The Lighthouse Journal of Social Sciences, Vol. 03, Issue 1, Summer 2024, pp. 67-88

Global Culture of Cybersecurity: A Multi-vocal Literature Review Protocol

Nisar Muhammad[1], Siffat Ullah Khan[2]

ABSTRACT

With the increasing use of technology and interconnected devices globally, the number of cyber-attacks has also grown exponentially. Technological countermeasures alone are insufficient to effectively control these attacks at an acceptable level. Despite advancements in technology, human errors and vulnerabilities continue to pose significant challenges in protecting digital assets worldwide. One of the most effective methods to mitigate cyber-attacks is to establish and nurture a culture of cybersecurity at the global, national, organizational, and group levels. While much research has been focused on organizational and national-level cybersecurity culture, the research pertaining to global cybersecurity culture is currently lacking and underexplored. This gap is evident in the limited academic literature addressing global cybersecurity culture. However, there is grey literature available from various regional and international organizations and cybersecurity forums, such as policy documents, reports, and white papers that provide valuable insights and practical perspectives. The primary objective of this research is to develop a protocol for conducting a comprehensive literature review to evaluate existing literature, both white and grey, and highlight advancements in the field of global cybersecurity culture and propose future directions. We are currently implementing this protocol.

Keywords: *Multi-vocal literature review (MLR), Global cybersecurity culture, Global culture of cybersecurity, cybersecurity, cybersecurity culture, challenges, success factors, domains and dimensions, practices, strategies*

INTRODUCTION

The exponential growth of information has made cyber-attacks a substantial challenge for states, organizations, society, and individuals alike (Ibrahim, 2022; Sharma et al., 2023). As these cyber-attacks evolve in complexity and frequency, safeguarding data and critical infrastructure has become vital (Chen, 2023). Over the past decade, the field of cybersecurity has gained popularity within the research community due to the alarming rise in cybercrimes and cybercrime

[1] *Software-Engineering-Research-Group (SERG-UOM), Department of Computer Science and IT, University of Malakand, Pakistan Department of Computer Science and IT (CS&IT), University of Malakand, Pakistan.* ***Corresponding Author's Email****:* malaknadpk@gmail.com

[2] *Software-Engineering-Research-Group (SERG-UOM), Department of Computer Science and IT, University of Malakand, Pakistan*

Manuscript Submitted: March 20, 2024
Manuscript Accepted: June 25, 2024

behaviors (Humayun et al., 2020; Reegård et al., 2020). Studies have shown that technological advancements and frameworks alone are not enough to protect sensitive information and digital assets without a strong cybersecurity culture in place (Alnifie & Kim, 2023; Mwim et al., 2023; Reegård et al., 2020). Appropriate cybersecurity measures are crucial to mitigate the substantial impact of threats, risks, and vulnerabilities.

One of the most effective approaches to mitigate cyber-attacks globally is to create and maintain a culture of cybersecurity at a global level, a need recognized by United Nations (UNGA, 2003). Several regional and international initiatives have been taken by public and private sector organizations, such as the United Nations, ITU, WEF, WB, GGE, GCA, UNIDIR, ENISA, ASEAN regional forum, SCO, and Microsoft Corporation, to develop a global cybersecurity culture (Camino, 2017). However, the area of the global culture of cybersecurity is unexplored in the research community and needs further study to contribute to mitigating cybersecurity threats worldwide (Paziuk & Mitsik, 2019). Additionally, grey literature including policy documents, theses, reports, blogs, acts/resolutions of regional and international organizations, and white papers provide valuable insights and practical perspectives on the global culture of cybersecurity.

This study aims to contribute to the ongoing discussion on global cybersecurity culture by conducting a comprehensive multi-vocal literature review (MLR). The purpose of the review is to examine the existing challenges and proposed solutions in order to highlight the importance of addressing the growing cybersecurity threats at the international level. The current literature lacks a systematic, multi-vocal study to identify the key success factors, challenges, and practices necessary for fostering a robust global cybersecurity culture. To address this gap, this research will conduct a comprehensive analysis of pertinent literature, both white and grey, and explore the following research questions.

i. What is the state-of-the-art in Global Cybersecurity culture?
ii. What are the domains dimensions to be considered in building and maintaining Global Cybersecurity Culture?
iii. What are the influencing factors to be adopted in building and maintaining Global Cybersecurity Culture?
iv. What are the challenges to be avoided in building and maintaining Global Cybersecurity Culture?
v. What are the practices to ensure Global Cybersecurity Culture?

The rest of the paper is organized as follows: section 2 provides details about the culture of cybersecurity. Section 3 covers related work. Section 4 outlines the methodology. Section 5 details data extraction. Section 6 discusses synthesis. Section 7 covers the validation of the protocol. Finally, section 8 presents the conclusion and future work.

CYBERSECURITY CULTURE

In today's digital world, it is crucial to develop a strong cybersecurity culture in order to proactively defend against the evolving cyber threats at a global scale. This culture promotes shared responsibility and integrates cybersecurity into daily practices, empowering individuals as

the first line of defense (AlHogail & Mirza, 2014a; Gcaza & von Solms, 2017a). Cybersecurity culture refers to the shared beliefs, values, attitudes, and behaviors related to cybersecurity within national and international organizations, communities, or on a global scale, aimed at protecting digital assets, preserving privacy, and mitigating cyber risks (Astakhova, 2014; Da Veiga, 2009; Okere et al., 2012). According to Reegård et al. (Reegård et al., 2020), security culture is composed of four layers: knowledge, tacit assumptions, espoused values, and artifacts, as shown in Figure 1. Despite technical advancements, it is important to note that human errors still account for 74% of breaches[3] (Verizon 2023), making the human element a weak link in the cybersecurity chain (Granova et al., 2023; Kannelønning & Katsikas, 2023; Klein & Zwilling, 2023). Therefore, addressing human vulnerabilities alongside technology is essential in effectively mitigating risks. This underscores the need for a robust cybersecurity culture at all levels, especially at the global level (Da Veiga, 2016; Matsumoto, 2019), as explained below.

Levels of Cybersecurity Culture

Veiga et al. (Da Veiga, 2016) proposed a multilevel model of cybersecurity culture that includes individual, organizational, national, and international/global levels. Likewise, Tziarras (Tziarras, 2014b) introduced a multi-level management cybersecurity framework that highlights communication patterns between different levels, such as non-state, state, regional, and inter-regional levels. In literature (Da Veiga, 2016), different levels of cybersecurity culture have been discussed, each focusing on specific aspects of cybersecurity awareness and practices, which are discussed below.

Personal cybersecurity culture

Personal level cybersecurity culture involves being proactive in adopting secure practices while interacting with ICT devices, such as using strong passwords and staying informed about cybersecurity risks. Dorosh et al. (Dorosh et al., 2020; Mahmudova, 2023) investigated the idea of personal information security culture as a foundation for establishing a security culture, while others examined individual personality traits that contribute to violations of cybersecurity policies (Alhogail & Mirza, 2014b; Georgiadou et al., 2020; McBride et al., 2012).

Group cybersecurity culture

Emerging from a broader understanding of organizational cybersecurity culture, group level cybersecurity culture refers to the shared beliefs, attitudes, and behaviors regarding cybersecurity within specific teams or groups. Several researchers have studied the effectiveness of group-level cybersecurity behaviors and factors for maintaining their desired level of cybersecurity (Pullin, 2018; Yoo et al., 2020). Researchers emphasize that group-level dynamics are as important as individual-level effectiveness because group mechanisms provide a basis for the development of the overall culture of cybersecurity in an organization or society in general (Herath & Rao, 2009; Ioannou et al., 2019; Sharma & Aparicio, 2022).

---

[3] Verizon, Data Breach Investigations Report 2023,
https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Organizational cybersecurity culture

Organizational cybersecurity culture encompasses the shared beliefs, values, and behaviors concerning cybersecurity within an organization (AlHogail & Mirza, 2014a; Da Veiga et al., 2020; Niekerk & Issa, 2006; Van Niekerk & Von Solms, 2006). It includes the shared understanding and practices embraced by employees, leaders, and stakeholders. It is imperative to note that a significant portion of research has been carried out in the realm of organizational cybersecurity culture, mainly due to its profound influence on the overall cybersecurity environment (Kannelønning & Katsikas, 2023). Numerous studies have investigated the organizational culture in relation to achieving the desired levels of cybersecurity (Adéleda Veigaa, 2017; Santos et al., 2021; Schlienger & Teufel, 2003). Various organizational cybersecurity culture models/frameworks have been proposed by scholars to assess readiness and the level of cybersecurity culture for promoting cultural hygiene in organizations (Fisher et al., 2021; Hasan et al., 2021; Holiness Nikel & Oguejiofor Amaechi, 2022).

National cybersecurity culture

The national culture of cybersecurity aims to address the cultural and societal dimensions of cybersecurity at a national level. It encompasses the shared principles, values, and conduct regarding cybersecurity within a nation or country. Gcaza et al. (Jansen Van Vuuren et al., 2015) proposed an ontology for the domain of national cybersecurity culture. Other studies show the effectiveness of national-level cybersecurity strategies in promoting cybersecurity practices on a national scale (Gcaza & Von Solms, 2017b; Odebade & Benkhelifa, 2023; Shillair et al., 2022). For example, the Cybersecurity Audit Model (CSAM) (Sabillon, 2022; Sabillon et al., 2018), the Framework for National Cybersecurity Capacity Buildings (Ghernouti-Hélie, 2010; Naseir, 2021; Tallón-Ballesteros, 2021), cybersecurity capacity maturity approaches for nations (Creese et al., 2017; *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition*, 2021), the European Union's national strategy for cybersecurity (*ENISA National Cyber Security Strategy Good Practice Guide*, 2012), and the ITU's strategy guide for national cybersecurity in 2011 and 2021 (ITU, 2021).

Global cybersecurity culture

Zenonas Tziarras et al. (Tziarras, 2014a) define the security culture of multileveled cybersecurity as "*A body of collective—i.e., non-state, sub-national, and national—attitudes, patterns of behavior, beliefs, as well as conceptions of (cyber) security, shaped based on the need to secure multiple referent objects against various cyberthreats, which would influence cybersecurity strategie*s". Based on this definition, the Global Cybersecurity Culture (GCSC) would be a collective set of shared values, attitudes, behaviors, and practices related to cybersecurity that bring people together on a global scale. This culture should be practiced at all levels—global, national, organizational, and individual—to ensure comprehensive and collaborative security measures across the globe. It encompasses norms, practices, and a mindset that shape how cybersecurity is perceived and approached worldwide. Various academic papers, policy documents, and reports have contributed to shaping the concept of global cybersecurity culture, with diverse perspectives (Paziuk & Mitsik, 2019; Stein & Solange, 2011; UNGA, 2003).

The emphasis is on the importance of a unified and cohesive approach to cybersecurity that goes beyond geographical and cultural boundaries (Ghernaouti-Hélie, 2009). It recognizes that cybersecurity challenges are not limited to specific regions but rather require a collective effort to address and mitigate risks on a global level (UNGA, 2003, 2009).

These levels highlight the complex nature of cybersecurity culture and the importance of addressing it across different levels and dimensions to effectively mitigate cybersecurity risks. The multi-level dynamics of cybersecurity culture are explained in the next section.

Multilevel dynamics of cybersecurity culture

The cybersecurity culture is present at the personal, group, organizational, national, and global levels (Da Veiga, 2016). Each level of cybersecurity influences the overall security posture of individuals, organizations, and nations within the digital landscape, forming a multilevel model. This is similar to the multilevel model proposed Miriam Erez and Efrat Gati (Erez & Gati, 2004). These different levels of cybersecurity culture complement and interact with each other, creating an interconnected framework to address the ever-evolving challenges related to cybersecurity worldwide. The culture works in top-down and bottom-up approaches, where cyber norms and values at the macro level become shared experiences and behaviors at the micro level. Similarly, behavior at the micro level leads to universally accepted cyber norms at the global level through bottom-up processes, as shown in Figure 1. The key components of cybersecurity culture are present at all levels, interacting and mutually influencing one another, and collectively shaping the overall security posture of individuals, organizations, and nations globally in the digital realm.

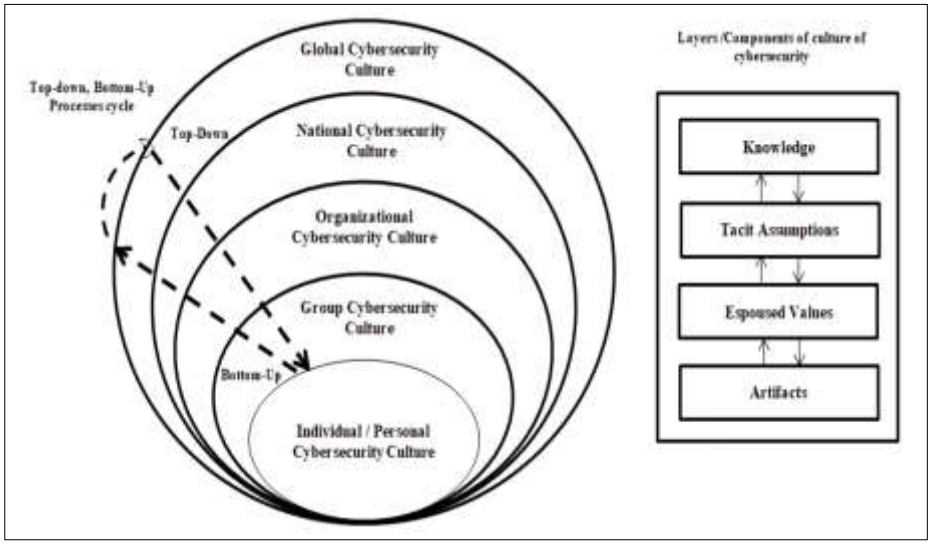

Figure 1: Cybersecurity culture top-down and bottom-up approaches across levels

RELATED WORKS

The creation of a global culture of cybersecurity involves various approaches and collaborative efforts led by various regional and international organizations, such as the United Nations (UN) and the International Telecommunication Union (ITU). For example, the UN General Assembly's resolution "Creation of a global culture of cybersecurity, 57/239, 2003" (UNGA, 2003) provides a foundation for developing of norms and principles for responsible state behavior. Table 1 outlined the approaches that have contributed to promoting a safe and secure digital environment worldwide by fostering a culture of cybersecurity. Additionally, initiatives like the Global Cybersecurity Agenda (Stein, 2007) and the Global Commission on the Stability of Cyberspace contribute to global governance and stability in the cyberspace.

Table 1: Approaches contributed to the formation of a global culture of cybersecurity

Study Area	Contributions
Norms and Principles	Formulation of norms and principles by the United Nation's Group of Governmental Experts (UNGGE, 2015)
International Legal Framework	The Convention on Cybercrime or the Budapest Convention (UNISA, 2004). Legislative efforts like the Cybersecurity Act of the European Union (*Cybersecurity Act of the European Union*, 2019).
Multilateral Cooperation	The United Nations General Assembly resolution "Creation of a global culture of cybersecurity, 57/239, 2003" (UNGA, 2003, 2009).
Certification and Standards	NIST CSF (*NIST Cybersecurity Framework (CSF)*, 2018) and ISO 2700, and certification of the cybersecurity
Governance and Collaboration frameworks	The Global Cybersecurity Agenda (Schjølberg, 2020; Touré & Schjølberg, 2007) and Global Commission on the Stability of Cyberspace (GCSC, 2019)

Despite the efforts of governments, international organizations, academia, and industry experts, the field of global cybersecurity culture is facing numerous challenges that pose significant threats to digital infrastructures worldwide. Issues such as the rapid evolution of cyber threats, political disagreements over norms and laws, and limited cooperation continue to hinder progress in fostering a strong global cybersecurity culture. However, there is a noticeable gap in the existing literature: the lack of comprehensive exploration and solutions through systematic reviews, particularly a multi-vocal literature review. This research protocol aims to address this gap by adopting a multi-vocal literature review approach to systematically explore various challenges, identify key success factors, and elucidate best practices necessary for navigating the complex landscape of global cybersecurity culture. To achieve this, the protocol will investigate the following research questions.

RESEARCH METHODOLOGY

The basic purpose of this study is to conduct a comprehensive literature review using the Multi-vocal Literature Review (MLR) approach, specifically focusing on Global Cybersecurity Culture. The MLR approach, which is part of the broader framework of Systematic Literature

Review (Kitchenham & Charters, 2007; Kitchenham et al., 2010), follows the guidelines established by Garousi et al. (Garousi et al., 2019), which have gained significant recognition in software engineering research. This methodology enables researchers to capture emerging trends and insights in rapidly evolving fields, thereby enhancing the depth and breadth of scholarly investigation.

Search Strategy

The search strategy for this Multi-vocal Literature Review (MLR) protocol on Global Cybersecurity Culture aims to comprehensively and systematically explore academic and grey literature sources. The search strategy for this study involves using a combination of searches in digital libraries, manual searches, and citation chaining techniques to find relevant academic articles, reports, white papers, theses, and other grey literature sources (Garousi et al., 2019). Databases include IEEE Xplore, Springer Link, Google Scholar, Wiley Online, Science Direct, ACM Digital Library and relevant governmental and organizational websites. Carefully selected keywords and search terms will be used for the formation of search strings to cover the multidimensional aspects of Global Cybersecurity Culture, including cybersecurity culture, practices, strategies, and challenges. Additionally, manual searches will also be performed to find relevant grey literature outside of traditional academic sources, such as industry reports, policy documents, and expert blogs. Snowballing techniques will be used to further trace references and identify similar works and related literature (Wohlin, 2014).

Trial search

Major terms and their alternatives identified from the research questions are: global cybersecurity culture, domains and dimensions, challenges, success factors, and best practices. A trial search was performed using the following search string across multiple databases, including IEEE Xplore, ACM, Springer Link, and Google Scholar.

(“Cyber security culture” OR “Cybersecurity culture” OR “Global cybersecurity culture” OR “International security culture”) AND (Challenges OR risks OR issues OR factors OR practices OR solutions OR domains OR dimensions guidelines)

Constructing search term

The PICO framework (Population, Interventions, Comparison, and Outcome) is used to structure a refined search string for this multi-vocal literature review (MLR) (Karyda, 2017), as provided in Table 2. The same methodology has been used by other researchers (Humayun et al., 2022). The following details will provide the basis for the search string to be constructed to find the desired literature relevant to the research questions.

Table 1: PICO Criteria for search string for global cybersecurity culture

S.NO	PICO Criteria	Details
i.	Population	Governments, Private sector organizations, professional, policymakers, political actors working to foster Global cybersecurity culture
ii.	Intervention	Identification of global cybersecurity culture challenges, success factors, domains and dimensions and practices
iii.	Experimental Design	Multi-vocal Literature Review (MLR)
iv.	Outcomes	List of global cybersecurity culture challenges, success factors, domains and dimensions and their practices

For example, our research question is formulated as below:

[What are the domains and dimensions, challenges, success factors, and practices?]---------- "INTERVENTION"

In the context of [Global Cybersecurity Culture] ---------- "POPULATION"

To be considered for

[Global Culture of Cybersecurity]----------"OUTCOMES OF RELEVANCE"

Identifying search terms

To identify search terms the following strategy is followed.

a. The research questions are used to obtain key terms by using the PICO criteria.
b. Find the alternative major terms and alternative used in the research questions.
c. Verify the identified terms in relevant research articles.
d. Use Boolean operators AND, OR, NOT to construct search string.

Results for a)

"Global cybersecurity culture",
"Success factors",
Challenges,
Practices,
"Building and maintaining global cybersecurity culture"

Results for b)

To identify synonyms and alternative words that will be used in development of the final search string, the articles and publications deemed relevant during the trial search will serve as validation sources for the finalizing the search strings. Global cybersecurity culture: ("global cybersecurity culture" OR "Global cyber security culture" OR "International Security Culture" OR "Global cyber-security culture")

Challenges: (chanllenges OR issues OR barriers OR risks)

Factors: (Factors OR motivators OR "success factors")

domains: (dimensions OR "key determinants")

Practices: (Practices OR solutions OR guidlines)

Building and maintaining global cybersecurity culture: ("Development and maintenance of global cybersecurity culture" OR "building cybersecurity culture"OR "maintaining cybersecurity culture")

Results for c)

Global cybersecurity culture, practices, cybersecurity culture, information security culture, challenges, dimensions, domains, features.

Results for d)

Search String

We used different search strings for different digital libraries according to their syntax/formate as shown in Table 3.

Search constraints and validation

While developing this protocol, we are trying to search all possible literature published in the area of global cybersecurity culture, and there are no constraints or time boundries.

Table 2: Search string and digital libraries for searching relevant literature to global cybersecurity culture

S.NO	Database	Search String
1	IEEE Xplore Springer Link Google Scholar	(("global cybersecurity culture" OR "international cybersecurity culture" OR "global cyber-security culture" OR "global culture of cybersecurity") AND (domains OR dimensions OR challenges OR "success factors" OR practices))
2	ACM Digital Library Science-Direct Wiley Online Library	(("global cybersecurity culture" OR "cybersecurity culture" OR "global culture of cybersecurity" OR "global information security Culture" OR "global cyber-security culture"))

Resources to be searched for white literature (WL)

Digital libraries to be searched for finding relevant white literature are shown in Table 4. Additionally, the snowballing technique will be utilized to enhance the list of white literature to extend the search results, and to identify more relevant sources (Wohlin, 2014).

Table 3: Digital libraries for searching white literature (WL)

S.NO	Name of Databases
•	IEEE Xplore
•	ACM Digital Library
•	Science Direct
•	Springer Link
•	Wiley Online Digital Library
•	Google Scholar (Search Engine)

Resources to be searched for grey literature (GL)

The same search string mentioned in Table 3 will be used to find grey literature related to global cybersecurity culture, adhering to the strategies and guidelines advocated by Garousi et al. (Garousi et al., 2019). The same approach has also been suggested by other researchers (Abrar et al., 2023; Garousi et al., 2019).

- Google and Bing search engines
- ProQuest dissertations and thesis global databases, Opengrey, and Networked Digital Library of Theses and Dissertations (NDLTD)
- Website of United Nations,World Bank (WB), World Economic Forum (WEF), ENISA, ITU, SCO, OAS, ASEAN, BRICS, G8/G20, NATO, OECD, and OSEC.
- Direct contact or via social media: Individuals will be contacted directly, through email, or social media to provide their unpublished grey literature. We joined popular LinkedIn groups related to cybersecurity. 'Cybersecurity' has a total of 22,321 members, 'Cybersecurity community' has 5,349 members, 'NIST cybersecurity professional' comprising a total of 11,042 members, 'Cybersecurity Professionals' comprising a total of 54,512 members. Facebook-related groups: Global Cybersecurity Enthusiasts having 3,210 members, Global Cybersecurity Networks comprise of 6,100 members, Cyber Security Updates comprise of 6,900 members, Cyber Security Community having 31,000 members, CyberSecurity having 86,000 members, Cybersecurity Lounge having 162,000 members, Cyber Security Research having 1,400 members, and Global Cybersecurity comprise of 4,200 members.
- Reference lists and backlinks: Backlinks and forwardlinks will be used to search for relevant sources.

Search Result Management

In order to ensure efficient retrieval, each reference will be given a unique tracking number, structured as "database name/page number/serial number". Duplicate articles/sources will be identified and removed, especially when the same article appears in multiple databases/sources. Grey literature will also be assigned a tracking number, structured as “serial number/source/type”. By capturing and storing search result images in a dedicated directory, transparency will be enhanced throughout the process. The attributes of white and grey literature for initial listing are provided in Table 5 and Table 6.

Table 4: Fields/attributes of listing search result of White Literature (WL)

S.NO	Fields/attributes of white literature (WL)
i.	Tracking ID
ii.	Year of publicaton
iii.	Title of the research article
iv.	Type of article
v.	Database/Digital library
vi.	Remarks

Resources selection for white and grey literature

This section describes the criteria for the final paper selection from the initial total retrieved publications. Relevant publications will be included in the final selection process and irrelevant publications will be ignored, by using the Tollgate approach and inclusion/exclusion criteria (Afzal et al., 2009).

Table 5: Fields/attributes of listing search result of white literature (WL)

S.NO	Fields/attributes of grey literature (GL)
i.	Tracking ID
ii.	Year of Publicaton
iii.	Title of the grey source
iv.	Type of the grey source
v.	Producer organization name
vi.	Authors name(s)
vii.	Hyperlink
viii.	Date of publishing
ix.	Access date
x.	Remarks

Inclusion/Exclusion criteria of the white literature (WL)

This section defines the inclusion and exclusion criteria that analyze the overall search results and exclude the literature that is not relevant to the research topic of global cybersecurity culture. The inclusion criteria for white literature are provided in Table 7, and the exclusion criteria are given in Table 8.

Table 6: Inclusion criteria for White Literature (WL)

S.NO	Inclusion Criteria
i.	Conferences or journal publications relevant to the global cybersecurity culture.
ii.	Publications which describe the challenges/barriers/risks/issues in the context of global cybersecurity culture.
iii.	Publications which discuss various practices/solutions for the cybersecurity challenges.

The exclusion criteria for white literature are given below.

Table 7: Exclusion criteria for White Literature (WL)

S.NO	Exclusion Criteria
i.	Publications, those are not relevant to the global cybersecurity culture
ii.	Publications that are written in languages other than English.
iii.	Duplicate piece of literature related to the research questions.
iv.	Publications whose full text is not available online.
v.	Publications those are not relevant to the research questions.

Inclusion/Exclusion criteria of the grey literature (GL)

Based on the guidelines provided by Garousi et al. (Garousi et al., 2019), the inclusion and exclusion criteria of grey sources will be applied, as outlined in Table 9 and Table 10. All possible sources will be considered if written in the English language and fulfill the criteria.

Table 8: Inclusion criteria for Grey Literature (GL)

S.NO	Inclusion Criteria for GL
i.	Grey literature sources that explain global cybersecurity culture.
ii.	Grey literature sources that discuss challenges and best practices of global cybersecurity culture.
iii.	Guidelines, policies, white papers, standards, and reports published by organizations and vendors.

The following are the conditions and criteria for excluding irrelevant grey sources:

Table 9: Exclusion criteria for Grey Literature (GL)

S.NO	Exclusion Criteria for GL
i.	Grey literature sources that are not relevant to global cybersecurity culture.
ii.	Grey literature sources that are written in languages other than English.
iii.	Duplicate pieces of literature related to the research questions.
	Grey literature sources for which the full text is not available online.

Primary sources selection criteria of the white literature (WL)

The primary source selection process is a major step in a multi-vocal literature review (MLR). For primary source selection, the tollgate technique proposed by (Afzal et al., 2009) will be used, which includes a comprehensive search using the search string we formulated. In the second phase,title and abstract review will be conducted to remove irrelevant studies. Similarly, in the third phase, the shortlisted sources will be reviewed by the introduction and conclusions section. In the last phase, a thorough review will be performed of the full text of the publications shortlisted to achieve the final list of primary sources.

Primary sources selection criteria of the grey literature (GL)

Following the recommendations of Garousi et al. (Garousi et al., 2019), the process of selecting grey literature involves conducting searches on general web search engines, specialized relevant online databases/websites, and social media platforms such as Twitter, Facebook, YouTube, and others using customized search terms. The searching and selection process of grey literature can be challenging due to its wide variety and less controlled nature. Therefore, it is important to have careful selection criteria that take into account source type, inclusion/exclusion criteria, and proper quality assessment criteria.

Combining final selection of the white and grey literature

After completing the source selection process for the academic/white and grey literature, both will be combined.

Quality assessment of the selected sample of the white and grey literature

The quality and credibility of articles are crucial. Therefore, to select the final white literature sources, we will use the quality assessment criteria for white literature outlined in Table 11. We will assess quality using a three-tier scale (yes=1, partially=0.5, and no=0), following the recommendations of Da Silva et al. (Da Silva et al., 2011). Similar three-tier scale criteria will be used to filter low-quality grey literature, as shown in Table 12.

Data extraction form for multi-vocal literature review

The attributes of sources that will be extracted for grey and white literature are shown in Table 13. Once this stage is complete, a secondary reviewer will conduct an inter-rater reliability test, utilizing a quality checklist and involving two reviewers. If the extracted data are similar, they will be accepted. However, if there are differences, the primary reviewer will repeat the process.

Table 10: Quality assessment criteria of the white literature (WL)

S.NO	Quality assesment criteria of white literature (WL)	Likert Scale
WL_QA1	Does the study discuss the global cybersecurity culture?	Yes=1, Partially=0.5, No = 0
WL_QA2	Does the publication discuss challenges/riskds/barriers that are to be avoided for building and maintaining global cybersecuirty culture.	
WL_QA3	Does the publication discuss practices/solutions for the challenges to be avoided in the development and maintenance of global cybersecuirty culture.	
WL_QA4	Does the paper report clear results?	
WL_QA5	Are the findings of the paper based on clear stated research methodology?	
WL_QA6	Does the publication have clear stated goal/research questions?	

Table 11: Quality assessment Criteria of Grey literature (GL)

S.NO	Quality assesment criteria of grey literature (GL)	Likert Scale
GL_QA1	Is the publishing organization renowned and reputable?	Yes=1, Partially=0.5, No = 0
GL_QA2	Does the source clearly state its aims and objectives?	
GL_QA3	Is there a clear stated methodology used in the work?	
GL_QA4	Does the sources have references related to Global Cybersecurity Culture?	
GL_QA5	Is the publication date explicitly stated?	
GL_QA6	Does the study discuss the global cybersecurity culture?	
GL_QA7	Does the work discuss challenges/risks/issues/barriers that are to be avoided for building and maintaining global cybersecuirty culture.	
GL_QA8	Does the work discuss practices/solutions for the challenge to be avoided in the development and maintenance of global cybersecuirty culture.	

Data Synthesis

During the data synthesis phase of this MLR, we will review sources and organize data into meaningful categories in order to identify relationships and connections among the collected data points. The objective of this phase is to generate inferences and draw conclusions that address the research questions. The data will be summarized in a synthesis table stored in MS Excel format, and the final results will be published in relevant research journals.

Validation of the MLR Protocol

The research supervisor continuously reviewed the MLR protocol during the development of its various phases. After completing the MLR protocol, it was presented to the software engineering research group (SERG-UOM) and at the workshop titled "Software Engineering Aspects of Cybersecurity and Artificial Intelligence: Current Trends and Vision for the Next Decade" held in April 2024 at the Department of CS&IT, University of Malakand. The protocol was then revised based on the feedback received.

CONCLUSION AND FUTURE WORK

This MLR protocol provides a systematic approach to comprehensively review the literature on global cybersecurity culture. It includes both academic and grey literature sources to ensure a thorough understanding of the current state-of-the-art in global cybersecurity culture. The proposed multilevel model by M. Erez et al. serves as a framework for understanding cybersecurity culture across personal, group, organizational, national, and global levels and highlights the interconnections and mutual influence among these levels. By synthesizing and analyzing the findings, this MLR protocol aims to identify key challenges, success factors, and practices in the existing literature, offering valuable insights to the field of cybersecurity research. We are currently in the implementation phase of this MLR and plan to publish the final results in relevant research journals. Additionally, future studies could explore emerging technologies or evolving threat landscapes on global cybersecurity practices. This MLR protocol sets the foundation for ongoing research to enhance our understanding of global cybersecurity culture and to inform cybersecurity policy and practice.

Table 12: Data extraction form for global cybersecurity culture

S.NO	Data Extraction Attributes for White Literature (WL)	Data Extraction Form/Attributes for Grey Literature (GL)
i.	Date of Review	Date of Review
ii.	Serial Number	Serial Number
iii.	Tracking ID	Tracking ID
iv.	Source Title	Source Title
v.	Author(s) Name(s)	Source Hyperlink, date/time accessed
vi.	Year of Publiction	Author(s) Name(s)
vii.	Database/Search Engine	Year/date of online availibility of article/reports/blog
viii.	Methodology (Questionnaire Review, Interview, Case Study, Report, Survey, etc.)	Organization Name if any
ix.	Domains and dimension of global cybersecurity culture, as mentioned in the paper, if any	Domains and dimension of global cybersecurity culture, as mentioned in the paper/report, if any
x.	Challenges to be avoided in building and maintaing a Global Cybersecurity Culture, as mentioned in the paper/report, if any	Challenges to be avoided in building and maintaing a Global Cybersecurity Culture, as mentioned in the article/report, if any
xi.	Success factors to be followed in building and maintaining a global cybersecurity culture, as mentioned in the paper, if any.	Success factors to be followed in building and maintaining a global cybersecurity culture, as mentioned in the paper/report, if any.
xii.	Best Practices for building Global Cybersecuirty Culture, as mentioned in the paper, if any	Best Practices for building Global Cybersecuirty Culture, as mentioned in the article/report, if any

REFERENCES

Abrar, M. F., Khan, M. S., Khan, I., Ali, G., & Shah, S. (2023). Digital Information Credibility: Towards a Set of Guidelines for Quality Assessment of Grey Literature in Multivocal Literature Review. *Applied Sciences*, *13*(7), 4483-4483.

Adéleda Veigaa, N. M. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72-94. https://doi.org/10.1016/J.COSE.2017.05.002

Afzal, W., Torkar, R., & Feldt, R. (2009). A systematic review of search-based testing for non-functional system properties. *Information and Software Technology*, *51*(6), 957-976.

AlHogail, A., & Mirza, A. (2014a). Information security culture: a definition and a literature review. 2014 World Congress on Computer Applications and Information Systems (WCCAIS),

Alhogail, A., & Mirza, A. (2014b). A proposal of an organizational information security culture framework. *Proceedings of 2014 International Conference on Information, Communication Technology and System, ICTS 2014*, 243-249. https://doi.org/10.1109/ICTS.2014.7010591

Alnifie, K. M., & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. *Journal of Information Security*, *14*(2), 93-110.

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing 2014 41:1*, *41*(1), 22-28. https://doi.org/10.3103/S0147688214010067

Camino, K. (2017). *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* (United Nations Institute for Disarmament Research (UNIDIR), Issue. https://unidir.org/wp-content/uploads/2023/05/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Chen, E. T. (2023). The Importance of Cybersecurity for Organizations: Implementing Cybersecurity to Prevent Cyberattacks. In *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 46-58). IGI Global.

Creese, S., Bada, M., Ignatuschstschenko, L., & Roberts, T. (2017). Cybersecurity Capacity Maturity Model for Nations (CMM), revised edition. In: Oxford: Global Cyber Security Capacity Centre. Available at www. sbs. ox. ac ….

Cybersecurity Act of the European Union. (2019).

Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition. (2021).

Da Silva, F. Q. B., Santos, A. L. M., Soares, S., França, A. C. C., Monteiro, C. V. F., & Maciel, F. F. (2011). Six years of systematic literature reviews in software engineering: An updated tertiary study. *Information and Software Technology*, *53*(9), 899-913.

Da Veiga, A. (2009). Cultivating and assessing information security culture ISCF analysis. In: University of Pretoria.

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI Computing Conference (SAI),

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713-101713.

Dorosh, M., Voitsekhovska, M., & Balchenko, I. (2020). Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. *Advances in Intelligent Systems and Computing*, *938*, 503-512. https://doi.org/10.1007/978-3-030-16621-2_47/COVER

ENISA National Cyber Security Strategy Good Practice Guide. (2012).

Erez, M., & Gati, E. (2004). A dynamic, multi-level model of culture: From the micro level of the individual to the macro level of a global culture. *Applied Psychology*, *53*(4), 583-598. https://doi.org/10.1111/J.1464-0597.2004.00190.X

Fisher, R., Porod, C., Organizational, S. P. J. o., & Undefined. (2021). Motivating employees and organizations to adopt a cybersecurity-focused culture. *search.proquest.com*. https://search.proquest.com/openview/3833f1f4fe5ed2962c59695949fa8009/1?pq-origsite=gscholar&cbl=1576346

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*, 101-121. https://doi.org/https://doi.org/10.1016/j.infsof.2018.09.006

Gcaza, N., & von Solms, R. (2017a). Cybersecurity culture: an ill-defined problem. IFIP World Conference on Information Security Education,

Gcaza, N., & Von Solms, R. (2017b). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1-17.

GCSC. (2019). *Promoting stability in cyberspace to build peace and prosperity*.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, 1-11. https://doi.org/10.1080/08874417.2020.1845583

Ghernaouti-Hélie, S. (2009). An inclusive information society needs a global approach of information security. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 658-662. https://doi.org/10.1109/ARES.2009.127

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. 2010 International Conference on Availability, Reliability and Security,

Granova, V., Mashatan, A., & Turetken, O. (2023). Changing Hearts and Minds: The Role of Cybersecurity Champion Programs in Cybersecurity Culture. International Conference on Human-Computer Interaction,

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726-102726. https://doi.org/10.1016/J.JISA.2020.102726

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/EJIS.2009.6/TABLES/6

Holiness Nikel, F., & Oguejiofor Amaechi, A. (2022). An Assessment of Employee Knowledge, Awareness, Attitude towards Organizational Cybersecurity in Cameroon. *scholar.archive.org*, *7*(1), 2022-2022. https://doi.org/10.5539/nct.v7n1p1

Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. *Applied Sciences*, *12*(8), 3953-3953.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189. https://doi.org/10.1007/S13369-019-04319-2/TABLES/9

Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 76-108.

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*. https://doi.org/10.1109/CYBERSECPODS.2019.8885240

ITU. (2021). *ITU Guide to Developing aNational CybersecurityStrategy 2021* (Strategic Engagement in Cybersecurity, Issue. https://www.itu.int/pub/D-STR-CYB_GUIDE.01

Jansen Van Vuuren, J. C., Gcaza, N., Gcaza, N., Von Solms, R., & Van Vuuren, J. (2015). An Ontology for a National Cyber-Security Culture Environment. *researchgate.net*, 1-1. https://www.researchgate.net/profile/Noluxolo-Gcaza/publication/306292545_An_Ontology_for_a_National_Cyber-Security_Culture_Environment/links/59c4b73baca272c71bb60487/An-Ontology-for-a-National-Cyber-Security-Culture-Environment.pdf

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-08-2022-0139/FULL/PDF

Karyda, M. (2017). Fostering Information Security Culture In Organizations: A Research Agenda. *MCIS 2017 Proceedings*. https://aisel.aisnet.org/mcis2017/28

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. *2*.

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering – A tertiary study. *Information and Software Technology*, *52*(8), 792-805. https://doi.org/10.1016/J.INFSOF.2010.03.006

Klein, G., & Zwilling, M. (2023). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. *Journal of Computer Information Systems*, 1-15.

Mahmudova, R. S. (2023). Cyber-physical Systems: Security Problems and Issues of Personnel Information Security Culture. *I. J. Education and Management Engineering*, *2023*, *2*,, *2*, 18-26 https://doi.org/10.5815/ijeme.2023.02.03

Matsumoto, D., ed. (2019). The Handbook of Culture and Psychology. *The Handbook of Culture and Psychology*. https://doi.org/10.1093/OSO/9780190679743.001.0001

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.3551&rep=rep1&type=pdf

Mwim, E. N., Mtsweni, J., & Chimbo, B. (2023). Conceptual Mapping of the Cybersecurity Culture to Human Factor Domain Framework. Future of Information and Communication Conference,

Naseir, M. A. B. (2021). National cybersecurity capacity building framework for counties in a transitional phase. http://eprints.bournemouth.ac.uk/35646/

Niekerk, J. V., & Issa, R. V. S. (2006). Understanding Information Security Culture: A Conceptual Framework.*Citeseer*.https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.125&rep=rep1&type=pdf

NIST Cybersecurity Framework (CSF). (2018).

Odebade, A. T., & Benkhelifa, E. (2023). A Comparative Study of National Cyber Security Strategies of ten nations. *arXiv preprint arXiv:2303.13938*.

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing information security culture: A critical analysis of current approaches. 2012 Information Security for South Africa,

Paziuk, A., & Mitsik, V. (2019). Global cybersecurity culture in the international discourse: values and principles. *National Academy of Managerial Staff of Culture & Arts*(2), 103.

Pullin, D. W. (2018). Cybersecurity: Positive Changes Through Processes and Team Culture. *Front Health Serv Manage*, *35*(1), 3-12.https://doi.org/10.1097/HAP.0000000000000038

Reegård, K., Blackett, C., & Katta, V. (2020). The Concept of Cybersecurity Culture. 4036-4043. https://doi.org/10.3850/978-981-11-2724-3_0761-CD

Sabillon, R. (2022). The cybersecurity audit model (CSAM). In *Research Anthology on Business Aspects of Cybersecurity* (pp. 77-139). IGI Global.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2018). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, *2017-November*, 253-259. https://doi.org/10.1109/INCISCOS.2017.20

Santos, P., Peixoto, M., & Vilela, J. (2021). Understanding the Information Security Culture of Organizations: Results of a Survey. XVII Brazilian Symposium on Information Systems, New York, NY, USA.

Schjølberg, T. (2020). *Guidelines for utilization of the global cybersecurity agenda (GCA)* (Report by the Secretary-General, International Telecommunication Union (ITU), Issue. https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change (cyber security culture behavior model). *South African Computer Journal*, *2003*(31), 46-52.

Sharma, M., Pant, S., Yadav, P., Sharma, D. K., Gupta, N., & Srivastava, G. (2023). Advancing security in the industrial internet of things using deep progressive neural networks. *Mobile Networks and Applications*, 1-13.

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, *120*, 102774-102774.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, *119*, 102756-102756. https://doi.org/10.1016/J.COSE.2022.102756

Stein, S. (2007). *ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)*.

Stein, S., & Solange, G.-H. (2011). A Global Treaty on Cybersecurity and Cybercrime, Second edition. *Cybercrime Law*. https://www.scarg.org/wp-content/uploads/2013/10/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf

Tallón-Ballesteros, A. (2021). Assessment of National Cybersecurity Capacity for Countries in a Transitional Phase: The Spring Land Case Study. *Modern Management Based on Big Data II and Machine Learning and Intelligent Systems III: Proceedings of MMBD*, 144.

Touré, H. I., & Schjølberg, S. (2007). *ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Chairman's Report*. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

Tziarras, Z. (2014a). The Security Culture of a Global and Multileveled Cyber Security. In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory*. https://doi.org/10.1007/978-1-4939-1028-1_13

Tziarras, Z. (2014b). The security culture of a global and multileveled cybersecurity. In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory* (pp. 319-335). Springer New York. https://doi.org/10.1007/978-1-4939-1028-1_13/COVER

Creation of a global culture of cybersecurity :resolution, (2003). https://digitallibrary.un.org/record/482184/files/A_RES_57_239-EN.pdf

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures: resolution, (2009).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (2015). https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf

Convention on Cybercrime /Budapest Convention, (2004). https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280071e5b&clang=_en

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. ISSA,

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. Proceedings of the 18th international conference on evaluation and assessment in software engineering,

Yoo, C., Goo, J., & Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *Management Information Systems Quarterly*, *44*(2). https://aisel.aisnet.org/misq/vol44/iss2/15