initiatives for several regions of the world that have followed the steps and initiatives of the EU (Kertysova et al, 2018). Also the efforts of the EU has succeeded in strengthening cybersecurity resolve among several developing third world nations of the globe as findings indicated that through the strategic partnership the Commission has succeeded in driving digital technology and cyber defence infrastructures in these nations (Bendiek & Matt, 2019; Kertysova et al, 2018). These moves both within and beyond the EU has indicated some level of responsiveness and dedication to the global technological age where the need for cyber governance and cyber resilience increasingly grows by the widening cyberspace. Also the efforts concentrated at developing cyber policies within the region has also helped to relatively create an atmosphere of consciousness and awareness at least among governments on the need for extending strategic security discourse to the cyberspace. The establishment of the various cybersecurity agencies at the national level for

member nations of the Commission in the last two decades can be readily traced to the initiatives and diplomacy of the EU in this area. As such the activeness of the EU in the development of cybersecurity and cyber resilience measures within the region cannot be ignored in the discourse on cybersecurity.

Evidently, the initiation and establishment of policies such as the 2001 Budapest Convention on Cybercrimes which became operational in 2011, the 2013 Cyber Security Strategy which was revised and updated in 2018, the 2014 Cyber Defence Policy which was aimed at installing defensive measures and mechanisms in the cyberspace across the region, the 2015 European Digital Single Market which aimed at enhancing harnessing and integrating the European digital technology market especially the private sector and the public sector for easy collaborations and trust-building, the 2016 Directive on the Security of Network and Information System otherwise known as NIS Directive that further issued guidelines and policies for strengthening cyber governance and cybersecurity within the region, the 2017 Cyber Diplomacy Toolbox that aimed at strengthening political and foreign diplomacy between member-countries and the 2017 New Cybersecurity Regulatory Package that revised the mandate of ENISA, the 2018 update on the European Cyber Security Strategy, the 2019 Cybersecurity Act that improved on Cybersecurity Certification for member countries and empowered ENISA as a permanent agency. Similarly the several policies launched in 2020 were also instrumental in strengthening cyber defence and resilience infrastructures in the region.

Although concerns have been raised about the implementation and effectiveness of these policies, the response from countries and the annual evaluation of existing policies and state of affairs of the EU cyberspace for the purpose of enriching and addressing policy and diplomacy loopholes are important steps commitment to which are sure to guarantee attainment of cybersecurity and resilience within the region. However, a close look at the initiation patterns of cyber policies by the EU will indicate that policies are mostly reactive and not anticipatory i.e. cyber policies are mostly in response to an existing state or occurrence of activities in the cyberspace which may not be pleasant or consistent with the aims of the EU. For example although the Budapest Convention on Cybercrimes were initiated as far back as 2001, adoption and implementation among member-countries only began in 2011 after several nations had fallen victims to massive cyber-attacks and national cybercrimes initiatives had proven impossible to address cyber concerns. Even at this, there was no adequate anticipation of future threats that

would be prevalent in the regional cyberspace especially in consideration of the aggressive activities of Russia.

As such the Cybercrime Convention did not recognise cyber threats as a national security threat even though the cases of Estonia and Georgia were relatively recent. This narrow focus on criminal acts on the cyberspace thus was inadequate in enhancing cybersecurity measures and defence mechanisms even when the document was reviewed in 2013 and issues such as criminal prosecution and the establishment of Cybercrimes Centre in the Europol (European Police) were addressed. The 2013 Cyber Security Strategy similarly which was a response to the growing threats on the national cyber infrastructure and diplomacy, was also largely not taken very seriously as 11 nations did not immediately respond to the concerns or the recommendations of the policy when it was ratified (Mortera-Martinez, 2018). This seem to indicate that some nations either did not understand the full implications of such a policy or where not fully convinced about the necessity of its implementation in an ever growing cyberspace. This posture and position towards cybersecurity initiatives could also be reasoned to be the rationale behind the meagre investment in cyber development innovations and technologies. For the other policies that followed the 2013 Cyber Strategy, they followed similar patterns of responding to crisis and occurrences in the cyberspace.

For instance the several cyber-attacks on EU countries from 2013 to 2017 increased considerably as noted by the ECA report (2019) even after several policies were established at the EU level. This suggests either that the EU did not comprehensively address the pervasive threats on the region's internet space or because member-countries did not fully implement the recommendations of the Commission. Attacks on the healthcare sectors, economic and government institutions even after the operationalization of the Cyber Security Strategy are indications that the efforts of the EU and the regional cybersecurity agencies have either not yielded the intended results or that threats are evolving beyond the anticipation of the EU. As the report by the ECA noted, some countries within the EU were still reluctant to acknowledge the vulnerability of the internet space to the pervading threats on their cyberspace. Cyber terrorism and other ideological threats particularly arising from terrorist groups in partnerships with State-actors are a continual threat to the EU cyberspace as historical and recent occurrences have shown but these concerns are somehow not fully addressed even though several of the cyber policies have indicated fostering diplomacy as parts of their objectives. Therefore while considerable efforts have been committed to the development of technical in-

frastructures and cyber technologies at least by policy at the regional level, implementations have not fully reflected such commitments.

A major danger associated with reactionary measures rather than preventive measures as observed from the study is that more national and regional infrastructures and data on the internet space are much more vulnerable to attacks and exploitation by ill-cyber users especially those who are continually exploring the cyberspace in search of vulnerabilities in national and regional institutions. Thus there is need for deliberate investment in cyber defence technologies by nations to not only develop security measures but also technologies that supersede the technological capacities of these ill-intended cyber users. This is instructional because as findings show, States both within and beyond the EU possess the necessary resources needed to develop the necessary technology to protect the cyberspace if deployed rightly while criminal minded hackers and other categories of cyber threat actors hardly possess these technologies except in partnerships with State actors. This means therefore that with the right deployment of State resources and technology, defensive and anticipatory technologies can be developed by nations within the EU. The efforts deployed by the EU is however limited especially if member countries for whatever reason do not share and implement the concerns and recommendations of the EU cybersecurity agencies. While some regional institutions may also be subjected to such vulnerabilities and attacks, nations are much more likely to be affected as evident in the attacks the UK healthcare institution, Ukraine's power grid and Finland's banks amongst other numerous cases (Kertysova et al, 2018; Mortera-Martinez, 2018).

Since relative attention has been drawn towards funding and investment in the cyber technological innovations, more effective approaches may now involve addressing the national implementation strategies and state of member nations since evidences show mixed reactions towards regional policies especially between richer and poorer nations within the Commission. The political disparity and ideological disposition as well as economic divide between member nations are factors that could hamper and may be responsible for the unequal implementation among countries. Also the recent political developments in the EU and the world politics generally are concerns that may affect the existing and continual efforts of the EU in terms of cybersecurity. The implication of Brexit on Europe's cybersecurity strategies cannot be ignored if future prospects and sustainability of the cyber governance objectives of the EU must be attained. This is because the UK has been a major player and actor in the development of the several re-

gional policies on cybersecurity both in terms of funding and technology. Therefore the exit of Britain from the EU is very likely to create diplomatic and technological loopholes that may be difficult to fill in a politically dynamic and unstable world.

This is compounded by the ever increasing and growing need for sufficient cybersecurity and resilience within the EU as threats are projected to increase with coming years. Even though it could be reasoned that nations who were otherwise dormant and sluggish in response to regional cybersecurity policies may now be more active in an attempt to fill in the gaps created at the regional level, very few of these nations possess the same financial and technological resources. Therefore more intentionality and commitment towards implementing the numerous cybersecurity policies must be exhibited by member nations. Interestingly, efforts at enhancing cybersecurity and cyber resilience since the last two decades within the EU have not proved sufficient to protect cyber users (private and public) from the vulnerabilities and threats that continue to threaten users. And these efforts were initiated at a time when cyber threats were an emerging phenomenon at least at the scale and proportion that is currently experienced. At the present however these efforts have hardly stopped or even reduced the level of threats and vulnerabilities on the cyberspace as active users of the internet are continually increasing with little effective governance strategies.

The concern therefore is what could be responsible for the ever increasing threats even with efforts targeted at developing cybersecurity strategies by several nations both within the EU and around the globe generally. This is more disturbing considering that nations are supposed to possess more sophisticated and advanced technologies than individual and private organisations (Shackelford, 2017). In the reasoning of Morgan & Gordijn (2020), Schlehahn (2020) and Craig & Levy (2017), the inability to attain considerable cybersecurity goals at the national and organisational levels could be traceable to the level of cyber awareness and education among cyber users. The fact that most employees and organisations do not take cybersecurity measures importantly could be a direct cause of this trend or as Giantas (2019) reasoned, cyber threat actors in an attempt to continually perpetrate and stay above law enforcement agencies, are constantly developing their cyber skills to outsmart government initiatives. Whatever the reasons, there may be need to pay attention to developing cyber awareness and education schemes among the EU especially among the private sector which is mostly targeted for financial frauds (Giantas, 2019; ECA, 2019). Of course it could be safely assumed that the vulnerability of nations and institutions within the EU to cyber threats is traceable to

the ignorance of cyber users to the tactics of these criminally-minded actors and technical know-how on cybersecurity technologies. In other words very few public and private organisations possess workforce that are sufficiently skilled in the cyberspace that can engage defensive and preventive cybersecurity measures. This factor rather than the evolving skills of hackers and cyber terrorists may be reasonably responsible for the level of successful attacks recorded in the EU cyberspace.

In summary, the efforts by the EU on achieving cybersecurity in the regional has so far been commendable as they have been instrumental in developing security consciousness among member countries both within and beyond the EU. Also the problems related to the implementation of the various cyber policies have been given sufficient appraisals and addressed in subsequent regional policies. However these efforts can be considerably improved on to move from reactive measures to preventive measures such that national, organisational and personal cyber infrastructures and resources are not wiped out or exploited by the ever increasing threat-actors on the cyberspace. More so the attention of the EU may also be equally focused on improving diplomacy amongst member nations and not just cyber diplomacy as implementation of the existing policies which are capable of resulting in cyber resilience and cyber governance are not entirely implemented for political and economic reasons which are not totally addressed in the existing cyber policies. Also the EU's efforts may now be more generally directed at achieving a cyber-literate audience for existing cybersecurity policies and technologies to be more fruitful at the regional and national levels. The fact that internet threats and attacks directed at national and regional organisations are likely to increase in coming years necessitates not only an investment in cyber technologies but also considerable attention in raising a cybersecurity conscious and skilful citizenry. This factor more than the skilfulness of hackers and other threat actors across the internet space, may be responsible for attaining cybersecurity and resilience within the EU.

5.4. Analysis of the Challenges of EU Cyber Security Strategies

An identification of the challenges of the EU Cyber Security Strategies was done in the previous chapter, however an analysis of these and other challenges identified in the course of the study is done in this section. Ordinarily, the challenges facing the successful implementation as related in the literature covers issues as funding and spending, lack of meaningful evaluation and accountability of the Cyber Security Strategy, gaps in

the EU law and its uneven transposition with cyber policies, governance system and standards, budgetary issues, problem of information sharing between national and regional agencies, response systems, awareness and skills development on cybersecurity, and protection of critical national and societal infrastructures etc. Close analysis of these situations however uncover political and diplomatic issues that are not addressed in existing literatures hence this section discusses the identified challenges of the EU Cyber Security Strategies in more details and analyses their implications on the EU's cybersecurity and cyber governance ambition.

i. Conceptual Diversification and Perception of Cybersecurity

The effects and implication of conceptual diversification and perceptions of cybersecurity in the EU region have been extensively discussed in the previous section. It is worth noting here however that this presents a major challenge to the EU Cyber Security efforts as it does not allow for a committed and concerted effort towards achieving cyber peace and cyber governance even with the huge budgets of nations and the European Commission allocated to this aim. The political, economic and technological perceptions influencing the definition and conceptualisation of cybersecurity must thus be addressed to improve the prospects of achieving cyber peace. Also it is worth noting that a unified understanding and definition of the concept of cybersecurity at least as it relates to the EU as well as a common appreciation of the threats and vulnerabilities of the cyberspace for member countries and stakeholders is necessary to forge a unified front towards attaining effective cyber governance and cyber resilience in the region. While not undermining more narrow nationalistic perceptions of cybersecurity (as they arise from perceived – real or imagined – threats from State actors within and beyond the EU), promoting such nationalistic concerns may do more harm than good to the regional Cyber Security objectives. Hence practical diplomacy and not just cyber diplomacy is necessary to address existing conceptions and misconceptions of cybersecurity for the purpose of regional practical threats. Diplomacy of course does not mean undermining the national cyber security concerns of member nations but addressing the root of these perceptions and concerns which are mostly founded on historical and recent antecedents between member nations on the cyberspace. For a major player in global security and cyber defence technologies as the EU, relegating political, philosophical and ideological differences with their practical implications on regional cyber-

security initiatives go unresolved only amounts to promoting policies with little possibility on practical realities. The basis of this diversified perception and approach to cybersecurity must thus be addressed.

ii. Difference in Approaches of Tackling Cybersecurity Menace

A major challenge arising from the implementation of the EU Cyber Security Strategy in the EU is the difference in approach in addressing cybersecurity which is an offshoot of the perception problem. As findings indicate, while some actors and stakeholders favour a technological approach to tackling the menace in the form of building software programmes, firewalls, enhancing research in cybersecurity and other such strategies, some others are aligned with policy approaches and still others with cybersecurity education. While these approaches are all important steps and approaches for tackling the cyber security menace within the EU region, there are actors who are more aligned with specific approaches for specific reasons. As such in implementing the EU Cyber Security Strategy, these biases are very likely to play out and affect the attainment of the overall goals and objectives of the strategies. For wealthy nations and technologically advanced countries, the concern and approach likely to be adopted in tackling cyber threats relate more to cybersecurity education and establishing policies as seen in the case of the EU where countries like the UK and Germany have invested considerably in cybersecurity policy and education (Griffith, 2018; Kertysova et al, 2018; Mortera-Martinez, 2018). In contrast however, nations with less technical and technological abilities are more aligned with building cyber resilience by investing considerably in technology. While these different categories of countries are likely to adopt all three approaches (policy, technological, and education) in the course of building cybersecurity and enhancing cyber governance, they are more likely to be committed or show preference for areas of perceived weakness and greater needs.

As earlier stated, this difference in the preference of actions to mitigating cyber threats among EU members is closely related to the perceptions of the nations on their vulnerability and areas of weaknesses. Estonia, Ukraine and other victims of Russian hegemony within the EU are more likely thus to engage in structures that enhance their national cybersecurity structure primarily before investing in long education and policy approaches. The difference in approaches to addressing cybersecurity within the EU is further compounded by the lack of a meaningful evaluation and accountability strategy

for cybersecurity strategies among EU members. As indicated by findings, while the EU Cyber Security Strategy outlines necessary steps and objectives for member countries to meet and engage for the purpose of achieving cyber governance and security, there are no measurable benchmarks for evaluating the implementation of these goals. As a result nations are almost entirely left on their own to implement whatever strategies they think reflects their best interests. This has thus influenced a diversified implementation approach. For one, the investment of funds and other resources for the attainment of the goals of the Cyber Strategy is grossly affected by the lack of regional evaluation benchmarks for member nations so that a uniformed investment in cybersecurity initiatives by member nations is not possible.

This lapse has made some scholars opine that the EU Cyber Security Strategy at best is only a policy document with stated objectives but not a measurable instrument that can be evaluated to know the degree of progress that is made in relation to members' implementation. At best it is regarded as a document expressing wishes and not necessarily strategizing the necessary steps to be evaluated by the regional Cybersecurity body. These lapses therefore promote diversified approaches that are not measured at the regional level to know their implications and impacts on the overall stated objectives. Nations are therefore left to pursue any aspect of the policy document that appeals to them most. This is a challenge to the overall attainment of cyber peace and cyber governance in the EU because attaining such objectives as stated in the EU Cyber Security Strategy necessarily requires promoting a set of actions among member nations as well as working in close relations within the EU. Due to the lack of concerted approaches and lack of evaluative mechanisms, member nations and institutions are reported to perform no internal auditing to determine how successful policy implementation have been both at the national and regional levels. A documentation of the necessary expectations from member countries within a set period of time is an important boost to the implementation efforts of the Cyber Security Strategy however this is lacking hence non-measurable approaches are engaged across the EU region. As implied by Lété and Pernik (2017), knowing what is expected of them to do within a specified period of time may further strengthen the resolve of member countries to adopt necessary steps in furtherance of the cyber governance and cyber peace within the region.

To address the differences in approach to cybersecurity, there must necessarily be a conscious effort at developing measurable objectives and accountability structures with which member nations can measure progress at the national and regional level. These

reports or measurable objectives will assist nations to diversify and engage mutual approaches to building cybersecurity within the region rather than engaging biased approaches. A benefit of a regional evaluative benchmark is that nations are likely to better align national interests with regional cybersecurity strategies thereby making implementation easier. In cases of conflict of interests, the accountability document may also state the necessary course of action to avoid neglecting regional goals and considerations. However while there remains a lack of measurable and evaluative instruments for member nations to take specific course of actions more seriously, a concerted approach to building cybersecurity governance within the EU may prove difficult. Therefore a document of this nature is required to better outline and recommend nation-specific course of actions for member countries to curb disharmonious pursuit of cybersecurity strategies by member nations.

iii. Political Relations Between and Beyond EU Members

A major challenge identified from the study affecting the goals and objectives of the EU Cyber Strategy is the political interactions and relations between EU member countries. This is perhaps one of the most important determinants of the success or otherwise of the Cyber Security Strategy because as findings indicated, there are intermittent and hostile political relationships among member countries (Giantas, 2019; Kertysova et al, 2018; Craig & Valeriano, 2016; Bendiek, 2012). Far from being technical or technological, the trends of cyber threats and attacks over the years within the region have indicated a pattern of politically motivated cyber conflicts and confrontations. Hence Brady & Heinl (2020) expressed the opinion that cybersecurity at least within the EU is more of a political problem than it is a technological problem. The fact that the major attacks cyber-attacks that have assumed national proportions recorded by EU countries and neighbour-countries were targeted at national cyber infrastructures and were products of political disputes between countries seem to suggest the fact that the true threats to the cyberspace within the EU is political relations and interactions (Meer, 2015). While other forms of threats are prevalent within the EU cyberspace however, politically motivated cyber-attacks seem to be the most devastating and prevalent threat especially for smaller nations within the region. This is important for policy actions and foreign diplomacy because nations with hegemonic expansion tendencies as Russia and far-east China have not disguised their intention of seeking and promoting their political influ-

ences over nations in Europe either by flouting global standards or undermining regional security protocols (Pâris, 2021; Jayakumar, 2020).

This of course has implications on the regional interaction between nations in the EU especially between those benefitting from foreign relations with these politically ambitious nations and others who feel threatened by their encroachment into the EU territory. The political intrigues over the last couple of years have also shown that the real threats on the cyberspace especially for EU countries may not necessarily be outsider threats even with the constant hacker threats but European actors within the EU (Pâris, 2021). This proves the point therefore that a major threat to the attainment of the EU cyber governance and cyber peace initiative is the political interaction among the nations within the region. Even in cases of threats arising from beyond the EU, there have been indications of links to EU countries (Pâris, 2021; Giantas, 2019; Kertysova et al, 2018). Different political perspectives and philosophical alignments among the EU countries therefore pose a more direct threat to EU cybersecurity than outsiders. As Craig & Valeriano (2016) rightly observed, political differences and conflicts are now currently engaged in the cyberspace. This informs the concept of cyber peace and cyber war. As far as the EU is concerned however, the political interaction between groups of member countries can be better characterised as a state of hostility or non-cordiality. This state of affairs even though not reflected in the physical exchange of military might is tested and exhibited on the cyberspace. The fact that Russia has singlehandedly being in direct and indirect cyber confrontations with nations like Estonia, Ukraine, Bulgaria and NATO allies as the United States is indication that cyber threats at least within the EU are actually a product of conflict of political and philosophical interests among nations (Pâris, 2021; Giantas, 2019). While the EU Cyber Strategy document addresses all categories of threats in the cyberspace however, they ignore this very vital aspect of cybersecurity which is the interactions and relations between countries.

Building interactions and relationships among EU countries on the basis of regional cybersecurity can only be productive in an atmosphere of shared understanding and mutual relations, not in a suspicious and ill-willed relationship. This particular factor has been unaddressed by the EU Cyber Security initiatives. While the ENISA and other regional cyber agencies are established to foster cooperation between member countries in the sphere of cybersecurity, the political and philosophical basis for mutual interaction and cooperation is largely missing. For instance, the pervading political and cyber hostile behaviour of Russia has particularly posed a serious threat to smaller nations so that

the perception of cybersecurity is now more generally associated with building cyber defences against the spying and hacking capabilities of big nations like Russia (Pâris, 2021; Giantas, 2019; Lété & Pernik, 2017). Furthermore, while political events in Europe in the dawn of the 21st century reflected the genuine hostility of Russia towards other nations within the EU region, cybersecurity strategies did not take into consideration the need to mend these political and philosophical fences between nations before establishing cyber policies to govern the EU region. This of course presents a political and technical problem to several nations because as far as cybersecurity and national security is concerned, they are faced not with faceless human agents behind computer systems but with specific ambitious nations who will deploy all their resources at their disposal to promote their political and philosophical influence over these small nations. Hence collaborating with such nations would be viewed as being vulnerable to the enemy or very threat they seek protection from.

Protection from this form of threat therefore would mean protecting cyber infrastructures and national infrastructures from access to these state-actors even through regional platforms. These fears are not unfounded and have influenced the cybersecurity strategies of several nations and local organisations and institutions within countries in the EU. The report by the ECA (2019) that organisations that feel their interests are not represented and protected by the EU Cyber Security Strategy and hence resort to flawed implementation of the regional cybersecurity policy recommendations, is indication of the mistrust for such regional encroachments. As a result of this, there is a weak implementation structure of regional cybersecurity initiatives especially among the private sector, which feel their organisational interests are not represented and protected. Furthermore, the effect of the suspicious political climate among member countries has ensured that cybersecurity is not given a priority among public and private institutions especially at the decision making levels (ECA, 2019; Giantas, 2019). It would necessarily be that if these policies were viewed as being in the interest of the private and public sectors, member countries would do all within their capacity to implement these processes. But the fact that there is a seeming nonchalance at the organisational and national level to fully own and participate in the actualisation of the regional cybersecurity and cyber governance initiatives suggest the suspicions and intrigues surrounding the development and implementation of cybersecurity governance within the EU.

As Kavanagh (2017) and Bendiek (2012) rightly questioned in their studies, the concept of cyber governance is still questioned among EU member countries and private

institutions especially as it relates to the hegemony question between states. While the EU Cyber Security Strategy is doubtlessly poised towards ensuring effective cyber governance in the EU cyberspace, the fear of smaller nations is whose governance are these policies trying to establish? And whose interests do these cyber governance initiatives guarantee and protect? The question is pertinent because less technologically advanced nations are subject to the more advanced countries within the region and these technologically advanced countries through the EU are evidently spearheading the need and development for cyber governance to protect her rich cyber infrastructure and resources. Furthermore, the technologies and cyber systems provided for enhancing and protecting these cyber initiatives originate from advanced countries that are already suspected for their capitalist and political dominance tendencies. Therefore the question arises for nations which feel vulnerable to the tactics and spying prowess of advanced countries, that whose interests are represented and protected by the regional cybersecurity policies. For scholars like Rone (2020), Inversini (2020) and Craig & Valeriano (2018), the real intention is to extend the political dominance of capitalist democratic countries to the cyberspace in the guise of protect the cyberspace from attacks and threats that are ordinarily perpetrated by some of these nations. Thus the suspicion of being subjected politically, economically and also extending this to the internet space presents a challenge to smaller nations.

The findings from the study seem to indicate that this factor is one of the numerous factors responsible for the nonchalant and flawed implementation of the Cyber Security Strategy of the EU. As long as these underpinning fears persist for smaller nations, the question of interest, interaction and relationship between nations will continue to affect the implementation process of regional cybersecurity strategies (Demertzis & Wolff, 2019; Giantas, 2019). The developed and developing dichotomy between nations in the EU and the resulting political intrigues that characterise such interactions is therefore a necessary factor that must be considered in the implementation process of cybersecurity security initiatives as well as the development of a cyber-governance framework that will be acceptable to the various categories of nations in the EU (Cappelletti, 2021). Without dissuading these fears by addressing the hegemonic and political encroachment tendencies of nations within the EU especially those related to national security and human rights violations, the face-value collaborations enshrined in the EU Cyber Security Strategies may at best only result in a cosmetic solution to a deeper problem. Foreign diplomacy and interaction between member countries ought to be addressed to re-

lax the political atmosphere from one of hostile and intermittent interactions to one of mutual respect and understanding. Only in such an atmosphere will a consensual approach to cybersecurity and cyber governance be productive both at the domestic and regional level.

iv. Funding and Implementation of the Cyber Security Strategy Across Member Nations

Inadequate funding and budget spendings for the implementation of the Cyber Security Strategy was another major challenge discovered from the study as affecting the successful implementation of the policy. This inability to adequately fund the implementation process of the Cyber Security Strategy by member States can be traceable to several factors. For one, many EU member nations and the European Commission have committed comparatively low budgets to the actualisation of the policy recommendations either due to the unavailability of funds or little appreciation of the cyber governance objective of the EU. As findings indicate, the annual spendings and budget by the EU and the member countries on cybersecurity represented just one-tenth of the United States' annual budget on cybersecurity. In other words, in comparison with the United States dedication to building cyber resilience and cyber governance, the EU region is yet to appreciate the depth of cyber threats and cyber-attacks as well as the need for improving cybersecurity within the region. A proof of this is the level of investment assigned to such regional concerns both at the regional and the national level although as noted by the ECA (2019) report, many nations within the region are economically unable to contribute such huge financial commitments to developing regional cyber infrastructures. The question however that is to be considered is that do nations within the EU view cybersecurity as a worthy and necessary concern worth the allocation of huge security budgets and spendings?

The fact of budget allocations and spendings cannot be discussed without considering the level of appreciation and recognition of the need for building cybersecurity initiatives and enhancing regional cyber governance to protect critical cyber infrastructure. If the previous concerns discussed above are put into consideration, then the reluctance and insignificant budget allocation to cybersecurity can be better understood. While economics and ability may be important factors, the belief and support of nations may be more important considerations affecting the budget and investment in this endeavour.

As Bendiek and Kettemann (2021) would observe, nations genuinely concerned about the national security and integrity of their sovereignty even in the cyberspace would doubtless invest in these sectors to protect and assert their sovereignty. The fact that such committed financial commitments are lacking in the EU seems to indicate loss of trust in the whole process. If the fact that operational budgets for running regional cybersecurity agencies and implementing the various policy actions for attaining cyber governance are grossly lacking even with members' supports is put into consideration (ECA, 2019), then it could be safe to say that nations are yet to appreciate the importance of building cybersecurity framework into the cyberspace within the EU. As such while there are laudable initiatives and programmes for enhancing cybersecurity, financial empowerments for implementing such ideals and goals are grossly lacking within the EU.

Resulting from this pattern of reluctance in committing financially to budgets is the lack of initiatives to understudy the financial implications and implementation of the EU Cyber Security Strategy to know the exact financial needs, spendings and evaluation of such budgets (ECA, 2019). Hence not only do nations not commit financially, there is a seeming reluctance to investigate and evaluate the financial costs and implications of the policy. The fact that majority of the funding for regional cybersecurity initiatives are funded from the general budgets of the EU and member countries and not from separate budget committed to this purpose imposes other forms of challenges. For one, programmes and projects are subjected to the bureaucratic limitations of several nations and must necessarily represent national interests considerably (ECA, 2019; Giantas, 2019). While there is need to improve the economic standard of EU member countries so as to considerably invest and fund cybersecurity initiatives, there is also the need to deepen the appreciation of cybersecurity needs by member countries. According to Bendiek and Kettemann (2021), smaller nations may be suspicious of funding initiatives that undermines their national security and takes advantage of their cyber vulnerability hence committing financial to regional cybersecurity initiatives must necessarily be on a platform of national interest rather on a regional interest. While this may be nationalistic in perspective, it however affects the development of a regional cybersecurity framework.

Furthermore, the lack of investment on cyber initiatives by public institutions also affects private organisations. As findings have shown, due to the lack of access to finances, private organisations seeking to engage cybersecurity initiatives for their organisa-

tions are unable to do so resulting in the use of vulnerable and out-dated technologies vulnerable to attacks and penetration (ECA, 2019). This is indicative of the fact that while the EU Cyber Security Strategy carefully outlines the objectives and intended goals of the cybersecurity policies, in reality, there are no capacities and opportunities for implementing the specific actions necessary for attaining such state of cyber resilience. The report by the ECA (2019) had revealed that few private organisations seeking to adhere to regional cybersecurity standards by upgrading their technical and technological systems have not been able to access loans and financial resources for the purpose thus frustrating the whole purpose of the policy in the first place. Furthermore, investment in the private sector for the purpose of enhancing technical and cyber innovations to build the overall cyber infrastructure and cybersecurity capacity of the EU and EU member countries are largely lacking (Pâris, 2021; Myers, 2020). The EU therefore faces a double problem of not being able to encourage the upgrading of the private sector which drives technological innovations. In comparison with the United States of America, considerable financial budgets are annually allocated to driving cyber research and upgrading cybersecurity systems (Myers, 2020). This is directly responsible for the level of highly skilled cyber users in the country.

Attaining any form of security, whether human, national or military, requires considerable commitment to financing laudable security initiatives. In the same vein, the success of the EU Cyber Security Strategy is closely tied to the financial commitments of member nations so that specific measurable and time-bound evaluation can be possible to ascertain the success or otherwise of cybersecurity strategies. With the current analysis and state of budget funding and spendings for the implementation of the regional cybersecurity policy however, the goal of cyber governance may not be achieved and timely so. But boosting funding from member countries and institutions must necessarily result from a harmonious consideration of the needs for building cybersecurity in the region. Also considerable efforts must be dedicated to analysing and outlining the specific budget needs and financial commitments needed by nations to see the successful implementation of the cybersecurity strategy. As it is, the fluctuating and inconsistent funding patterns of the Cyber Security Strategy by member countries may not be able to field programs as building technical and technological capacities of member nations, encouraging research in cyber technology, developing organisation-specific guidelines and cybersecurity awareness across the EU region (Brady & Heinl, 2020; ECA, 2019; Giantas, 2019). These initiatives require constant funding and budget allocations espe-

cially as cybersecurity is increasingly becoming the new domain of national and regional security. But all of this is dependent on the level of trust member countries have in the regional cybersecurity governance framework.

Also considerable attention on the private sector is important for enhancing the prospects of developing cyber skilled experts. As the ECA (2019) report indicates, although the EU's research and innovation sector is considerably robust in its research and findings, there are hardly any practical implications to match this level of robustness in research. This indicates therefore that not only is investment in research necessary but there needs to be considerable investment in innovations within the cyber sector of the EU. Public and private organisations showing interests in research and innovations require adequate funding from member countries and the international institutions within the EU to enable deeper research and innovations into cyber technologies that would be necessarily complement the ideals of the cybersecurity policies. One of the benefits of this dimension to implementing and attaining cybersecurity is that research and innovations from this end would be custom made to reflect the needs of the EU and her member countries rather than depending on existing technologies that gives provision for loopholes and access by the manufacturing nation.

Therefore adequate and consistent funding from member countries cannot be overemphasised for the goal of attaining cybersecurity in the region. Closely connected to this is the fact that spending programmes for the EU Cyber Strategy are managed by different parts of the Commission duplicating sources of funding. This is further complicated by member-States' co-financing method which necessitate other levels of multiple processes for accessing funds. Accessing scarcely available funds is difficult enough, the duplication and multiplicity of financial sources for cybersecurity purposes makes the whole implementation process a bit complicated so that definite and timely projects are delayed (ECA, 2019). While multiple source of funding is important for fast-tracking the implementation of certain vital aspects of the Cyber Security Strategy, the lack of convergence of these multiple sources to foster harmonious distribution and administration of these funds have only complicated the funding processes for cybersecurity projects at the regional level. As indicated by the European Commission (2020) considerable efforts have been targeted towards achieving a coordinated funding system as well as cyber defence budgets, it remains to be seen however how these spendings have translated to practical security in the cyber space.

v. Political and Technical Limitations of the Cyber Security Strategy

The fact that the Cyber Security Strategy is not a legally binding document that requires strict adherence and implementation from member States, also presents a major challenge to the attainment of cybersecurity and cyber governance in the EU region (Backman, 2019; Kovács, 2018). Although a regional policy, there is no force of law to ensure that the recommendations are strictly complied with across the EU region. This is largely because the policy can only be implemented out of goodwill and recognition for the nature of threat posed by ill cyber users. Also the authority of the EU does not extend to countries beyond Europe to guarantee similar adherence to cybersecurity enhancing codes and strategies that protects the cyberspace of European users (Sterlini et al, 2019). This limitation poses a problem because cyber violations and threats can originate from any country willing to engage cyber confrontations with EU member countries. Technically the regional policies are recommendations to member countries to upgrade and develop their cybersecurity infrastructure. This technical and political limitation therefore makes proper implementation purely of these policies at the disposition and prerogative of the nation concerned. Fully complying with these directives is a matter of choice and interests and not a binding rule for member countries hence adherence is largely intermittent and unreliable.

The varying reports and slack in implementation of the policy as well as the lack of adequate funding and other implementation issues arising from nations can be directly related to the fact that nations are under no obligations to adhere strictly to these codes. Thus although the policy framework provides the platform for achieving cybersecurity and ensuring cyber governance in the EU, the legal status and authority to see to the implementation of this is not guaranteed. Also as findings from the study indicates, threats on the EU cyberspace is not only limited to the political interaction and activities of ill cyber users within the EU but from beyond (Myers, 2020; Lațici, 2019). Indeed EU countries have been reported to partner with skilled hackers and cyber experts outside the region to perpetrate attacks and other illegal cyber operations with European targets (Pâris 2021; Lațici, 2019). While this is a constant fear however, the Cyber Security Strategy politically and technically does not apply to other nations and cyber users beyond the EU and hence does not restrict other users of the internet from carrying out their illegal activities especially those targeted at EU cyber networks. This presents a challenge because while the EU still attempts to arrive at a secure and well governed

cyberspace, the loopholes and slow implementation process of achieving this goal continually opens cyber users to cyber-attacks from outside users.

With no form of restriction or adherence to any code limiting illegal cyber activities, it is likely that cyber threats in the EU cyberspace will experience continual growth in the coming years. The policy however cannot stop these threats especially when they are politically motivated. The challenge therefore is for a coordinated implementation of cyber policies that guarantees or presents a safe cyber haven. These two limitations present a challenge to the attainment of cyber governance and cyber peace as envisaged by the EU Cyber Security Strategy. For one, there is a lack of sincere coordinated and dedicated approach to implementing the various recommendations and strategies outlined by the various Cyber Security policies within the EU while on the other hand there is a technical and political limitation on the jurisdiction of the policies which drives cybersecurity in the EU. Considering that the policies do not have the necessary legal weight and stature to command compliance and obedience from her member countries and also to restrict the level of cyber-attacks and threats directed at the EU member-States means that attacks and threats are likely to continue unabated with little restriction and cyber resilience.

The result of the political limitation is evident in the slow implementation and attention cybersecurity and cyber defence strategies are accorded by member States especially those who are politically and economically less advanced. As Jayakumar (2020) observed, the level of threats directed at EU countries necessitates a conscious and committed effort to building regional cyber resilience and defence infrastructures. And while the EU has made plans for these, the policy in itself does not guarantee cybersecurity or cybersecurity governance as it is not automatically implemented or considered a forceful need by some nations. Furthermore, the political interaction and organisation of the EU cybersecurity structure require more conscious and committed investment of financial and personnel resources to be able to harness and implement the policy recommendations. This factor is important in the absence of a legally binding document to stimulate committed obedience and compliance. With the current state of the Cyber Security Strategy, only nations genuinely and deeply concerned with cyber-attacks and conflicts in the cyberspace as it affects their national security and infrastructure may commit considerably to the implementation of the recommendations of the EU Cyber Security Strategy and other similar policies. For others who may not feel exactly deeply threatened by the menace in the cyberspace, solidarity and regional concern may be the

motivation to support such policy but even at this, the attention may only be minimal and not the deep and committed approach necessary for instituting and gradually building cyber resilience and cybersecurity systems into national cybersecurity infrastructures.

When the consideration of the technical and political limitations of the policy is put into consideration, the need to be more strategic and concerned with developing cyber defences and governance strategies is presented before member-States. Put more succinctly, whether or not EU member countries are committed to implementing cybersecurity strategies and defence mechanisms, cyber threats and attacks especially politically motivated cyber confrontations are likely to grow in the nearest future. Building and developing strategic regional cyber defences across member-States however makes this pervading threat manageable but more devastating in the absence of these defence mechanisms. While the EU has also championed programs and projects for global cybersecurity, these initiatives which are long term approach to cybersecurity do not necessarily guarantee enhanced cybersecurity initiatives within the EU region. The only basis for attaining such sophistication and resilience as envisaged by the EU is the unaltered and deliberate implementation of the various policy documents on cybersecurity. This factor therefore presents a major challenge that must be appraised for the EU Cyber Security Strategy to receive required authority and legal basis for implementation. For some nations and key players, as long as the Cyber Strategy does not possess the force of law, compliance and implementation will not be forceful or total.

Existing grievances and political interactions among countries may continue to affect the level of adherence to these cyber policies. Much more diplomacy may need to be in place to guarantee compliance level. This also affects the commitment of funds and other resources to the cybersecurity goals. As implied by this study, the political interaction of EU countries coloured by subtle struggle for supremacy and sovereignty does more to adversely affect compliance level than it enhances it. With persisting suspicious relations and perceptions of vulnerability to the technological power and sophistication of nations, there may be continual systematic disregard for regional cybersecurity policies which are viewed as regional control documents (Bendiek & Maat, 2019). The alternative may be not only addressing diplomatic relations among member countries but also upgrading existing policies to legislations with binding force on member countries. Like other computer security and technology laws and legislations guiding the EU, the cybersecurity policies may yield more positive results and achieve more success in terms of

endorsement and implementation when they are updated to the status of law. This will consolidate global efforts championed by the EU to further strengthen the cyberspace and build resilience into cyber technologies thereby enhancing cyber governance in the EU.

Although it is granted that there may always be serious threats and vulnerabilities on the internet space due to the boundless and largely ungoverned nature of the internet space, these threats as it relates to the EU cyberspace can be better tamed and eliminated when stronger legislative actions are adopted by member countries in the region. By going beyond recommendations and general objectives for member countries to achieve/attain, laws and legislatures will enhance the rate of implementation, the grievances and political hostility among countries notwithstanding. By not providing any sanctions for non-implementation of these policy strategies, loopholes are created for nations to implement any of the strategies according to preference and at whatever time suits them (Lațici, 2019). Furthermore, timeliness is important in this discourse of implementation. The EU Cyber Security Strategies must also necessarily involve specific timelines within which member countries must have implemented recommended and mandatory steps for achieving cyber governance. The combination of the possibility of sanctions and the upgrade of the existing policies to the status of laws and legislations may do more to enhance the timely implementation of the Cyber Security Strategy as well as enhance the chances of achieving cyber governance in the EU cyberspace.

In summary therefore the political and technical limitations of the Cyber Security Strategy policies provide sufficient grounds for the slow and in some cases, non-implementation of the required cybersecurity strategies and recommendations. As a matter of nation and regional security, there is need to strengthen the legal weight of existing policies for stricter and timely compliance. What is obtainable among nations whereby implementation is solely dependent on not only the ability but the prerogative of member-countries undermines the regional cybersecurity aims and objectives. This factor has necessitated the ECA (2019) report suggest that the Cyber Security Strategy is at best a document expressing wishes for regional cybersecurity than it is a legal guideline for attaining the stated vision of cyber governance and cyber peace among EU countries.

vi. Exploitation of Existing Political and Technical Loopholes

A factor that is easily overlooked in the consideration of challenges of the EU Cyber Security Strategy is the possibility for exploiting political and technical vulnerabilities created by key State players in the EU. While technical challenges are considered, the implications of the political atmosphere and tensions between EU Member countries are hardly considered in the pursuit of regional policies. However this analysis discourse identifies that a consequence of the existing political and technical vulnerability between nations in the EU is the possibility for exploitation by hackers and other ill cyber users. As indicated by findings from this study, the relationship between countries within the EU has not been very cordial hence adherence to regional policies which do not have the force of law may be a bit difficult. In an atmosphere where necessary policies and strategies needed for building cyber resilience and defence is lacking due to political and philosophical differences, several loopholes are created at the national and regional levels for attacks. These loopholes can be traceable to several courses of actions for cybersecurity taken by member States, organisations and citizens different from recommended best practises as stated in the EU Cyber Security Strategy. Failure for instance to implement the recommended cybersecurity measures and defence mechanisms at the national, organisational, and individual levels may create opportunities for attacks.

As findings have shown, some organisations and institutions out of grievance and concerns that regional cybersecurity measures do not take their interests into consideration had neglected implementing them against regional standards (ECA, 2019). Also challenges relating to the non-inclusion of cybersecurity enhancing policies and strategies in the decision making boards of several organisations in the EU region have also been identified (ECA, 2019). These reports do not present an optimal or coordinated approach to improving regional cybersecurity standards even though several regional cyber agencies and institutions have been set up to assist nations achieve cyber resilience. Nations, organisations and individual users of the internet space who downplay regional steps and recommendations for improving cybersecurity and cyber resilience as a result of this neglect stands a chance to be exploited since cyber vulnerabilities are not addressed and taken seriously for whatever reasons. Also the air of suspicion between the various members of the Commission due to past hostilities and political differences further compounds the political atmosphere needed for successful implementation of re-

gional security and cybersecurity measures. With such unstable atmosphere created, adversarial elements seeking to carry out targeted attacks on member countries and the EU at large are capable of taking advantage of the vulnerability created to launch attacks which may go undetected. For instance, fundamentalists and extremists seeking to recruit sympathisers within the EU cyberspace can be easily successful due to the inability to update and upgrade cybersecurity technologies at the national and institutional levels as revealed in the case of Junaid Hussain Abu Hussain al-Britani (Jayakumar, 2020) who was recruited as an extremist in the UK even without going to any Islamic countries. He successfully launched cyber-attacks against the UK and was also instrumental in the development of several computer programmes and software that were used to disrupt internet activities within the UK and the EU even after serving jail terms.

Like him, young computer experts who eventually fall victims of cyber-terrorism may be forced to undertake actions that undermine the security of EU member countries at large. With persistent threats as this, cybersecurity breaches may be more frequent especially as security measures and technologies are not given a priority due to existing discords and suspicion of such initiatives. In such an atmosphere, the vision of the EU Cyber Strategy and other cybersecurity enhancing policies may be grossly affected as penetrations by extreme elements and ill-intentioned cyber users may succeed in recruiting more sympathisers across the EU as visible in the recruitment of Junaid Hussain. The sympathiser cyber-attack on the UK Healthcare institution by the Tunisian Fallaga Team in solidarity with Syria and in protest of the EU's role in the prosecution of the war are indications that recruitments and radicalisations as well as sympathetic identification with extremists groups are possibilities that confront the EU cyberspace and Cyber Security Strategy policy. Therefore the political differences and air of suspicion visible among member countries that has resulted in the patronisation of black-hat hackers to carry out threats against some other nations as visible in the NotPetya attacks allegedly carried out by hackers in Ukraine with links to Russia are indicators that continue to threaten the over cybersecurity goals of the EU even though they are not openly discussed or addressed in cybersecurity policy discourse and documents.

Not addressing these issues however does more to undermine the threat levels posed by the adverse effects this air of hostility presents to the overall cybersecurity, cyber peace and cyber peace goals of the EU Cyber Security Strategy policy. Since there have been evidences of nations like Russia patronising black market hackers and equipping them with sophisticated State-owned resources to launch attacks against fellow Europe-

an countries, it is only safe to assume that other nations may be compelled to take similar course of action in protection of their cyber infrastructure and national security especially in the case that they lack the wherewithal to adequately protect their critical infrastructures in the main time. This possibility therefore affects the prospects for total implementation of the regional cybersecurity policies that seeks to update and improve regional cybersecurity measures by adhering to recommended guidelines for member countries. The point here is that while member countries may all be concerned with protecting their cyberspace and critical infrastructures against pervading cyber threats, they may not be quite comfortable with implementing guidelines stated by regional cybersecurity agencies out of suspicion for the hidden agenda of nationalist cyber experts. As such either these initiatives are ignored or underplayed as discovered in the study of Bendiek, Bossong, and Schulze (2017) or they are mildly implemented at various levels just to better check the incursion and possibility of intrusion by ambitious countries.

The adversarial effects at the regional level however is that the EU region is by this inaction of member countries and individual users, exposed to cyber breaches and attacks by external parties seeking to take advantage of existing cyber loopholes. The fact that majority of the devastating cyber-attacks and threats that have occurred in the EU cyberspace are State-inspired and politically-motivated is instructive of the nature of relationship and interaction that exists between member countries at least at the cyber level (Jayakumar, 2020; Giantas, 2019). Furthermore enhancing cyber capacities and cyber resilience necessarily involves a singular regional political vision where members and citizens are convinced and persuaded about the importance and need for a particular course of action. As it is in the EU however, this vital ingredient is missing, no less due to the diversified political views than to the political ambition of some nations within the union. Achieving and pursuing this singular vision is therefore made more difficult even though member countries agree on the need to attain this vision. The diverse forms of approaches and non-coordinated implementation of the EU Cyber Security Strategy policy adopted by member nations as indicated in this study is also grounds for varying results that may not help the attainment of the regional cybersecurity and cyber resilient objective. Cyber growth and development with such implementation styles will be unsafely diversified.

This diversification in the level of cyber technologies of member nations will also means that some nations will be more vulnerable to cyber threats and attacks than some others. More importantly, loopholes for penetrating naïve cyber users within the EU cy-

berspace would have been created by this unequal growth and development in the region. A second concern and a major one nonetheless is that avenues will also be created for terrorist groups who are increasingly turning to cyber technologies and the internet space to perpetrate their activities. This is more recently indicated by the show of support for the Taliban government of Afghanistan by the Russian government. Implied in the display of public support for this extreme fundamentalist regime is that resources for the prosecution of the religious extremism and fundamentalism represented by the Taliban government will be provided by the Russian government. With such prospects, the overall security and cyber integrity of the EU is further put to test and alert since the Commission was a major supporter of the Western stint in the nation of Afghanistan and ill sentiments shared for the US are also expressed to the EU and her member countries. As such while efforts are geared towards enhancing national and regional security as well as cybersecurity around the EU, the support of Russia with her sophisticated and advanced cyber technologies may prove to be a major threat to the overall aim of cybersecurity and cyber governance as related by the EU Cyber Security Strategy.

To a large extent this confirms the suspicion of Russia as a major threat to the cybersecurity and regional security of the EU by smaller nations who have felt the aggressive tendencies of Russia in recent times. As such adopting a cybersecurity policy that is on the one hand supported by nations like Russia and on the other hand disregarded by their political ambitions and alliances would be viewed suspiciously by these nations, resulting in either flawed implementation or disregard for the policy altogether. There is therefore need to address the philosophical and political questions surrounding the interactions of fellow EU countries for regional policies on cybersecurity to have strongholds and unbiased implementation across member countries. Meanwhile the recent development in Afghanistan and its implications on Western territorial and cyber security must not be overlooked especially in a time when Europe is still trying to grappling with her own political peculiarities and the withdrawal of Britain from the EU.

No doubt these developments must have some effects on the overall plans and visions of the EU especially in consideration of the fact that majority of the funds invested in the regional cybersecurity initiative were received from the UK and few other developed countries within the region. Managing these political developments for optimal results are necessary for the attainment of cybersecurity and cyber governance in the EU region because allowing broadening and spread of vulnerabilities on the grounds of political differences only means more devastating effects for the region. Therefore alt-

hough not stated in the EU Cyber Strategy, the political climate and interaction among member countries to a large extent determines the success of implementation. In the current state however, the political interactions among some member countries does not allow for the successful implementation of the cyber policy rather it encourages the intrusion and exploitation of security vulnerabilities in the EU cyberspace.

In summary, dealing with the political climate especially as it relates to the activities of Russia in the EU cyberspace is important for addressing national and regional loopholes. Although not limited to Russia, there is the need to address the political interaction and differences among member nations which serve as springboard for the occurrence of ill-intentioned cyber users. Ranging from the activities of hackers to extremist groups and other e-financial fraudsters, the attainment of cyber resilience and cybersecurity against these threats are better projected in an atmosphere of collaboration and healthy political interaction void of suspicion.

vii. Less Cybersecurity Awareness and Skills by Major Population Of Cyberspace Users

Although findings from the study has indicated that cyber threats and hackers are a major concern in the EU cyberspace for internet users of all categories, a closer analysis of findings would show that this was this case because majority of cyber users were unskilled in the cyberspace and hence were vulnerable to attacks. While considerable attention has been paid to building cybersecurity technologies and systems, the implementation of these technologies is solely dependent on the skill and expertise of the users (Myers, 2020). This has particularly been identified as a challenge because as findings show, even though organisations and institutions would implement or acquire modern cyber technologies to enhance cybersecurity, the launching and use of these technologies is largely dependent on the know-how of employees. And majority of organisational staff even in technology companies are not all highly skilled in cyberspace and internet navigation. This raises a fundamental concern for the institutionalisation of cybersecurity measures in the EU cyberspace because cybersecurity and cyber governance is dependent on the technical and internet knowledge and skills possessed by the actors engaging cyberspace. In fact, with this challenge, cyber governance seems a much easier task compared to engaging cybersecurity measures.

In the absence of necessary skills to implement the defensive strategies needed to protect a computer network, the efforts of the various stakeholders would have been in vain hence the role of cybersecurity awareness and education is considered in the EU Cyber Security Strategy policy. The goal is to encourage cyber education and awareness by dedicating considerable programmes and projects to raising the cyber skills and awareness of EU citizens (Myers, 2020; ECA, 2019; Carlton & Levy, 2017). While this is provided for in the policy documents however, implementation has not been reported to follow the same enthusiasm and vigour as the policy. Cases of data bridges and vulnerabilities to all kinds of online scams and fraudulent activities have been recorded in EU countries in recent times even with cybersecurity awareness being a necessary part of the regional policy. As reported by the ECA (2019), this can be traceable to the fact that implementation of this programme especially in the private sector has not been particularly reflective of the regional cybersecurity policies. The ECA report also noted that cybersecurity initiatives have not been given priority implementation across some organisations and institutions across the EU thus retarding and reducing the prospects for developing the skills and awareness of employees on cybersecurity and cyber technologies. To be fair, there have been several institutional and professional programmes for developing cybersecurity skills for all categories of cyberspace users both online and offline (European Commission, 2020; Mortera-Martinez, 2018). These programmes are targeted at professionally and skilfully increasing the capacities of internet users so as to be prepared and enhance cyber resilience in case of attacks. However, a vast majority of active internet users across the EU are largely unaware and unskilled of these programmes either due to ignorance of the pervading threats on the internet space or lack of interest in the subject. The result therefore is that both in the private and public sectors, internet users are still very vulnerable to internet-based attacks and threats.

This vast pool of uninformed and unskilled internet population both in the private and corporate sectors presents huge source of vulnerabilities and attacks to private and organisational websites with little resistance because hackers and other ill-intentioned actors on the cyberspace located within and beyond the EU are continually developing their cyber skills to avoid detection (Antunes et al, 2021; CyberPeace Initiative, 2021). On the other hand, reports from private and public organisations across the EU are indicating both reluctance and inability to develop cybersecurity awareness and education tools for employees and citizens even with the level of awareness on cyber vulnerability raised in the region (ECA, 2019). This does not only affect the overall aims of the cy-

bersecurity policy of the EU but it also affects the capacity of the EU to produce sophisticated internet and cyber defence infrastructures in the nearest future. Importantly, the cyberspace is continually flooded with different categories of internet users employing the technology for different reasons and due to the fact that daily business services and activities are increasingly carried out through the internet, cyber education and expertise skills is a growing asset that nations across the globe are coming to appreciate and encourage. In climes where vulnerability to attacks on the cyberspace have been more likely than others, efforts are been made to not only develop cyber defence technologies but also improve the capacity of citizens in relations to cybersecurity. This factor more than just acquiring foreign defence cyber technologies tends to determine the level of cybersecurity and cyber governance that can be achieved within a nation and as the case may be, a region.

As this study therefore considers it, the inability to drive considerable cybersecurity awareness and education schemes and programmes in line with the goals and objectives of the regional cybersecurity strategy only negates the vision of the policy document. Although considerable attention is invested in developing defensive cyber technologies, similar attention and commitment may need to be invested in other sectors for consolidated results. The series of cyber-attacks directed at EU nations have seldom targeted military and defence bases but the majority have been targeted at the economic and government cyber infrastructure which possess less sophisticated and expert levels on cyber technologies. This may be a pointer to the fact that not only in military defences, but also in other public and economic sectors of the nation, efforts at developing the cyber defensive technologies and manpower is needed to improve cybersecurity. Also attaining cyber peace in the EU cyberspace may not necessarily mean the cessation of violence and confrontation among EU countries both within and beyond the cyberspace but the ability to identify and address cyber threats/attacks when they are arise and take down such without much damage to regional and national security.

This would mean that nations must necessarily be conscientious about implementing cybersecurity and defensive technologies. This is because attacks are likely to arise from any external actor and be directed at any sector of interest dependent on the goal and objective of the attacks. If citizens and employees across public and private institutions therefore are not considerably skilled in cybersecurity and defensive systems and procedures, the goal of the regional cybersecurity policy may be defeated in the long run. Apart from taking crash courses on cybersecurity, there is also the need for deliber-

ate development of a cybersecurity population with special considerations to developing experts for all sectors. As findings have shown although most cyber users are daily engaged in the internet for different reasons, little appreciation and understanding of defensive strategies against threats and vulnerabilities are lacking amongst this vast population of internet users. For some persons especially younger users of the internet, the pervading threats and vulnerabilities identified and discussed by several reports and studies (Giantas, 2019; Paget, 2013), are distant realities which do not apply to them. For smaller businesses and enterprises, the sentiments are largely the same, reflecting the position and fact that cybersecurity and cyber threats are still vastly viewed as non-existent or insignificant in private affairs (Giantas, 2019).

This situation thus reduces the motivation and tendency for individual and small business enterprises to adopt and engage the vast cybersecurity resources made available on the internet especially through the EU policy on raising awareness and education. The implication of course is that although more internet users may be recorded across the EU region ranging from private to public users, the awareness level and expert skills on the internet security systems are quite low. And with such a phenomenon, there can be hardly any effective implementation of the Cyber Security Strategy. As long as the subjects of cybersecurity and cyber governance sound unfamiliar and distant from persons, the willingness and need to build capacity in the field may remain low. Indeed cyber users may not be compelled to take a career in cybersecurity and cyber defence mechanisms but as findings from the United States have also indicated, providing platforms for the development and establishment of cyber experts and cyber technologies not only helps to enhance national security but provides a vast market for cyber defence both in technological and human resource (Myers, 2020; Gilligan & Pardo, 2020). Effective translation of the aspirations of the EU policy on Cyber Security depends considerably on the technological resource of cyber users in the various EU member countries. The tendency to reserve expert resources for national security enhancing systems was rightly recognised by Jayakumar (2020), Giantas (2019) and Meer (2015), but this may be because there is limited expert manpower on cybersecurity at the national level before considering regional concerns.

Further compounding the challenge on the attainment of cybersecurity within the EU through the EU Cyber Security Strategy is the fact that a good population of individual cyber users who display interest in cyberspace and cyber defence systems are freelance individuals whose expertise may constitute more threats to ordinary users (Jayakumar,

2020; Myers, 2020). This is especially the case because most highly skilled cyber users are either used to perpetrate threats in the internet space or are champions of causes in the internet space that may constitute more threat than security to the EU. In the same vein, the growing trend in the internet space that makes crime-as-a-service is increasingly taking the Western cyberspace so that cyber users are poised to developing their cyber skills so they can be used or patronised to make devastating and dangerous assignments by the numerous groups seeking to carry out major attacks on the EU and her member States (Jayakumar, 2020; Brady & Heinl, 2020; ECA, 2019). This growing concern in the EU cyberspace poses a serious challenge to implementation of the Cyber Security Strategy because majority of the internet users are young persons whose opinions and philosophies are still being formed and influenced largely but internet contents.

As Jayakumar (2020) rightly observed, the sense of importance for some of these very young cyber users is closely tied to their identification with a political or social group on the internet space and their ability to carry out a task or assignment in furtherance of the corporate cause. With little concern to the implications of these attacks on national and regional security, these vulnerable users can be used to perpetrate attacks on the EU cyberspace with no less devastating effects. Therefore there is the challenge of not only building cybersecurity awareness and education among citizens but also the greater concern of monitoring and ensuring the right use of cyber skills by citizens. The irony of the awareness level of European cyberspace users at least in some countries, is that while considerably skilled cyber experts do not necessarily provide their services to the government and public institutions, majority of those who work for corporate public and private institutions do not possess the requisite knowledge and awareness to prevent cyber-attacks and engage defensive measures during attacks. This is visible in the attacks on healthcare and banking sectors as recorded in the WannaCry and NotPetya attacks where hospital and banking facilities could not repel or even detect the presence of malwares deployed by hackers.

Such a situation puts the implementation of the EU Cyber Security Strategy at risks since the majority of persons who possess the requisite skills and knowledge to engage cyber defensive measures are more likely than not to be victims of emotional manipulation for political and ideological reasons. Even for law enforcement agencies, the lack of trainings and awareness on cybersecurity measures have been identified (ECA, 2019) with obvious implications on cybersecurity. In an era where sociological crimes are increasingly giving way to internet based crimes, the ability of existing law enforcement

agencies in the EU to dedicate significant resources to developing the cyber skills, awareness and education of various operatives across the region is important. Reports of less technical trainings and underrepresentation of cyber related courses in some universities across the EU is indication that raising the awareness and expertise on cybersecurity still needs greater attention and deliberations (ECA, 2019). While professional short courses and on-the-job trainings are important to keep employees abreast of the current realities and technologies for protecting data on the cyberspace, deliberate investment in the academic education of students especially on cyber technologies and cyber defences are more long term approaches that are likely to yield more productive results in terms of cybersecurity and cyber resilience.

This is because pursuing careers in cyber defences and cybersecurity fields are more likely to result in the development and innovation of cyber defence and security technologies without foreign influences. Furthermore, this may likely enhance the attainment of the EU as a cybersecurity and cyber defence technology manufacturer thus establishing the EU as a major global cyber player as against its current status (Pâris 2021; ECA, 2019). In all, the various dimensions of cyber awareness and education in the attainment of cybersecurity and cyber resilience cannot be overemphasised. Attaining regional cyber governance at least must necessarily involve a pervasive degree of cyber aware and skilled citizens. Although this may also constitute regional concerns in terms of ensuring compliance and control of the activities of such an expert population, it is all the same a requirement for becoming cyber resilient. The various programmes aimed at raising awareness and skills of EU security agencies and citizens must therefore necessarily be encouraged and nurtured till they yield the required results.

5.5. Theoretical Discussion of Findings – Nodal Security Governance

As the nodal security governance framework used for the study suggests, the EU has served as a non-governmental institution dedicated to driving cybersecurity governance within the region amongst other economic and security purposes. This does not mean however that it does not draw support from existing governments and security institutions to achieve her purpose, rather the EU operates on the strength of the constituent members as far as their technologies and resources are concerned. The crux of this framework as it concerns cybersecurity governance is non-hierarchical and a priori structure of governance within the structure that makes it possible to embark on bal-

anced policies and approaches to cybersecurity governance with the interest of both private and public sector participants. As such the EU has succeeded beyond the capacity of a single nation to drive policies and diplomacies that focus on enhancing national and regional strategies for cybersecurity among member nations within the EU region. As stated by Nøkleberg (2016), the four essential approaches to implementing nodal security governance frameworks are reactive strategies based on punishment, reaction and retribution of crimes related to the criminal justice system; nodal technologies for exerting influence over a course of events; nodal resources which determines the level of implementation of technologies for enhancing security governance; and lastly nodal institutional structure for the mobilisation of resources, mentalities and technologies for the common goal. These anchors are used to analyse the findings of the study.

First is the establishment of reactive and retributive strategies for responding to crimes and criminal justice systems within the nodal security framework. Without this strategy there is no law and order in the system to guarantee adherence and commitment to the overall stated standards. This is largely missing in the execution and implementation of the EU cybersecurity framework and the European Commission at large. Although stated and implied in various provisions and objectives of the Cybersecurity Security Strategies of the EU, there have been no reactions and responses in the form of punishments to nations that have continually violated the stated rules of engagement in the EU. For one, Russia has continually violated the security and sovereignty of nations both within and without the cyberspace but have been subjected to no decisive form of sanctions and punishment at least to deter future occurrences from it and other nations with such ambitions. Importantly, although the EU Cyber Security framework serves as a guide, the European Commission wields the necessary resource and authority to enforce such justice strategies within the region. The failure to do this has made the EU appear weak in her implementation strategies of criminal justice in her region. As a key player in regional and global politics, the selective administration of justice by the EU, especially when the developed and developing dichotomy between nations are put into consideration, makes it appear biased in the administration of justice.

Sufficient attainment of respect and adherence to the Commission's Cybersecurity code must necessarily involve the ability to command compliance with the stated codes as well as deterrence from violating these codes. And one of the tools according to the nodal theory for actualising this is the definite implementation of sanctions and punishments for violators whether or not they are State-actors or non-state actors. Therefore by

not addressing the flagrant disregard and disobedience of regional values stated by the EU, more grounds and justifications for violations are created across the EU. Perhaps evidence of this is the disregard of China for regional and global trade standards in trade ties with European countries. In an attempt to expand her technical and technological market, China has repeatedly violated global trade standards with significant impacts on the EU but surprisingly has not received any definite sanctions from the EU for such violations aside public statements. This can be arguably traced to the EU's system of slow reaction to violations within the continent. While the EU in partnership with NATO allies has taken decisive actions against governments that tend to violate global political and governance standards, the same energy and dedication is largely missing in dealing with violators of regional values and standards in cybersecurity. Therefore this very important step required for the effective implementation of cybersecurity, cyber resilient and cybersecurity governance initiatives is absent in the EU nodal framework. This in no small way affects the sustainability and efficiency of the framework. As provided for in the existing policies, there must now be decisive approaches and definite actions by the EU to ensure compliance with regional values by member nations and trade partners especially technological and cyber trade partners. This is necessary to further strengthen the nodal network on cybersecurity.

Secondly the nodal security governance framework hints on the technologies or methods for addressing events as they occur. These are rules of engagements and policies to drive the sustainability of the nodal network in the face of several occurrences. The EU has considerably made sufficient strides in this as several policies and legislative frameworks for guiding the regional partnership have been developed over time. These frameworks have helped to establish national technologies and systems for addressing similar cybersecurity concerns in the various member nations. For instance both the private and public sectors of nations have set up organisational and institutional policies that incorporate cybersecurity consciousness into employees and individual cyber users. This has enhanced the cyber awareness and security risks prevalent in the cyberspace to public and private users of the internet space, as such caution and deliberate carefulness consciously deployed by several users of the internet space. Furthermore, the EU has succeeded in enhancing cybersecurity skills among several nations by encouraging cybersecurity training and education among employees and other categories of the internet space and also enhanced research and innovation investments of nations within the EU. These methodologies and technologies are equipped with teaching

internet users how to respond to cyber-attacks when they occur as well as how to deter these attacks from occurring in the first place.

Another vital success of the EU in the development of methodologies and technologies of cybersecurity governance has to do with the designation and definition of roles of the various cybersecurity actors in the case of prosecuting violators and administering justice. Initially there were several hiccups bothering on the prosecution of cybercriminals especially across national boundaries and territories. With the consideration that cybercrimes and cyber-attacks could involve transnational and foreign identities thus leading to conflict of interests in prosecution, the EU fostered designation of approaches and roles for member nations to eliminate judicial and criminal justice barriers and conflicts. The aim according to the nodal framework is to enhance the workability of the EU framework in the course of events so that complications in implementation do not hinder the actualisation of the frameworks. Thus, workability of the cybersecurity policies as it concerns criminal justice, cyber-attacks, resilience and effective cyber governance are relatively covered by the EU cybersecurity frameworks. While there are still grounds for improvement, existing policies at least provide prescription for actions in the event of cyber-attacks and prosecution of violators. As seen in the previous section, the implementation of these strategies rather than the provisions requires more attention than currently devoted to it.

Thirdly the nodal security governance framework discusses the importance of resources in providing the necessary technologies for enhancing security from the existing networks. This has been a little complex in the EU cybersecurity agenda as findings indicated that although member nations possess different capacities, commitment to the regional cybersecurity network has not been reflective of the dedication to the actualisation of cybersecurity governance goals. Reports had indicated that the US committed more financial resources to developing and attaining cybersecurity than the EU region combined. This lack of financial commitment to the implementation of stated regional cybersecurity aims and objectives have resulted in a slow implementation as well as flawed implementation of the necessary strategies for attaining regional cybersecurity governance and cyber resilience. The concerns and rationale for this non-committal of resources to the regional agenda have been identified above as resulting from political interactions and hostility among member countries. The distrust and atmosphere of suspicion that underlay interactions and diplomacy among member countries has further coloured the commitment of members to the success of the cybersecurity strategies. For

one, the fear of being vulnerable to the technological and cyber sophistication of politically domineering countries within the region drives non-cooperation at least at a regional level. Countries as identified from the study are more likely to engage resources for national strategies than in partnership with nations that threaten their national sovereignty and political existence, as such commitments are mostly restricted.

Another dimension of the resources factor in the EU cybersecurity agenda is that due to the fact that resources are jointly funded by nations and the EU, the terms for accessing these funds from national institutions are sometimes tailored to reflect national interests rather than regional interests. This serves as an opportunity for member nations to drive nationalistic interests at a regional level because financial resources are considerably drawn from their coffers. This therefore compounds the existing state of resources to the regional cause. Essentially without the necessary financial resources, there will be no efficient innovative researches or even successful implementation of cybersecurity enhancing awareness and education across academic institutions in the EU. Other laudable objectives and methodologies such as the financing of ENISA which was recently given a permanent mandate of operation within the EU is also faced with operational and running problems. This is compounded by the withdrawal of Britain from the EU whereas she was a major regional financial partner instrumental in the formation of the Commission and the mobilisation for the initiation of the regional cybersecurity initiative. This reduces the prospects and viability of the EU to meet her regional targets in the cybersecurity sector specifically as well as other sectors generally. With such shaking and unstable source of resources therefore, the EU Cybersecurity framework is bedevilled with resources challenge which are altogether essentially for practically implementing the strategies necessary for enhancing cyber governance and cybersecurity within the region.

Lastly there is the need for development of the institutional structure to guide the mobilisation and deployment of the resources, mentalities and technologies within the nodal security governance framework. The EU Commission have tried to harness the various resources, mentalities and technologies through the ENISA and other regional cybersecurity agencies by enforcing regional policies and legislations as well as conferences and conventions based on the goals of the EU region. Subsequently various nations have come together under the platform of the EU and through the ENISA to implement the several approaches to enhance cybersecurity across the EU region. While this has resulted in some measures of success for the EU, the evidences from the study

indicates that the EU has not fully harnessed the resources at its disposal to encourage and enhance cybersecurity governance of the region. Importantly, the nodal security governance framework provides that the nodal network not only harness the resources and technologies at her disposal but also the mentalities to foster successful mobilisation and deployment. With this lens, the EU has been somewhat successful in mobilising technologies and resources even though there are obvious flaws yet to be addressed. For example the question of resources addressed in the previous section reflects that the EU still faces challenges from member countries unwilling to commit considerable financial resources to the common cause due to the pervading complicated political environment among different categories of nations. Further in this atmosphere, there is also reluctance to commit advanced cyber technologies to the regional cybersecurity goal for national security concerns especially appearing vulnerable to the threats and attacks of nations with political domineering attitudes. These concerns are however hardly addressed by the existing EU cybersecurity nodal framework which according to the Nodal security governance framework is set up to harness these resources for the cybersecurity governance of the EU region. While this concern persist however, there is root concern that seems to go unattended in the existing which bothers on enhancing mentalities.

The nodal security governance recognises the fact that nodal networks are made up of actors and stakeholders with differing ideological foundations and alignment hence a rigidly structured security governance system like the State may not be able to fully harness the resources from the system especially for security ends. This is however possible in the nodal framework as the EU and the supporting EU cybersecurity agencies. As such the EU is expected to work towards mobilising the various ideological leanings and differences resident in the European region which inform political governance and security governance for the purpose of attaining cybersecurity. The understanding is that no single political ideology or security governance strategy would be sufficient to address regional concerns particularly for vastly diversified region as the EU. Hence part of the requirements is that the EU commit considerable resources to building a synergy between the divergent mentalities and ideologies within the region for the purpose of achieving a unified goal. This does not necessarily mean pulling down or eliminating national ideologies and mentalities while elevating a rival mentality or ideology, rather it connotes driving the various views and ideologies towards collaborating within the network to achieve a single focus which in this case is the attainment of cybersecurity governance in the region. Evidences portray however that within the EU, divergent po-

litical and economic views have been allowed to thrive thus affecting the actualisation of a unified front against cyber insecurity and attacks. Nations with domineering and aggressive tendencies with grievances against the West for incursion and division of their otherwise large political empires have constantly maintained a position of hostility and aggression to otherwise smaller nations. On the other hands, nations with victimisation and vulnerability fears have also not stopped to express their distrust of the entire regional framework and its inability to protect and uphold their national economic interests. Other nationalist fears and views have erupted over time that challenges the implementation and efficiency of the EU cyber strategy. These differing views and mentalities have however not been reconciled by the nodal EU system which is supposed to drive this reconciliation and mobilisation process. The reluctance to address threatening political mentalities and ideologies that adversely affect cooperate collaborative existence has been evident with adverse implications on national and regional security governance.

The advantages presented by the nodal security governance model in the form of mobilising mentalities and ideologies for the common good must be thus harnessed for the attainment of cybersecurity governance in the EU region. Continually allowing this system of divergent views to thrive with little diplomatic efforts for steering them towards the common goal ultimately negates regional efforts at attaining cybersecurity governance. The cybersecurity concerns of the EU must therefore necessarily adopt measures to ensure unification and mobilisation of member countries' political ideologies to foster a unified front. Typical of this is the promotion of several cybersecurity perceptions and conceptualisation among member countries which affects a general region specific definition of the problem and in return makes an agreement on the specific mitigation strategy difficult. In other words, due to the fact that nations within the EU perceive cybersecurity strategies and threats differently, efforts towards mitigating these threats are diversified as nations would tend to weigh in some approaches that reflect their views than others which do not. As such equal mobilisation of technological and financial as well as political resources may not be altogether possible. But this is traceable to the inability of the EU to harness these ideologies and mentalities on which the various approaches and commitments to cybersecurity thrive. There is necessary need therefore to not only considerably understand and promote equitable mobilisation of technologies and resources of member countries but also the mentalities and ideologies of these countries to enhance a considerably unified front against cyber threats and at-

tacks. Importantly, if such a unified force is formed as envisaged so that synergy in technologies, resources and mentalities is achieved or relatively enhanced, cyber threats and cyber-attacks against the EU region would have experience relative decline.

This is likely traceable to two factors; one would be that the advanced technologies available to some countries as well as resources in others would have been made available to other nations within the region thus significantly updating and increasing cybersecurity and cyber resilience in the region. Secondly it would considerably reduce the level of cyber-attacks and threats targeted at EU countries because as findings from this study have indicated, majority of the cyber-attacks affecting EU countries on a national scale are from nations within the EU. With the right mobilisation of political ideologies however, these threats are likely to result in a downward trend of cyber-attacks streamlining cyber threats to majorly cyber terrorism and radicalism tendencies, financial frauds and other such threats. Such results are however essentially tied to the synergy between the various political ideologies within the region so resources are not poised towards combating the cyber infrastructures of neighbours but at enhancing cybersecurity regional infrastructures and enhancing deterrence and resilience in the EU cyberspace.

Therefore in summary, the EU's cybersecurity governance aim which has been embarked on since the beginning on the new millennium and continually reviewed must necessarily encourage the full potentials of the nodal security framework. To be fair, the EU has made steps in the directions and steps recommended by the nodal system evident in bringing nations together to establish cybersecurity frameworks and assist the same in various member nations. With such leadership strides in the areas of policy making and synergy building, the EU must now not shy away from the deeper level of harnessing divergent views in maintaining and upholding regional values especially as it relates to cybersecurity governance. The complete success and effectiveness of the cybersecurity strategies in the EU is directly traceable to this factor. Extending cybersecurity governance to the larger world by making Europe a safe haven for cyber activities must necessarily involve aligning the various ideologies and resources within the EU with definite stands against violations of these values. Cases of synergy and partnerships with criminal and terrorist elements to perpetrate attacks on nations and institutions within the EU must erupt decisive responses from the nodal system. The same approach must also be dedicated to deterring trade partners and nations which violate regional values and global trade standards as it relates to promoting cyber technologies.

This is important because no individual nation can possess or deploy the resources available with the nodal EU structure hence full potentials must be harnessed to deep commitment to the existing cybersecurity frameworks.

5.6. Answers to Research Questions

RQ 1 What is the conceptualisation of cybersecurity as it concerns the EU?

Findings from the study indicate that there is still a massive diversification of understanding and conceptualisation of cybersecurity as it concerns the EU. Although there are nodal cybersecurity frameworks such as the EU and within the EU, saddled with harnessing regional resources and mentalities for improved cybersecurity governance within the EU region, the various conceptualisations of cybersecurity, cyber-threats and cyber resilience influenced by the political interaction and diplomacy between member-countries serve to undermine a unilateral approach to effectively combating cybersecurity. As findings indicate the perception of cyber threats and cyber resilience among the various constituting units in the EU cybersecurity nodal framework are mostly biased and different reflecting the existential and political threats experienced by these nations. Hence some nations view cybersecurity essentially as protection from politically aggressive nations within the EU seeking to pursue their political dominance agenda even through cyberspace while others understand the phenomenon to involve threats from outside actors. In all, the study understands that the perception of cybersecurity by the various EU actors are essentially politically influenced following the history of distrust and attacks of cyber infrastructure by neighbouring countries. With this atmosphere of differing opinions and conceptualisation of cybersecurity even among scholars and experts, cyber technologies and approaches are largely biased and nationalist tailored to reflect national security needs. This of course creates a loophole for the regional cybersecurity framework as well as cybersecurity governance ambition of the EU. With no firm strategic belief in a common problem defined by its importance to the constituting parts that make up the EU, there are little prospects to the harmonisation of strategies to address these regional concerns. Therefore conceptual unification at least at the regional level is important for driving cybersecurity governance framework.

RQ 2 What efforts have the EU commission put in place to achieve cyber-peace?

The EU has also been very active and instrumental in the formation and establishment of regional and global strategies and networks for developing cybersecurity and cyber resilience among member countries within and without the EU. The formation of the regional cybersecurity agencies as the ENISA and the creation of cybersecurity units in existing national law enforcement agencies across EU member countries directly traceable to the policies and diplomacy of the EU to improve cybersecurity, cyber resilience and drive cyber governance. However in terms of cyber peace where diplomacy and not just cyber-diplomacy is needed to address underlying political sentiments influencing the attitudes, behaviours and reactions of member countries towards implementation of cybersecurity policies and legislations are largely left unattended. For example while the EU focuses on ensuring cybersecurity diplomacy is incorporated into various Cybersecurity policies over the years, there is little provision for addressing the feeling of vulnerabilities expressed by smaller nations whose sovereignty are threatened by nations like Russia and China who tend to aggressively violate national and regional diplomatic standards to win over European nations. The success of China's trade and diplomacy in Western Europe for instance has been significantly traced to her obvious disregard for global trade standards especially within the EU. Similarly Russia which has been severally implicated in virtually every case of cyber-attacks on national cyber infrastructures across countries both within and beyond the EU have not had any definite sanctions from the EU. In both cases, the EU has allowed these nations to drive policies that negate the values and objectives of the EU cybersecurity strategy with no definite reactive policies thus further driving EU member nations apart at least politically. This also has the implications of increasing fraternisation with other countries beyond the EU on cybersecurity technologies, the association of which is likely to violate and thus affect the actualisation of cybersecurity governance. By allowing China and other similar major cyber technologically advanced countries manipulate EU standards in trade relations with EU member countries, opportunities are created for other nations to exploit similar loopholes in the region.

RQ3 What are the challenges faced by the EU commission to ensure cyber-peace in the EU region?

The challenges facing the EU commission in the cyber-peace agenda as revealed from the study is primarily the political interaction and atmosphere among the EU

member nations. Interactions and collaborations are still largely biased and filled with distrust over regional policies owing to the historical and current realities among member nations. The fact that more cyber threats and attacks against national cyber infrastructures within the EU have resulted from States within the EU is instructive on the state of interaction and trust between nations. From this air of suspicion other challenges are birthed such as inadequate funding, inadequate implementation of regional cybersecurity strategies especially among the private sector, no monitoring and accountability strategies, cybersecurity unawareness and lack of implementation of innovative research in academic institutions in countries within the EU amongst other concerns that do more to harm the overall cybersecurity governance aims of the EU. Also the EU faces the challenge of vulnerability to online radicalisation of their citizens owing to ignorance and lack of skills in cybersecurity at the individual and corporate level. These are however majorly traced to the appreciation and acceptance of responsibilities for the implementation of the cybersecurity policies by member nations. Cyber peace is essential for the attainment of effective cybersecurity governance in the EU region. Although there may be internal challenges bordering on the availability of finances and other necessary resources at the national level, the implementation of the various cybersecurity frameworks in a political and cyber peaceful atmosphere is likely to result in more positive approach to eliminating identified challenges than in a hostile atmosphere.

6. CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

The study set out to identify the challenges of the EU Cyber Security Strategy from actualising the goal of cybersecurity and cyber resilience among member countries and the EU region at large by investigating the conceptual understanding of cybersecurity as well as the best approach to ensuring cybersecurity from this perspective, examine the efforts of the EU in relation to ensuring cyber peace and enhancing cybersecurity governance within the EU and lastly assessing the challenges of the EU Cyber Security Strategies. The study reviewed relevant literatures and documents on cybersecurity and findings were related and critically analysed. The findings indicated that the EU has been instrumental in enhancing cybersecurity governance initiatives both within the region and globally. Due to the establishment of strategic partnerships with third world countries, the EU has been able to foster technological and cybersecurity development schemes and policies that have been instrumental in the protection of national cyber infrastructures as well as propelling global institutions to make relevant policies and steps in enhancing global cybersecurity governance. Within the EU these steps have also resulted in the establishment of regional cybersecurity policies and agencies saddled with enhancing cybersecurity and building cyber resilience into existing national and regional institutions both in the public and private sectors. For the past two decades, the EU has fostered the initiation of cybersecurity-based policies for this purpose.

However much of what the EU has done has only tended towards to enhancing cybersecurity governance and resilience but not cyber-peace. The efforts have rightly outlined and pursued objectives that foster regional management and mobilisation of resources at her disposal however these efforts at least the more active ones have tended only towards cyber-governance and not cyber peace. This is because cyber-peace necessarily involves addressing root causes of cyber conflicts and warfare in the first place, the elimination of which prepares the cyberspace for a reign of cyber peace. This has however being systematically avoided by the on-going efforts of the EU. Cyber conflicts and the existing threats in the EU cyberspace have been traced specifically to dip-

lomatic relations and distrust among member countries. The historical antecedents of nations within the region have indicated an atmosphere of suspicion, distrust and hostility especially bothering on political ideologies, sovereignty and supremacy struggle. This conflict and struggle has given rise to various forms of attacks and hostility at the ideological level, political level, economic level, security and more recently cyberspace. Therefore the attempts to address cybersecurity threats by focusing on the manifestations of the existing conflicts rather than on the root cause sponsoring such hostilities only amounts to ignoring the main issue of contention for temporary behavioural diplomacy. The EU has largely turned a blind eye to the political hostilities among her member countries and narrowly focused on cyber diplomacy to foster behavioural and attitudinal changes in favour of her cybersecurity governance agenda. This approach cannot and does not guarantee lasting peace in the cyberspace. As the nodal security system proposes, addressing security concerns must necessarily involve the participation and support of the constituent networking members evident in aligning their mentalities and methodologies with corporate goals and aims. As it is however, the EU has not addressed the differing mentalities and ideologies that constitute the cybersecurity nodal framework.

The elimination of existing challenge therefore depends on the ability of the EU and her several cybersecurity agencies to foster cyber peace amongst her constituent elements especially with respect to mentalities and ideologies that ferment hostility. The cybersecurity governance agenda of the EU can only have sufficient expression and effectiveness in an atmosphere of relative peace. Peace here may ultimately mean respect for sovereign entities and their cyberspace as well as geographical territories. It could also recognition and respect for ideological and political difference as well as adherence to regional and global security and trade standards so that an air of cordiality and mutual respect is enhanced. For the EU fostering peace among her constituent parts must be topmost in her cybersecurity governance agenda as without peace, reasons for hostility and conflict can be generated with ease. While the development of cybersecurity technologies is also important for ensuring cyber resilience and cybersecurity, this does not ultimately guarantee cyber peace. The only guarantee that sophisticated and advanced cyber technologies will not be used against countries with less cybersecurity infrastructure is an atmosphere of peace, mutual respect and cordiality even in the face of opposing political and philosophical ideologies. Sufficient resources therefore are needed to enhance cyber peace by pursuing diplomatic peace between EU nations. Sanctions and

punishments for violations are also important policies that must be implemented in the event of violations by member countries.

REFERENCES

Achkoski, J. and Dojchinovski, M. 2011. *Cyber Terrorism and Cyber Crime – Threats For Cyber Security*. Available online at https://www.35329569.pdf

Adesina, O, S, 2017, Cybercrime and Poverty in Nigeria, *Canadian Social Science* Vol. 13, No. 4, 2017, pp. 19-29 DOI: 10.3968/9394 ISSN 1923-6697[Online]

Akyeşilmen, N. 2018. Cyber Good Governance: A New Challenge In International Power Politics? *Cyberpolitik Journal* Vol. 3, No. 5 & 6

Antunes, M., Maximiano, M., Gomes, R. and Pinto, D. 2021. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy* 2021, 1, 219–238. https://doi.org/10.3390/jcp1020012

APCO International, 2016. *An Introduction to Cybersecurity: A Guide for PSAPs* Version 1.0 July 2016 APCO Cybersecurity Committee

Armstrong, A, 2011, Sakawa Rumours: Occult Internet Fraud and Ghanaian Identity, *Department of Anthropology, Working Paper No 08/2011 14* Taviton Street London WC1H OBW, UK

Austin, S. 2018. Cybersecurity, *Insider Threat Best Practices Guide, 2nd Edition February 2018*, www.sifma.org

Australian Computer Society, 2016, *Cybersecurity: Threats, Challenges, Opportunities*, Sydney: 50 Level 11 Carrington Street.

Australian Computer Society, 2016, *Cybersecurity: Threats, Challenges, Opportunities*, Sydney: 50 Level 11 Carrington Street.

Backman, S. 2016. The Institutionalization of Cybersecurity Management at the EU-level 2013-2016, *Master's Programme of Politics & War Swedish Defence University*

Barmpaliou, N, 2020, Emerging Threats in Cybersecurity: Implications for Latin America and the Caribbean In Inter-American Development Bank, 2020, *Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean*, 2020 IDB Cybersecurity Report.

Bendiek, A, Bossong, R. and Schulze, M. 2017. The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges. *Stiftung Wissenschaft und Politik German Institute for International and Security Affairs*, 47, November, 2017

Bendiek, A. 2012. European Cyber Security Policy, *Stiftung Wissenschaft und Politik (SWP) Research Paper* 13, October 2012

Bendiek, A. and Kettemann, M. C. 2021. Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy, *SWP Research Paper* No. 16 FEBRUARY 2021

Bendiek, A. and Maat, E. P. 2019. The EU's Regulatory Approach to Cyber-security, *Research Division EU/Europe SWP Nr. 02, October 2019*

Berg, V, D, B, and Keymolen, E, 2017, Regulating security on the internet: control versus trust, *International Review of Law, Computers & Technology*, 31:2, 188-205, DOI: 10.1080/13600869.2017.1298504.

Berger, R. 2021. *Cyber security and data privacy: Key considerations for policymakers*. Huawei, January, 2021

Bodeau, D., Boyle, S., Fabius-Greene, J. and Graubart, R. 2010. *Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology* September 2010.

Boutellier, H. and Steden, R. 2011. Governing nodal governance: the 'anchoring' of local security networks, In A. Crawford (ed) *International and Comparative Criminal Justice and Urban Governance: Convergences and Divergences in Global, National and Local Settings*, Cambridge Publishers: pp: 461-482

Bradshaw, S., DeNardis, L., Hampson, F. O., Jardine, E. and Raymond, M. 2016. Chapter Three: The Emergence of Contention in Global Internet Governance. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance. Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Brady, S. and Heinl, C. 2020. Cybercrime: Current Threats and Responses. A review of the research literature, *Research and Data Analysis Unit* October 2020

Brown, A. D. 2011. Cyber terrorism and war, the looming threat to the industrialised state. *London School of Economics* blogs.lse.ac.uk/waronterror/2011/06/16/cyber-terrorism-and-war-the-looming-threat-to-the-industrialised-state/

Burris, S., Drahos, P. and Shearing, C. 2004. Nodal Governance, *Temple Law School Working Papers* 2004

Burrow, S, 2020, Work: The Pandemic that Stopped the World, *In World Economic Forum, Challenges and Opportunities in the Post-COVID-19 World Insight Report*, Switzerland: World Economic Forum

Burt, C. H. and Simons, R. L. 2013. Self-Control, Thrill Seeking, and Crime: Motivation Matters. *Criminal Justice And Behavior*, Vol. xx, No. x, Doi: 10.1177/0093854813485575

Canadian Centre for Cybersecurity. 2015. *An Introduction to the Cyber Threat Environment*. Government of Canada

Cappelletti, F. 2021. Free market and cybersecurity in Europe: The need for strategic public-private partnerships, *European Liberal Forum Discussion Paper* N° 04 JANUARY 2021 1/30

Cappelletti, F. and Martino, L. 2021. Achieving robust European cybersecurity through public-private partnerships: Approaches and developments, *European Liberal Forum Discussion Paper* N° 04 JANUARY 2021 1/30

Carlton, M. and Levy, Y. 2017. Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management* Volume 5, Issue 2, 2017

Chang, L. Y. C. and Grabosky, P. 2017. The governance of cyberspace. In P. Drahos (ed), *Regulatory Theory: Foundations and applications*, Canberra, Australia: ANU Press, The Australian National University.

Charvat, J. P. I. A. G. 2009. Cyber Terrorism: A New Dimension in Battlespace. *SO2 Course Centre of Excellence Defence Against Terrorism*

Chetty, N. & Alathur, S. 2018. *Hate Speech Review in the Context of Online Social Networks. Aggression and Violent Behaviour (2017)*, Doi:10.1016/j.avb.2018.05.003

Chopitea, T. 2012. Threat modelling of hacktivist groups: Organization, chain of command, and attack methods. *Master of Science Thesis in Secure and Dependable Computer Systems*, Chalmers University of Technology, University of Gothenburg, Sweden.

Christen, M., Gordijn, B. & Loi, M., 2020, Introduction, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cybersecurity*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 1

Conway, M. 2003. Hackers as Terrorists? Why it Doesn't Compute. *Computer Fraud and Security* 2003 (12) (December): 10-13.

Conway, M. 2017. *Is Cyberterrorism a Real Threat? – Yes*, available at https://www.Pro-Cyberterrorism_Ch_Doras_Version.pdf

Costigan, S. S. and Hennessy, M. A. (eds). 2016. *Cybersecurity A Generic Reference Curriculum*. NATO

Council of Europe (CoE). 2020. The Budapest Convention on Cybercrime: Benefits and impact in practice, *Cybercrime Convention Committee (T-CY)* (2020) 16. Strasbourg: CoE

Council of the European Union, 2018. *EU Cyber Defence Policy Framework (2018 update)*, Brussels, 19th November, 2018

Craig, A, and Valeriano, B, 2016, Conceptualising Cyber Arms Races, *2016 8th International Conference on Cyber Conflict Cyber Power N.Pissanidis, H.Rõigas, M.Veenendaal 2016.* NATO CCD COE Publications, Tallinn

Craig, A, and Valeriano, B, 2016, Conceptualising Cyber Arms Races, *2016 8th International Conference on Cyber Conflict Cyber Power N.Pissanidis, H.Rõigas, M.Veenendaal 2016.* NATO CCD COE Publications, Tallinn

Craig, A. And Valeriano, B. 2018. Realism and Cyber Conflict: Security in the Digital Age. *Realism in Practice: An Appraisal*. E-International Relations https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ FEB 3 2018

Craigen, D., Diakun-Thibault, N. and Purse, R. 2014. Defining Cybersecurity, *Technology Innovation Management Review* October 2014 www.timreview.ca

Creese, S, 2020, Regional Trends in Cybersecurity Readiness, 2016–2020, In Inter-American Development Bank, 2020, *Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean*, 2020 IDB Cybersecurity Report.

Cuihong, C. 2018. Global Cyber Governance: China's Contribution and Approach. *China Quarterly of International Strategic Studies*, Vol. 4, No. 1, 55–76 DOI: 10.1142/S2377740018500069

CyberPeace Institute. 2021. *Playing with Peoples' Lives: Cyber-attacks on Healthcare are Attacks on People*. CyberPeace Institute March 2021.

DCAF, 2021. *Guide to Good Governance in Cybersecurity*. Retrieved from https://www.CyberSecurity_Governance_ENG_Jan2021.pdf

Demertzis, M. and Wolff, G. 2019. Hybrid and cybersecurity threats and the European Union's financial system, *Policy Contribution* Issue n˚10, September 2019

DeNardis, L. 2016. Introduction. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance*. *Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Department of Homeland Security. 2020. *Homeland Threat Assessment October, 2020*, US: DHS

European Commission, 2020. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, *European Commission Press Release* 16th December 2020, Brussels.

European Commission. 2020. The EU's Cybersecurity Strategy for the Digital Decade, *Joint Communication To The European Parliament And The Council* 16th December, 2020 Brussels

European Union Court of Auditors, 2019, Challenges to effective EU cybersecurity policy, *ECA Briefing Paper March 2019*, Luxemburg: ECA

European Union Court of Auditors, 2019, Challenges to effective EU cybersecurity policy, *ECA Briefing Paper March 2019*, Luxemburg: ECA

European Union Court of Auditors, 2019, Challenges to effective EU cybersecurity policy, *ECA Briefing Paper March 2019*, Luxemburg: ECA

European Union, 2013, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, *Joint Communication to The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions*, Brussels, 7, 2, 2013

European Union, 2017, *EU cybersecurity initiatives working towards a more secure online environment*, retrieved from https://www.factsheet_cybersecurity_update_january_2017_41543.pdf

Eurosmart, n.d. *The European Cybersecurity Act*, Brussels: Eurosmart

Evan, T., Leverett, E., Ruffle, S. J., Coburn, A. W., Bourdeau, J., Gunaratna, R. and Ralph, D. 2017. Cyber Terrorism: Assessment of the Threat to Insurance, *Cambridge Risk Framework series*, Centre for Risk Studies, University of Cambridge.

Fidler, D, P, 2016, The U.S. Election Hacks, Cybersecurity, And International Law, *Symposium on Cybersecurity and the Changing International Law of Data* doi:10.1017/aju.2017.5

Fidler, D, P, 2016, The US Election Hacks, Cybersecurity, And International Law, *Symposium on Cybersecurity and the Changing International Law of Data* doi:10.1017/aju.2017.5

Fischer, E. A. 2014. Cybersecurity Issues and Challenges: In Brief. *Congressional Research Service* 7-5700 www.crs.gov R43831 December 16, 2014

Fuster, G. G. and Jasmontaite, L. 2020. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn and M. Loi (eds.), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21*, https://doi.org/10.1007/978-3-030-29053-5_5

Gaia, J., Ramamurthy, B., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X. and Yoo, C. W. 2020. Psychological Profiling of Hacking Potential, *Proceedings of the 53rd Hawaii International Conference on System Sciences* 2020

Giantas, D, 2019. Cybersecurity Threats in the EU. Threats, Frameworks and Future Perspectives, *LICS Working Paper Series* No 1, September, 2019

Gilligan, J and Pardo, T. A. 2020. *Managing Cyber Threats through Effective Governance: A Call to Action for Governors and State Legislatures*. CIS & University at Albany.

Gisel, L. and Olejnik, L. 2018. The Potential Human Cost of Cyber Operations. *ICRC Expert Meeting 14–16 November 2018* – Geneva

Gogwim, J, G, n.d, *Cybersecurity: Emerging Threats and Mitigation Strategies*, ICT Directorate University of Jos, Nigeria.

Griffith, M. K. 2018. *Strengthening the EU's Cyber Defence Capabilities Report of a CEPS Task Force* Brussels: Centre for European Policy Studies (CEPS)

Gunkel, D. J. 2005. Editorial: introduction to hacking and hacktivism. *New Media & Society* Vol 7(5):595–597 [DOI: 10.1177/1461444805056007]

Hampson, N. C.N. 2011. Hacktivism, Anonymous & A New Breed Of Protest In a Networked World. *Boston College International & Comparative Law Review*, Vol 1, pp:1-33

Harjanne, A., Muilu, E., Pääkkönen, J. and Smith, H, 2018, *Helsinki in the era of hybrid threats – Hybrid influencing and the city*, Helsinki: European Centre of Excellence for Countering Hybrid Threats.

Herczynski, P, 2020, The EU's Comprehensive Approach to Address Threats from Cyberspace, In Inter-American Development Bank, 2020, *Cybersecurity Risks,*

Progress, and the Way Forward in Latin America and the Caribbean, 2020 IDB Cybersecurity Report.

Herrmann, D. and Pridöhl, H. 2020. Basic Concepts and Models of Cybersecurity, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cybersecurity*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 11

Holley, C. and Shearing, C. 2017. A nodal perspective of governance: Advances in nodal governance thinking, In P. Drahos (ed) *Regulatory Theory: Foundations and applications*, Canberra, Australia: ANU Press, The Australian National University, pp: 163-180

Homburger, Z. 2019. The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace, *Global Society*, 33:2, 224-242, DOI: 10.1080/13600826.2019.1569502

Hunker, J. & Probst, C. W. 2011. Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, volume: 2, number: 1, pp. 4-27

Ibrahim, S, 2016, Causes of socioeconomic cybercrime in Nigeria, *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada*, pp. 1–9. https://doi.org/10.1109/ICCCF.2016.7740439

Inter-American Development Bank, 2020, *Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean*, 2020 IDB Cybersecurity Report.

Inversini, R. 2020. Cyber Peace: And How It Can Be Achieved, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cybersecurity*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 259

Jahankhani, H., Al-Nemrat, A. and Hosseinian-Far, A. 2014. *Cybercrime classification and characteristics*. DOI: 10.1016/B978-0-12-800743-3.00012-8

Jaikaran, C. 2020. Cybersecurity: A Primer. *Congressional Research Service* https://crsreports.congress.gov

Jayakumar, S. 2020. Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. With Three Case Studies on Estonia, Singapore, and the United States, *Handbook of Terrorism Prevention and Preparedness*, DOI: 10.19165/2020.6.0129

Jayakumar, S. 2020. Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. With Three Case Studies on Estonia, Singapore, and the United States, *Handbook of Terrorism Prevention and Preparedness*, DOI: 10.19165/2020.6.0129

Jayawardane, S., Larik, J. and Jackson, E. Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. *The Hague Institute for Global Justice Policy Brief* 17, November 2015.

Jeffray, C. 2014. The Threat of Cyber-Crime to the UK: RUSI Threat Assessment. *Royal United Services Institute Briefing Paper* June 2014

Karim, R., Bonhi, T. C. and Afroze, R. 2019. Governance of Cyberspace: Personal Liberty Vs. National Security. *International Journal Of Scientific & Technology Research* Volume 8, Issue 11, November 2019

Kaspersky, 2020. A Brief History of Computer Viruses and What the Future Holds. Retrieved from https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Kavanagh, C. 2018, *The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century*, United Nations Institute for Disarmament Research, Geneva: UNIDIR

Kavangh, C. 2017. The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, *United Nations Institute of Disarmament Research*

Kertysova, K., Frinking, E., Dool, V. D. K., Maričić, A. & Bhattacharyya, K. 2018. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*. The European Economic and Social Committee (EESC), March 2018.

Kertysova, K., Frinking, E., Dool, V. D. K., Maričić, A. & Bhattacharyya, K. 2018. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*. The European Economic and Social Committee (EESC), March 2018.

Klein, J. J. 2018. Deterring and Dissuading Cyberterrorism, *ASPJ Africa & Francophonie - 1st Quarter 2018.*

Koeppe, D. 2020. Towards Guidelines for Medical Professionals to Ensure Cybersecurity in Digital Health Care, In M. Christen, B. Gordijn, and M. Loi (eds). *The Eth-*

ics of Cybersecurity, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 331

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. and Osula, A.M. 2015. *Insider Threat Detection Study*. NATO Cooperative Cyber Defence Centre of Excellence, Estonia

Kosutic, D. 2012. 9 *Steps to Cybersecurity. The Manager's Information Security Strategy Manual*. Zagreb: EPPS Services Ltd

Kouliopoulos, A., Vandendriessche, M., and Saz-Carranza, A. 2020. *REPORT: Case study of cyber governance*. Global Governance and the European Union: Future Trends and Scenarios

Kovács, L. 2018. Cyber Security Policy and Strategy In The European Union And NATO, *Land Forces Academy Review* Vol. XXIII, No 1(89), 2018

Kozlowski, A. 2014. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, *European Scientific Journal February* 2014 /SPECIAL/ edition vol.3

Kremer, S., Mé, L., Rémy, D. and Roca, V. 2019. Cybersecurity Current challenges and Inria's research directions. *Inria White Book N°03*

Kurbalija, J. 2014. *An Introduction to Internet Governance, 6th Edition*. Switzerland: DiploFoundation

Lațici, T. 2019. Cyber: How big is the threat? *European Parliamentary Research Service (EPRS) Members' Research Service* PE 637.980 – July 2019

Lehto, M, 2013, Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies, *International Journal of Cyber Warfare and Terrorism, 3(3), 1-18*, July-September 2013 DOI: 10.4018/ijcwt.2013070101

Lété, B. and Pernik, P. 2017. EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions, *Security and Defense Policy* 2017, No. 38

Liveri, D. and Sarri, A. 2021. *An Evaluation Framework for National Cyber Security Strategies*, European Union Agency for Network and Information Security (ENISA), DOI: 10.2824/3903

Loi, M. and Christen, M. 2020. Ethical Frameworks for Cybersecurity, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cybersecurity*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 73

Lucas, G. 2020. Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence', In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cyber-security*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 245

Lukaševičiūtė, J. 2019. EU and NATO Cyber Security Policy, *Master Thesis Submitted To The Department Of Political Science, Faculty Of Political Science And Diplomacy*, Vytautas Magnus Universitety

Malla Reddy College Of Engineering & Technology, 2021, *Cyber Security [R18a0521] Lecture Notes B.Tech III Year – II Sem (R18) (2020-2021)*, Department Of CSE Malla Reddy College Of Engineering & Technology

Markopoulou, D., Papakonstantinou, V. and de Hert, P. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review* 35 (2019) 105336

Maurer, T. and Morgus, R. 2014. Compilation of Existing Cybersecurity and Information Security Related Definitions, *New America Report*, October, 2014

Maxion, R. 2012. Making experiments dependable. In R. Meushaw (ed) *The Next Wave: The National Security Agency's Review of Emerging Technologies* Vol 19, No. 2, 2012

Mazzarolo, G. and Jurcut, A. D. 2020. Insider Threats in Cybersecurity: The Enemy within the Gates. *European Cybersecurity Journal* Vol 6, Issue 1, 2020, pp: 57-63

Medeiros, B. P. and Goldoni, F. R. L. 2020. The Fundamental Conceptual Trinity of Cyberspace *Contexto Internacional* Vol. 42(1) Jan/Apr 2020 http://dx.doi.org/10.1590/S0102-8529.2019420100002

Meer, S. V. D. 2015. Foreign Policy Responses to International Cyber-attacks: Some Lessons Learned, *Clingendael Netherlands Institute of International Relations Policy Brief*

Metacom, 2003. *What Is Hacktivism? 2.0* (December 2003) http://www.thehacktivist.com/hacktivism1.php

Meushaw, R. 2012. Developing a blueprint for a science of cybersecurity. *The Next Wave: The National Security Agency's Review of Emerging Technologies* Vol 19, No. 2, 2012

Morgan, G. and Gordijn, B. 2020. A Care-Based Stakeholder Approach to Ethics of Cybersecurity in Business, In M. Christen, B. Gordijn, and M. Loi (eds). *The*

Ethics of Cybersecurity, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 119

Morten, B. 2016. What Is Cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal For Media Research* – n° 6/2016 – ISSN 2264-4733

Mortera-Martinez, C. 2018. Game over? Europe's cyber problem, *Open Society European Policy Institute*, July 2018

Moșoiu, O., Bălăceanu, I. and Mihai, E. Cyber terrorism and the effects of the Russian attacks on democratic states in East Europe. *Scientific Journal of Silesian University of Technology. Series Transport*. 2020, 106, 131-139. DOI: https://doi.org/10.20858/sjsutst.2020.106.11.

Mueller, M. 2018. Sovereignty and Cyberspace: Institutions and Internet governance. *Essay at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana* October 3rd 2018.

Muhammad, S. 2017. Conceptualising Cyber-Security: Warfare and Deterrence in Cyberspace. *Journal of Strategic Affairs*, 19-64

Munk, T. H. 2015. Cybersecurity in the European Region: Anticipatory Governance and Practices. *A PhD thesis submitted to The Faculty of Humanities, The School of Law, University of Manchester*

Munk, T. H. 2015. Cybersecurity in the European Region: Anticipatory Governance and Practices. *A PhD thesis submitted to The Faculty of Humanities, The School of Law, University of Manchester*

Myers, N, 2020, Cyber Security: Cyber Crime, Attacks and Terrorism, *ODU UN Day 2020 Issue Brief GA First Committee (DISC)*

Myers, N, 2020, Cyber Security: Cyber Crime, Attacks and Terrorism, *ODU UN Day 2020 Issue Brief GA First Committee (DISC)*

Myers, N, 2020, Cyber Security: Cyber Crime, Attacks and Terrorism, *ODU UN Day 2020 Issue Brief GA First Committee (DISC)*

National Association of County and City Health Officials. 2015. Cybersecurity: Risks and Recommendations for Increasingly Connected Local Health Departments. *NACCHO Issue Brief* February, 2015

Newman, J, and Bell, P, 2012, Social Network Media and Political Activism: A Growing Challenge for Law Enforcement, *Journal for Policing, Intelligence and Counter Terrorism* Vol.7, 36-50.

Nye (Jnr), J. S. 2016. Chapter One: The Regime Complex for Managing Global Cyber Activities. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance*. *Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Nøkleberg, M. 2016. Security Governance – An Empirical Analysis of the Norwegian Context, *Nordisk politiforskning*, Volume 3, no 1-2016 p. 53–82, DOI: 10.18261/issn.1894-8693-2016-01-05

Office of the Coordinator for Cyber Issues. 2015. *Internet Governance*. Office of the Coordinator For Cyber Issues (S/CCI) United States Department of State, August 2015.

Office of the Director of National Intelligence, 2021. *Annual Threat Assessment of the US Intelligence Community*, April 9, 2021. USA: DNI

Ojetayo, V, D, 2017, *Transnational Responses to Cybercrimes Challenges in the 21st Century: An Appraisal of Existing Treaties, a Call for a General Multi-Lateral Treaty*, (September 13, 2017), http://dx.doi.org/10.2139/ssrn.3036659

Oladimeji, R, 2019, 167 arrested, $169,850 recovered in EFCC/FBI Operation Rewired. *Punch Newspaper September 11th 2019* retrieved online at https://punchng.com/167-arrested-169850-recovered-in-efcc-fbi-operation-rewired/

Paget, F. 2013. Hacktivism. *Chaire de Cyberdefense et Cybersecurite July 2013, Article n°II.3*

Pande, J. 2017. *Introduction to Cyber Security*, Haldwani: Uttarakhand Open University

Pâris, C. 2021. Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace, *EU Diplomacy Papers* 1/2021

Parker, N, & Charnock, N, 2020, *England and Wales: Cyber-security laws and regulations 2020*. ICLG.com 2nd 11, 2020, retrieved from https://www.iclg.com/practice-areas/cybersecurity-laws-and-regulations/england-and-wales

Pasculli, L. 2020. The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. *Journal of Ethics and Legal Technologies* – Volume 2(1) – April 2020

Poel, I. V. D. 2020. 3 Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of*

Cybersecurity, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 45

Porrúa, M, and Contreras, B, 2020, What has Changed since the 2016 Report? In Inter-American Development Bank, 2020, *Cybersecurity Risks, Progress, and the Way Forward in Latin America and the Caribbean*, 2020 IDB Cybersecurity Report.

Raymond, M. 2016 Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot. *Strategic Studies Quarterly*, Winter 2016

Raymond, M. and DeNardis, L. 2016. Chapter Two: Multi-stakeholderism: Anatomy of an Inchoate Global Institution. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance. Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Reddy, G. N. and Reddy, G. J. U. 2013. A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies. Retrieved from https://www.1402.1842.pdf

Richards, I. and Wood, M. A. 2018. Hacktivists against Terrorism: A Cultural Criminological Analysis of Anonymous' Anti-IS Campaigns. *International Journal of Cyber Criminology* January – June 2018. Vol. 12(1): 187–205. DOI: 10.5281/zenodo.1467895

Robinson, M., Jones, K. and Janicke, H. 2015. Cyber Warfare: Issues and Challenges. *Journal of Computers and Security* March 2015 DOI: 10.1016/j.cose.2014.11.007

Robinson, M., Jones, K., Janicke, H. and Maglaras, L. 2018. *An Introduction to Cyber Peacekeeping* APRIL 2018 arXiv:1710.09616v2 [cs.CY] 24 Apr 2018

Roff, H. M. 2016. Cyber Peace: Cybersecurity Through the Lens of Positive Peace, *New America March* 2016 Cyber-security

Rone, J. 2020. Hacking and hacktivism. *Pre-final entry for the Routledge Encyclopedia of Citizen Media*, http://citizenmediaseries.org/published_volumes/routledge-encyclopedia-of-citizen-media/

Roscini, M. 2010. World Wide Warfare - Jus Ad Bellum and the Use of Cyber Force. In A. von Bogdandy and R. Wolfrum (eds) *Max Planck Yearbook of United Nations Law*, Vol 14, 2010, pp: 85-130. Netherlands: Koninklijke Brill NV

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J. and Schwartz, A. 2003. *Information Technology Security Handbook*. Washington DC: The World Bank

Sailio, M., Latvala, O.M. and Szanto, A. 2020. Cyber Threat Actors for the Factory of the Future. *Applied Sciences* 2020, 10, 4334; doi:10.3390/app10124334

Saroha, R. 2014. Profiling a Cyber Criminal. *International Journal of Information and Computation Technology* Volume 4, Number 3 (2014), pp. 253-258

Savage, J. E. and McConnell, B. W. 2015. *Exploring Multi-Stakeholder Internet Governance*. New York: East-West Institute

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. R. and Burnap, P. 2020. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics* 2020, 9, 1460; doi:10.3390/electronics9091460

Schlehahn, E. 2020. Cybersecurity and the State, In M. Christen, B. Gordijn, and M. Loi (eds). *The Ethics of Cybersecurity*, Switzerland: The International Library of Ethics, Law and Technology 21 https://doi.org/10.1007/978-3-030-29053-5 pp: 205

Schneider, F. 2012. Blueprint for a science of cybersecurity. In R. Meushaw (ed) *The Next Wave: The National Security Agency's Review of Emerging Technologies* Vol 19, No. 2, 2012

Scott, T. W. and Cupp, O. S. 2017. Ethics of Hacktivism. *Simons Center Special Report, The Ethics of Future Warfare*, 2017

Shackelford, S. J. & Kastelic, A. 2015. Toward A State-Centric Cyber Peace?: Analyzing The Role Of National Cybersecurity Strategies In Enhancing Global Cybersecurity. *Legislation and Public Policy* Vol. 18:895, 2015

Shackelford, S. J. 2013. Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance. *American University Law Review* 62, No.5 (2013): 1273-1364

Shackelford, S. J. 2014. *Managing Cyber Attacks in International Law, Business, and Relations: In search of cyber peace*. Cambridge University Press 978-1-107-00437-5

Shackelford, S. J. 2017. Exploring The 'Shared Responsibility' Of Cyber Peace: Should Cybersecurity Be A Human Right? *Ostrom Workshop White Paper Series July 2017*: *Program On Cybersecurity and Internet Governance*

Shackelford, S. J. 2017a. The Law of Cyber Peace, *Chicago Journal of International Law*: Vol. 18: No. 1, Article 1. Available at: https://chicagounbound.uchicago.edu/cjil/vol18/iss1/1

Shiryaev, Y. 2012. Cyberterrorism in the Context of Contemporary International Law, *Cyberterrorism* VOL. 14: 139, 2012, San Diego Int'l L.J.

Simplicity, n.d. The A to Z of Cybersecurity Glossary. Available at www.globalknowledge.com

Siobhan, T. 2020. Teenagers' Thrill Seeking Impulses can lead to cybercrime. *Engineering 360*, retrieved from https://insights.globalspec.com/article/13352/teenagers-thrill-seeking-impulses-can-lead-to-cyber-crime

Sleeman, J., Finin, T. and Halem, M. 2020. Temporal Understanding of Cybersecurity Threats

Snowden, E, 2019, *Permanent Record*, UK: MacMillan

Sorell, T. 2015. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. *Journal of Human Rights Practice* September 2015 DOI: 10.1093/jhuman/huv012

Stallings, W. 2019. *Effective Cybersecurity: Understanding and Using Standards and Best Practices*. USA: Addison-Wesley

Stephen, A, T, 2016, The Role of Digital and Social Media Marketing in Consumer Behavior, *Current Opinion in Psychology 2016,* 10:17–21 http://dx.doi.org/10.1016/j.copsyc.2015.10.016

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T. & Eeten, M. V. 2019. Governance Challenges for European Cyber Security Policy: Stakeholders Views. First Draft, *Cyber Security for Europe*

Storck, M, 2011, The Role of Social Media in Political Mobilisation: A Case Study of the January 2011 Egyptian Uprising, *MA dissertation submitted to the Department of International Relations, University of St Andrews, Scotland*

Suleman, L, 2018, Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists, *Criminology, Criminal Justice, Law & Society Volume 19, Issue 2*, Pages 63–80 Available online at https://scholasticahq.com/criminology-criminal-justice-law-society/

Tanczer, L. M. 2014. Hacktivism and the Male-Only Stereotype. *New Media & Society* http://dx.doi.org/10.1177/1461444814567983

Taylor, E. 2016. Chapter Five: ICANN: Bridging the Trust Gap. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance. Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Threat Working Group of the CSIS Commission on Cybersecurity. 2007. Threats Posed by the Internet. *Threat Working Group of the CSIS Commission on Cybersecurity for the 44th Presidency*

Tiirmaa-Klaar, H, 2011, Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels, *CERI-CNRS Sciences Pro* http://www.ceri-scienes-po.org

Tsakanyan, V.T. 2017. The Role Of Cybersecurity In World Politics *Vestnik RUDN International Relations* 2017 Vol. 17 No. 2 339—348 339 DOI: 10.22363/2313-0660-2017-17-2-339-348

United Nations Development Programme (UNDP), 2020, *2020 Human Development Perspectives Covid-19 And Human Development: Assessing the Crisis, Envisioning the Recovery*, New York: UNDP.

Vallor, S and Rewak, W. J. 2017. An Introduction to Cybersecurity Ethics.

Warman, M. 2021. *Explanatory Memorandum on the Joint Communication to the European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Age*, Submitted by the Department for Digital, Culture, Media and Sport on 26 January 2021.

Veale, M. and Brown, I. 2020. Cybersecurity, *Internet Policy Review*, No 9(4), pp:1-22. https://doi.org/10.14763/2020.4.1533

Wegener, H. 2011. Cyber Peace. *The Quest For Cyber Peace* International Telecommunication Union and World Federation of Scientists.

Verhulst, S. G., Noveck, B. S., Raines, J. and Declercq, A. 2016. Chapter Six: Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem. *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance. Global Commission on Internet Governance Research Volume Two*, CIGI & Chatham House

Westby, J. R., Wegener, H. and Barletta, W. 2010. *Rights and Responsibilities in Cyberspace Balancing the Need for Security and Liberty*. EastWest Institute/World Federation of Scientists

Whitty, M, T, 2018, 419 – It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa, *International Journal of Cyber Criminology January – June 2018,* Vol. 12(1): 97–114, DOI: 10.5281/zenodo.1467848

Wilson, C. and Laidlaw, G. 2017. Applying Nodal Governance to Combat Cybercrime: An Novel Approach *Journal of The Colloquium for Information System Security Education (CISSE)* Edition 5, Issue 1 - October 2017

Wilson, K. S. and Kiy, M. A. 2014. Some Fundamental Cybersecurity Concepts. *IEEE Access* Volume 2, 2014 Digital Object Identifier 10.1109/ACCESS.2014.2305658

Vishik, C., Matsubara, M. and Plonk, A. 2016. Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms, In A.M. Osula and H. Rõigas (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2016

Vishik, C., Matsubara, M., Plonk, A. 2016. Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. In A.M. Osula and H. Rõigas (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCDCOE Publications 2016

World Bank Group, 2019, *Global Cybersecurity Capacity Program Lessons Learned And Recommendations*, Washington DC: World Bank Group

Yan, L. 2019. Global Cyberspace Governance: State Actors and the China-US Cyber Relationship. *Contemporary International Relations* Vol. 29 No. 2, pp: 105-124

Zerzri, M. 2017. The Threat of Cyber Terrorism and Recommendations for Countermeasures, *Centre for Applied Policy Research, C. A. Perspectives on Tunisia* No. 04-2017