Towards Cultivating a Global Cybersecurity Culture: A Multivocal Literature Review of Challenges and Practices

Nisar Muhammad[*], Siffat Ullah Khan[†]

Abstract

Cybersecurity is a critical global concern that transcends national borders and requires coordinated responses. Cyber threats are becoming more frequent, sophisticated, and impactful. Existing research highlights that solutions that focus on technical, organizational, or individual aspects are insufficient to effectively secure cyberspace. In response, the development of Global Cybersecurity Culture (GCSC) has been recognized as a collective and long-term approach for mitigating the real-world impact of these cyber threats. However, limited studies have focused on how a GCSC can be developed and operationalized. In this study, we conducted a Multivocal Literature Review (MLR) to identify critical challenges and their associated practices that hinder the development of GCSC. This MLR was conducted following the established guidelines for MLR in Software Engineering research. A total of 39 primary studies, including both peer-reviewed and Grey Literature (GL) sources, were selected from an initial search of 3,549 literature sources. It identified 13 Critical Challenges, such as Lack of political consensus, the absence of international cyber law, digital sovereignty disputes, disputes over digital human rights, and lack of national cybersecurity capabilities. It also identified 41 associated practices to address these challenges. Furthermore, the identified challenges were clustered into four cultural layers including Knowledge, Tacit Assumptions, Espoused Values, and Artefacts, to provide a structured understanding of how they influence the development of GCSC. This research provides a basis for the development and operationalization of a GCSC by identifying its critical challenges and their associated practices. It also provides a foundation for future research and may inform the future development of maturity assessment models for GCSC.

Keywords: Multivocal Literature Review, Cybersecurity, Software Engineering, Global Cybersecurity Culture, Challenges, Practices.

Introduction

Cybersecurity is not a technical concern only, instead it evolved into a socio-political challenge at the global level. Common challenges reported in literature include technological interdependence, geopolitical tensions, absence of regulatory framework, and social concerns that require active international cooperation to protect cyberspace from cyber threats (Gurung, 2025; Pernice, 2018; Tziarras, 2014). Cyber threats not only compromise digital systems but also threaten economic security,

[*]Corresponding Author: Software Engineering Research Group (SERG), Department of Computer Science & IT, University of Malakand, Pakistan, nisarmuhammad@kp.gov.pk
[†]Software Engineering Research Group (SERG), Department of Computer Science & IT, University of Malakand, Pakistan, siffatullah@uom.edu.pk

democratic processes, and basic human rights (World Economic, 2025). Alongside day-to-day activities the world economies also shifted toward digital models. The security of data and business operations has become critical than ever and require strong and proactive cybersecurity measures (Adejumo & Ogburie, 2025; Al-ma'aitah, 2022). According to Cybersecurity Ventures, it is expected that cybercrimes at global level will cost the world $9.5 trillion USD in 2024 and reach $10.5 trillion USD by 2025 (Steve, 2023). On the other hand, this digital interdependence has also increased national security concerns due to the borderless nature of these cyber threats (Krishna et al., 2022). Cyber-attacks targeting critical infrastructures such as ransomware attacks, disinformation campaigns sponsored by state and non-state actors, and data breaches reveal that modern cyber threats increasingly exploit gaps in collective resilience rather than relying on technical vulnerabilities only (Cyberspace, 2020; World Economic, 2025).

Despite advances in technical and policy frameworks, including the United Nations (UN) Resolution 57/239, on the creation of a global culture of cybersecurity, responses remain fragmented across national jurisdictions (Camino, 2017). These fragmented approaches have been unable to effectively address the transnational nature of cyber threats for several reasons (Open-ended Working, 2021; Pernice, 2018; Pijović, 2021). First, the globalization of information systems has enabled organizations to operate across national borders. This interconnectedness facilitates business operations. However, it also increases vulnerabilities and exposes information systems to cyber-attacks. Second, human mistakes still play an important role in data breaches, and consequently, it has gained attention in cybersecurity research. Third, differences in cybersecurity laws, policies, and practices across countries create security gaps and inhibit effective international cooperation. Fourth, differences between sovereignty-centric and multi-stakeholder approaches to cybersecurity governance make it difficult to achieve international consensus and coordinated action. Finally, limited cybersecurity awareness and education leaves individuals and organizations vulnerable to cyber-attacks.

These challenges demonstrate that cybersecurity is not only a technical problem but a multidisciplinary challenge shaped by technological, legal, organizational, political, and human factors (Ghernaouti-Hélie, 2009; Pernice, 2018). To address this multidisciplinary challenge, the UN, through Resolutions 57/239 and 70/237, has emphasized the development of Global Cybersecurity Culture (GCSC) as a collective and long-term approach for strengthening cybersecurity (UNGA, 2003, 2009).

GCSC refers to the shared norms, values, and practices related to cybersecurity that are practiced at the global level while respecting local experiences and realities. Its importance is widely acknowledged, and various international and regional together with researchers, have proposed a range of solutions to operationalize GCSC (International Telecommunication, 2024; Paziuk & Mitsik, 2019; UN Institute for Disarmament, 2017). However, GCSC has not yet been fully operationalized because of its multidisciplinary nature, which requires coordination among researchers from different disciplines as well as regional and international organizations. It requires the integration of technical tools, legal frameworks (law), behavioral insights (psychology), social dynamics (sociology), and geopolitical coordination (international relations and political science) to safeguard our interconnected world (Kesler, 2024; Paziuk & Mitsik, 2019; Pernice, 2018). Prior research has examined cybersecurity challenges in isolation, such as technical analyses of malware propagation, public awareness campaigns, and policy studies related to cybersecurity (Abdo & Hossain, 2025; Gevorgyan et al., 2025; Khadka & Ullah, 2025; Pierucci, 2025; Singh et al., 2026). GCSC is a dynamic, multi-level, multi-layer, and multidisciplinary construct that requires a comprehensive interdisciplinary approach to address its broad scope and complex nature, as shown in Figure 1 (Erez & Gati, 2004; Niekerk & Issa, 2006; Reegård et al., 2020). Figure 1 illustrates the conceptual nature of GCSC. Cybersecurity culture is not a static, it is a dynamic concept that evolves continuously through experience, learning, feedback, and adaptation in response to emerging cyber threats (Erez & Gati, 2004). GCSC operates at multiple levels of governance, is shaped by multiple layers of culture, and integrates knowledge from diverse academic disciplines (Niekerk & Issa, 2006; Paziuk & Mitsik, 2019; Reegård et al., 2020). Together, these characteristics highlight the complexity of GCSC and emphasize that collective commitment, shared responsibility, and continuous collaboration are required to strengthen it. However, existing literature lacks a Multivocal Literature Review (MLR) that brings together findings from both academic and Grey Literature (GL) to examine the challenges and their associated practices for developing and operationalizing a GCSC.

To address this gap, this study conducts MLR, following the established Software Engineering guidelines, to identify the critical challenges and associated practices for developing and maintaining a GCSC. By investigating the following research questions, this study identifies 13 challenges and 41 practices to address them.

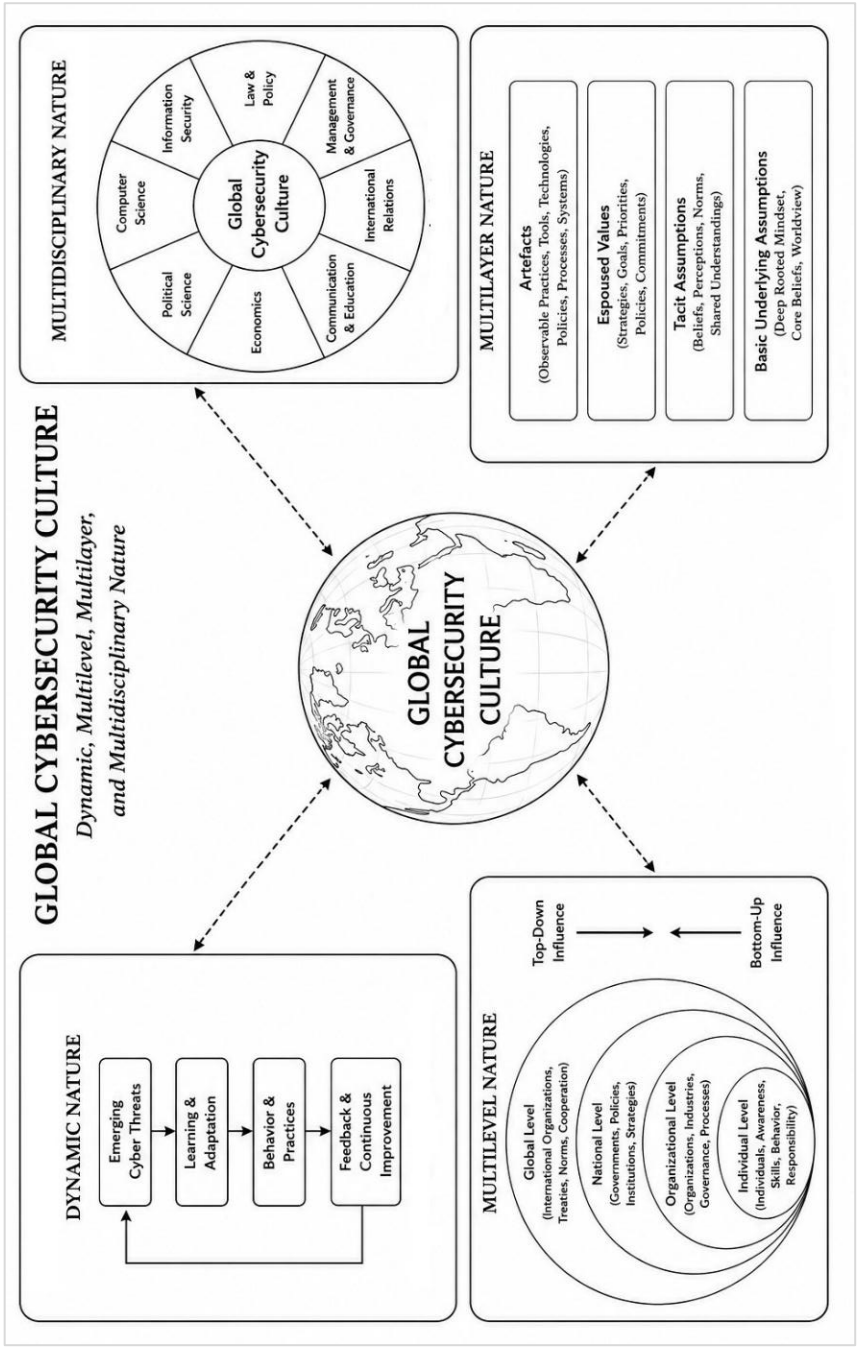


Figure 1: GCSC is a dynamic, multi-level, multi-layer, and multidisciplinary Concept (Erez & Gati, 2004; Niekerk & Issa, 2006; Reegård et al., 2020).

RQ1: What are the challenges that hinder the development and maintenance of GCSC from a Software Engineering perspective?
RQ2: What practices can be adopted to address the identified challenges of the GCSC?
RQ3: Do the identified challenges differ across research methodologies?
RQ4: Do the identified challenges differ across publication periods?

The remainder of this paper is organized as follows. The related work is presented in the Literature Review section. The research methodology is described in the Research Methodology section. The identified challenges and associated practices are presented and analyzed in the Results and Analysis section. The study limitations are discussed in the Threats to Validity section. Finally, the Conclusion and Future Research section summarizes the study and outlines directions for future work.

Literature Review

The present body of literature on the GCSC of cybersecurity is still relatively new and has not yet been thoroughly studied (Hurel & Lobato, 2018; Paziuk & Mitsik, 2019). Existing literature reveals fragmented efforts to reconcile technical, legal, and socio-political dimensions to enhance GCSC and promote responsible behavior in cyberspace (Camino, 2017; Meyer, 2020; Portnoy & Goodman, 2009).

While prior efforts have made progress and laid a solid foundation, three persistent and interrelated challenges undermine its effectiveness: geopolitical divisions over cybersecurity governance, the misalignment between cybersecurity policies and actual online behavior, and significant disparities in national technical and policy capabilities (Khan et al., 2024; World, 2024).

Table 1 summarizes key contributions to cultivating a GCSC and shows that previous research has addressed these challenges primarily from isolated technical, legal, or geopolitical perspectives. This fragmented approach highlights the need for a MLR to thoroughly review all available knowledge across disciplines and stakeholders for building and maintaining a GCSC.

Overall, previous studies have made important contributions to GCSC through technical, legal, governance, and policy initiatives. However, these efforts remain fragmented, and no systematic review has comprehensively synthesized the critical challenges and associated practices. This MLR addresses this gap by integrating evidence from both published and GL.

Table 1: Overview of existing work on developing and maintaining GCSC.

Reference	Contributions	Limitations
UN GA Resolution 57/239 (UNGA, 2003, 2009)	First formal recognition of GCSC; promoted international cooperation	Non-binding and lack of enforcement mechanism
Council of Europe Convention on Cybercrime (UNISA, 2004)	First international treaty on cybercrime; harmonized laws across borders	Limited to EU
Paris Call for Trust and Security (Cyberspace, 2020; Paris Call for Trust and Security in Cyberspace, 2018),	Multi-stakeholder pledge for cyberspace stability; endorsed by 80+ countries	Voluntary; no accountability framework.
ITU Global Cybersecurity Agenda (GCA) (Touré & Schjølberg, 2007)	Framework for capacity building in developing nations.	Primarily technical and overlooked socio-political aspects
UNGGE Reports (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013; "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 2015), OEWG Framework (Open-ended Working, 2021), ICT4PEACE norms project (Kerttunen & Kiisel, 2015)	Voluntary cyber norms and political consensus.	limited consensus on the adoption of these norms
Tallinn Manual 2.0 (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013),	Good initiative for regulating cyber operations.	It was a non-binding initiative with western centric perspective
Microsoft's Cybersecurity Norms (Five Principles for Shaping Cybersecurity Norms, 2013; Microsoft International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World, 2014)	Proposed private sector initiative and norms	Governments consideration and adoption issue
Geneva Manual 2024 (Anastasiya Kazakova & Droz, 2023; Geneva Declaration of Principles and Plan of Action World Summit on Information Society, 2005),	Multi-stakeholder principles for responsible state behaviors.	New; untested implementation
OSCE/OECD Cyber Guidelines (McDowell et al., 2014; OECD, 2002),	Confidence building measures.	Applied on member states; lacks global applicability
ASEAN (Kai Lin, 2023; Work plan on security of and in the use of Information and Communications Technologies (ICT), 2015), EU Regional Frameworks (Cyber Diplomacy Toolbox, 2017), Shanghai Cooperation Organization (SCO) Cyber Framework (International Code of Conduct for Information Security, 2015)	Regional initiatives	Fragmented; no alignment with global initiatives
UNIDIR Research (Camino, 2017)	Analysis of cyber norms' implementation challenges	Academic; limited influence on policy
Global Commission on Stability of Cyberspace (GCSC) (Marina & Michael, 2019)	Proposed 8 cyber norms.	Non-binding; dissolved in 2019
Security Culture of a Global and Multileveled Cyber Security (Tziarras, 2014)	Developed a global framework of global cybersecurity.	Overlooks geopolitical tensions; assumes cultural homogeneity across regions.

Research Methodology

We employed a MLR to integrate technical, policy, and behavioral perspectives and analyze the fragmented landscape of GCSC. MLR extends the conventional Systematic Literature Reviews (SLRs) and includes GL, such as policy documents, industry reports, research theses, government publications, blogs, and white papers, in addition to peer-reviewed research (Garousi et al., 2019). This method has also been used in prior studies (Ben Amor et al., 2025). This dual approach enables us to investigate cybersecurity challenges and their associated practices from an interdisciplinary perspective (Muhammad & Khan, 2024; Muhammad et al., 2026). The steps of the MLR methodology are described below.

Search Strategy

This study employed a systematic search strategy to cover the broad spectrum of studies on the GCSC in both academic and GL. The entire search process is thoroughly documented, including the selected databases, search strings, inclusion and exclusion criteria, and study limitations.

MLR Protocol Development

The protocol of the this MLR has been already published (Muhammad & Khan, 2024). This reduces the risk of bias and improve the transparency of the review process.

Search Strings Development

To structure our research questions, we used the PICO framework, as explained in Table 2. Our research questions are formulated as below:
[What are the challenges and their practices?] ------ “INTERVENTION”
In the context of [Global Cybersecurity Culture] ------“POPULATION”
To be addressed for [developing and maintaining a Global Cybersecurity Culture] ---------“OUTCOMES OF RELEVANCE”
for the stability and security of cyberspace.

After exploring different keyword combinations, as shown in Table 3, we formulated two search strings based on the format allowed in digital libraries and search databases.

Table 2: PICO criteria for research questions development.

PICO Criteria	Details
Population	Governments, private sectors organizations, cybersecurity professionals, policymakers, and individuals involved in GCSC
Intervention	Identification of GCSC challenges and their practices in GCSC
Experimental Design	MLR
Outcomes	List of global cybersecurity challenges and their practices for building and maintaining a global culture of digital security.

Table 3: Search string, synonyms and variations of search terms.

Keyword	Synonyms/Alternatives
GCSC	GCSC OR Global information security culture OR International cyber security culture Or Global cyber security culture
Challenges	Risks OR issues OR barriers
Practices	Practices OR solutions OR guidelines OR strategies

Using the term variations shown in Table 3, we formulated two search strings. Boolean operators (AND, OR, and NOT) were used to maximize search coverage. Some digital libraries like the Science Direct database, limit the number of Boolean operators that can be used in a single search query. Therefore, the original search string was simplified to meet these restrictions. The MLR was then performed using the following two search strings:

((“Global cybersecurity culture” OR “International cyber security culture” OR “Global cybersecurity culture” OR “Global information security culture”) AND (Challenges OR risks OR issues OR barriers Practices OR solutions OR guidelines))

((“Global cybersecurity culture” OR “cybersecurity culture” OR “global cyber security culture” OR “Global information security Culture” OR “global cyber-security culture”))

Academic Databases Searched

Academic literature was obtained from the main scientific databases. The following academic databases and GL sources were searched.

1. IEEE Xplore (www.ieeexplore.ieee.org)
2. SpringerLink (www.springerlink.com)
3. Google Scholar (Search engine) (scholar.google.com)
4. ACM digital library (www.acm.org)
5. Science Direct digital library (www.sciencedirect.com)
6. Wiley Online Library (onlinelibrary.wiley.com)

Grey Literature (GL) Sources Searched

GL was searched through government reports, policy documents, white papers, industry publications, and publications from international and regional organizations. For GL retrieval, Google and Bing search engines were used, along with the official websites of relevant organizations, such as the UN, NIST, and ENISA. In addition, specialized databases, including ProQuest, OpenGrey, and the Networked Digital Library of Theses and Dissertations (NDLTD), as well as relevant social media platforms, were searched to identify additional GL.

Snowballing Technique

The snowballing technique was conducted using the established guidelines proposed by Wohlin et al. (Wohlin, 2014). Snowballing was used after the initial search to identify relevant studies that may have been missed. This involved reviewing the reference lists of the selected studies (backward snowballing) and examining studies that cited them (forward snowballing). This process improved the coverage of the review by identifying additional relevant publications. Similar approaches have also been used in previous studies.

The retrieved publications were subsequently screened and selected using a structured study selection process, as described in the next section.

Primary Sources Selection

Organized screening of the retrieved literature was performed based on the pre-defined inclusion and exclusion criteria. Furthermore, a multi-stage Tollgate selection process was used to identify studies relevant to this review.

Table 4: Inclusion and Exclusion Criteria for the formal studies.

Inclusion Criteria for White Literature (WL)	Exclusion Criteria for WL
Conferences or journal publications relevant to the GCSC.	Publications, those are not relevant to the GCSC.
Publications which describe the challenges/barriers/risks/issues in the context of GCSC.	Publications written in other languages than English and not available online.
Publications which discuss various practices for the cybersecurity challenges.	Duplicate articles retrieved during search process in multiples databases or repositories.

Inclusion and Exclusion Criteria

The inclusion and exclusion criteria for both academic and GL were defined to ensure that only relevant articles were selected for the final sample, making the process of data extraction and subsequent analysis more efficient. The inclusion criteria for white studies are given in Table 4. Moreover, a rigorous inclusion and exclusion criteria for GL was applied, as described in Table 5.

Table 5: Inclusion and Exclusion Criteria for the formal studies.

Inclusion Criteria for GL	Exclusion Criteria for WL
Sources of GL that is related to the GCSC.	GL sources that are not relevant to GCSC.
Sources that discuss GCSC challenges and practices.	GL sources that are written in languages other than English.
Sources that discuss best practices related to GCSC.	Duplicate pieces of literature related to the research questions.
Related guidelines, policies, white papers, and reports published by states and organizations worldwide.	Sources which the full text is not available online.

Tollgate Selection Process

For primary sources selection, we followed the Tollgate technique and the inclusion/exclusion criteria outlined for primary source selection (Afzal et al., 2009). An inter-rater reliability procedure was used to reduce selection bias and increase consistency during the study selection process. Two researchers independently screened the retrieved studies against the predefined inclusion and exclusion using Tollgate screening procedure. Any disagreements and discrepancies were discussed and consensus was reached. The Tollgate selection process has the following steps:

Step 1: We used the search strings mentioned in Table 4, to retrieve relevant publications and found a total of 3,266.
Step 2: In second step the titles as well as abstracts of the articles were reviewed and we selected 171 from the initial pool of 3,266.
Step 3: Next, the introduction and conclusion sections of the selected publications were examined and we narrowed down our selection to 54 articles.
Step 4: Finally, we analyzed the entire texts of these 54 articles and identified 24 articles for data extraction and further synthesis.

The primary source selection process using Tollgate technique is depicted in Table 6. Moreover, Figure 1 presents the publication selection process and overall MLR implementation in this research.

Table 6: Primary selection process for WL and GL sources.

S.No.	Digital Libraries and Databases	Phase-1	Phase-2	Phase-3	Phase-4	Final Selection
1.	IEEE Xplore	50	28	08	02	02
2.	SpringerLink	3091	74	18	05	04
3.	Google Scholar	51	29	18	08	08
4.	ACM Digital Library	15	09	00	00	00
5.	Wiley Online Library	12	03	00	00	00
6.	Science Direct	37	18	00	00	00
7.	Snowballing	10	10	10	10	10
8.	Sub Total (WL)	3266	171	54	27	24
9.	GL	283				20
10.	Total (GL+WL)	3549				44

Grey Literature (GL) Selection Process

Furthermore, in order to ensure a thorough selection process for GL sources, we carefully assessed the retrieved sources based on the inclusion and exclusion criteria stated in the previous section. We conducted a detailed review of the full texts of all the 283 sources and selected 24 sources which met our criteria. Since GL do not follow any standardized structure, therefore, this method helped us to search documents efficiently and thereby selecting our final sources.

A total of 44 sources were selected including both WL and GL, as provided in Table 6. In final stage, following the Quality Assessment Criteria (QAC), 39 sources were finalized, which are listed in Table 13 (Appendix A) and Table 14 (Appendix B). The MLR process is shown in Figure 2.

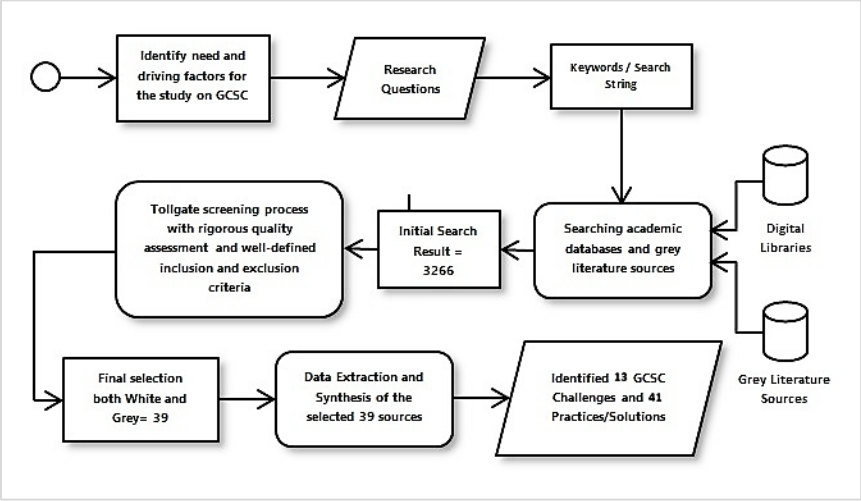


Figure 2: PRISMA process adopted in the MLR implementation

Quality Assessment Criteria (QAC)

Quality assessment was performed to ensure that only relevant and credible studies were included in the final review. Both WL and GL sources were subjected to a quality assessment using a pre-defined quality assessment checklist developed in the published MLR protocol. The relevance, credibility, methodological quality and contribution of each publication to the objectives of this study were assessed by the checklist. Each source was independently assessed using the predefined quality criteria by the reviewers. Any differences in the quality assessment were discussed and resolved by consensus under the guidance of the research supervisor. Studies that did not satisfy the minimum quality requirements were excluded from further analysis. This process improved the reliability of the review by ensuring that the final synthesis was based on high-quality and relevant evidence. The quality checklist for White Literature (WL) is given in Table 7.

To assess the quality of the selected articles, we used a three tier scale (Yes=1, partially=0.5, and NO=0) (Da Silva et al., 2011). The same is also applied to the GL quality QAC. A minimum threshold of three is set for qualifying the QAC mentioned above for WL. A total of 20

academic articles that achieved a score of three or higher were chosen for further data extraction and synthesis, as outlined in Table 13 (Appendix A).

Table 7: QAC of WL.

S.No.	QAC for WL
WL_QA1	Does the study discuss the GCSC?
WL_QA2	Does the publication discuss challenges/risks/barriers that are to be avoided for building and maintaining GCSC?
WL_QA3	Does the publication discuss practices for the challenges to be avoided in the formation GCSC.
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?

The QAC designed for GL are outlined in Table 8. To assess the quality of the selected GL sources, we used the same three tier scale criteria (Yes=1, partially=0.5, and NO=0). After evaluating the quality of the finalized sources based on the abovementioned criteria, sources that received a score of five or higher were considered. As a result, a total of 19 GL sources were selected, which can be found in Table 14 (Appendix B).

Table 8: QAC of GL.

S.No.	QAC for GL
GL_QA1	Is the publishing organization renowned and reputable?
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	Is the grey document supported by authoritative and contemporary references?
GL_QA5	Is the publication date explicitly stated?
GL_QA6	Does the study discuss the GCSC?
GL_QA7	Does the work discuss challenges/risks/issues/barriers related to GCSC?
GL_QA8	Does the work discuss practices for the global cybersecurity cultural challenge?

A total of 5 sources were excluded, both in WL and GL sources, during quality assessment process. Finally, the synthesis process was applied to the 39 selected studies, as described below.

Data Extraction and Synthesis

An inter-rater reliability procedure was also applied during the data extraction process. Two researchers independently extracted the needed data from the selected studies using a predefined data extraction form. The detail of the form has already been defined and published (Muhammad & Khan, 2024; Muhammad et al., 2026). Any discrepancies in the extracted information were discussed and consensus reached to ensure the accuracy and consistency of the extracted data.

Results and Analysis

Based on the MLR Protocol, this section synthesizes key challenges and actionable practices derived from interdisciplinary literature. The analysis provides insights for researchers, policymakers, practitioners, and other stakeholders involved in developing and maintaining GCSC.

Critical Challenges and their Practices

This MLR synthesizes 13 critical challenges and 41 actionable practices, as shown in Table 9, to advance a unified GCSC. Below, these findings are presented thematically, pairing each challenge with evidence-based practices tailored for policymakers and practitioners.

Table 9: Critical Challenges to the GCSC and their frequencies in MLR.

S.No.	GCSC Challenges	WL and GL Source IDs	Occurrences in WL and GL				Total occurrences (WL and GL)	
			WL (N=20)	WL %	GL (N=19)	GL %	Total (N=39)	Total %
CC1	Lack of international cooperation and collaboration	W1, W2, W4, W6, W7, W8, W9, W11, W12, W13, W14, W15, W16, W17, W18, W19, W20, G1, G2, G3, G4, G5, G6, G7, G8, G9, G10, G11, G12, G13, G14, G15, G16, G17, G18, G19	17	85	19	100	36	92
CC2	Evolving cyber threats and vulnerabilities	W1, W3, W4, W5, W6, W7, W9, W10, W11, W13, W14, W15, W16, W17, W18, W19, W20, G1, G2, G3, G4, G5, G6, G7, G8, G9, G10, G11, G12, G13, G14, G15, G16, G17, G18, G19	17	85	19	100	36	92
CC3	Absence of a coordinated global cybersecurity strategy	W1, W2, W4, W5, W6, W7, W9, W10, W11, W12, W13, W14, W15, W16, W17, W18, W19, W20, G1, G2, G3, G4, G5, G6, G7, G8, G10, G11, G12, G13, G14, G16, G17, G18, G19	18	90	17	89	35	90
CC4	Lack of national cybersecurity capabilities	W1, W3, W4, W5, W6, W7, W8, W9, W10, W11, W13, W14, W15, W16, W17, W18, W19, W20, G1, G3, G4, G5, G6, G7, G8, G9, G10, G11, G12, G13, G14, G16, G17, G18, G19	18	90	17	89	35	90
CC5	Lack of international consensus on digital human rights governance	W1, W2, W3, W4, W5, W6, W8, W9, W10, W11, W12, W13, W14, W15, W17, W18, W19, W20, G1, G2, G3, G4, G5, G6, G7, G8, G9, G11, G14, G15, G16, G17, G18, G19	18	90	16	84	34	87
CC6	Limited development and adoption of global cybersecurity norms	W2, W3, W4, W5, W6, W7, W8, W9, W10, W11, W13, W14, W16, W17, W18, W20, G1, G2, G4, G5, G8, G9, G10, G11, G12, G13, G14, G16, G17, G18, G19	16	80	15	79	31	79
CC7	Lack of International Political Consensus	W1, W2, W5, W6, W7, W8, W9, W10, W11, W12, W13, W14, W15, W17, W18, W20, G1, G2, G4, G5, G8, G9, G10, G11, G12, G13, G14, G16, G17, G18	16	80	14	74	30	77
CC8	Absence of international cyber law for cyberspace	W1, W2, W7, W9, W10, W11, W12, W13, W14, W15, W17, W18, W20, G1, G2, G3, G4, G5, G7, G8, G9, G10, G11, G12, G13, G16, G17, G18	13	65	15	79	28	72
CC9	Lack of Public Private Partnerships	W1, W4, W9, W10, W11, W12, W13, W14, W15, W16, W17, W18, W19, W20, G4, G5, G7, G8, G9, G10, G11, G12, G13, G14, G16, G17, G18, G19	14	70	14	74	28	72
CC10	International disputes over the interpretation of digital sovereignty	W1, W2, W7, W8, W10, W11, W13, W14, W15, W17, W18, W20, G1, G3, G5, G8, G10, G11, G13, G14, G16, G19	12	60	10	53	22	56
CC11	Absence of global governance authority for Cyberspace	W4, W8, W11, W13, W14, W15, W16, W17, W18, W19, W20, G1, G2, G3, G4, G8, G10, G13, G16, G17, G18, G19	11	55	11	58	22	56
CC12	Lack of adherence to international technical standards and best practices	W9, W10, W11, W13, W14, W16, W17, W18, W19, G1, G2, G3, G5, G9, G10, G11, G12, G14, G15, G16, G17	09	45	12	63	21	54
CC13	Lack of public awareness and education	W1, W3, W4, W5, W9, W11, W15, W16, W18, W19, G1, G3, G5, G7, G10, G11, G15, G17, G19	10	50	09	47	19	49

Clustering of GCSC Challenges Across Cultural Layers

To provide a structured understanding of the identified challenges, they were synthesized and organized into the four cultural layers that form the basis of GCSC: Knowledge, Tacit Assumptions, Espoused Values, and Artefacts, as shown in Table 10. Although the identified challenges could be grouped using different perspectives, such as governance, stakeholder groups, or technical and non-technical dimensions, this study classifies them according to the four cultural layers of GCSC. This theory-driven classification was selected because the objective of the study is to understand how the identified challenges influence the development of GCSC (Niekerk & Issa, 2006; Schein, 2009, 2010). An inter-rater reliability (IRR) procedure was also applied during the coding and synthesis process, with the assistance of a second researcher from the Software Engineering Research Group (SERG), University of Malakand. The identified challenges, associated practices, and their clustering into the four GCSC layers were independently reviewed by two researchers.

Table 10: Clustering of Critical Challenges into GCSC flayers.

Clusters: Layers of GCSC	S.No.	GCSC Challenges
Knowledge	CC4	Lack of National Cybersecurity Capabilities
	CC13	Lack of Public Awareness and Education
Tacit Assumptions	CC5	Lack of International Consensus on Digital Human Rights Governance
	CC7	Lack of International Political Consensus
	CC10	International Disputes over Digital Sovereignty
Espoused Values	CC1	Lack of International Cooperation and Collaboration
	CC3	Lack of a Coordinated Global Cybersecurity Strategy
	CC6	Limited Development and Adoption of Global Cybersecurity Norms
	CC8	Absence of International Cyber Law
	CC9	Lack of Public-Private Partnerships
	CC11	Absence of Global Cybersecurity Governance Authority
Artefacts	CC2	Evolving Cyber Threats and Vulnerabilities
	CC12	Lack of Adherence to International Technical Standards and Best Practices

Organizing the challenges into the layers of Knowledge, Tacit Assumptions, Espoused Values, and Artefacts provides a structured explanation of where these barriers originate and how they affect different cultural dimensions. Some originate from deficiencies in knowledge and awareness, others arise from differences in underlying beliefs and perceptions, several are associated with fragmented governance mechanisms and shared values, while others reflect weaknesses in technical implementation. This clustering enables the challenges to be interpreted from a cultural perspective and creates a direct link between the identified barriers, the success factors, and the development of GCSC.

The four cultural layers represent different aspects of the GCSC, as shown in Figure 3. Knowledge refers to what individuals, organizations, and nations know about cybersecurity, including awareness, skills, and expertise. Tacit Assumptions represent the underlying beliefs and mindsets that influence how cybersecurity is perceived and approached. Espoused Values reflect the values and principles that stakeholders formally express through policies, strategies, laws, standards, and commitments to cooperation. Artefacts represent the visible and observable aspects of cybersecurity culture, including technologies, technical standards, security practices, and other implemented mechanisms. This layer represents the visible outcomes of the values and assumptions and reflects what stakeholders implement.

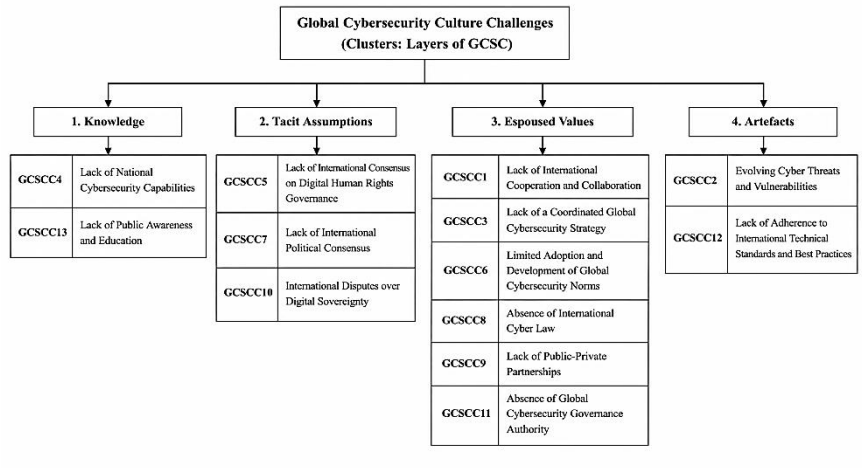


Figure 3: Clustering of the GCSC challenges.

The clustering was perfumed using deductive thematic analysis. Each challenge was examined to determine whether it primarily reflected deficiencies in cybersecurity knowledge, underlying beliefs and assumptions, formally expressed values and governance commitments, or observable technical and operational mechanisms. Although some challenges could be associated with more than one cultural layer, they were assigned to the layer that best represented their primary characteristic to maintain conceptual consistency.

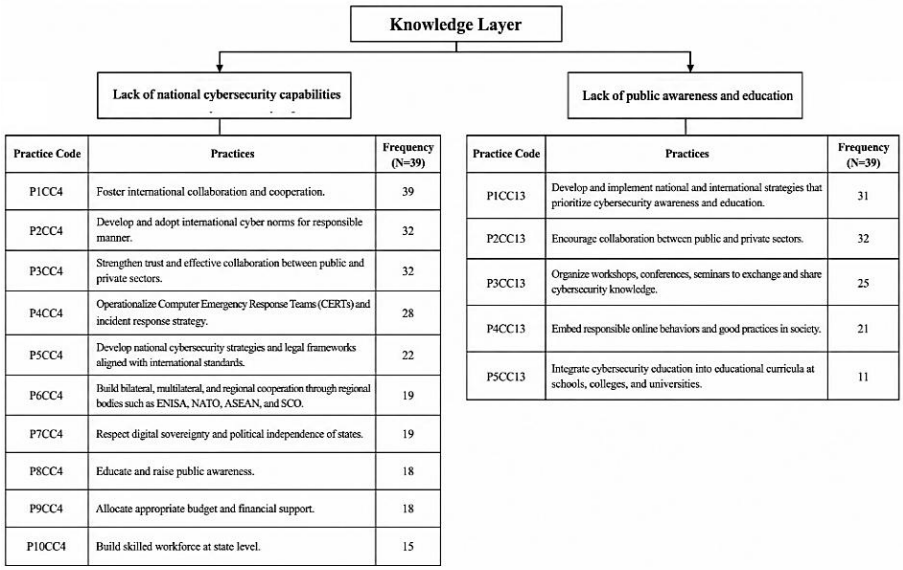
Cluster 1: Knowledge

This cluster includes Critical Challenges that arise from deficiencies in cybersecurity knowledge, skills, awareness, and

institutional capacity. The Critical Challenges and their practices are presented in Figure 4.

Lack of National Cybersecurity Capabilities

Governments often face significant challenges to meet the growing demand for cybersecurity preparedness due to lack of technical, policy, and political expertise, as well as a shortage of skilled cybersecurity professionals (Creese et al., 2021; Tabagari, 2016). This may limit their ability to effectively identify, assess, and mitigate cyber threats at global scale (Schjølberg, 2020; Touré & Schjølberg, 2007). Therefore, their critical infrastructure, computer systems and citizens remain vulnerable to cyber-attacks, and their capacity to defend themselves against external interference (Collett, 2021; Esteve-González et al., 2025).



Practice Code	Practices	Frequency (N=39)
P1CC4	Foster international collaboration and cooperation.	39
P2CC4	Develop and adopt international cyber norms for responsible manner.	32
P3CC4	Strengthen trust and effective collaboration between public and private sectors.	32
P4CC4	Operationalize Computer Emergency Response Teams (CERTs) and incident response strategy.	28
P5CC4	Develop national cybersecurity strategies and legal frameworks aligned with international standards.	22
P6CC4	Build bilateral, multilateral, and regional cooperation through regional bodies such as ENISA, NATO, ASEAN, and SCO.	19
P7CC4	Respect digital sovereignty and political independence of states.	19
P8CC4	Educate and raise public awareness.	18
P9CC4	Allocate appropriate budget and financial support.	18
P10CC4	Build skilled workforce at state level.	15

Practice Code	Practices	Frequency (N=39)
P1CC13	Develop and implement national and international strategies that prioritize cybersecurity awareness and education.	31
P2CC13	Encourage collaboration between public and private sectors.	32
P3CC13	Organize workshops, conferences, seminars to exchange and share cybersecurity knowledge.	25
P4CC13	Embed responsible online behaviors and good practices in society.	21
P5CC13	Integrate cybersecurity education into educational curricula at schools, colleges, and universities.	11

Figure 4: Challenges and their practices for the knowledge layer of the GCSC.

Lack of Public Awareness and Education

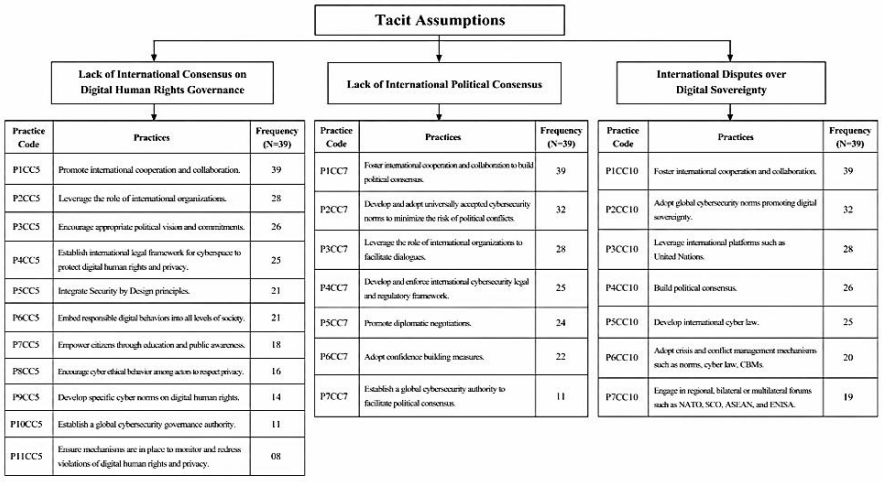
The increasing number of cybercrimes has become a major global issue. One of the contributing factors is limited public awareness and education about safe online practices. (Ghernaouti-Hélie, 2009; Wongmahesak et al., 2025). The lack of awareness increases the risk of cyber incidents, financial losses, data breaches, and even conflicts between states. This leaves individuals, organizations, and nations more vulnerable to cyber-attacks.(Admass et al., 2024).

Cluster 2: Tacit Assumptions

The critical challenges in this cluster arise from underlying beliefs, perceptions, ideologies, and differing viewpoints that influence the development of GCSC. The Critical Challenges and their practices mapped to this cluster are illustrated in Figure 5.

Lack of International Consensus on Digital Human Rights Governance

There is no international consensus on balancing fundamental human rights, such as privacy, access to information, and freedom of expression, with state control over the internet (Barrera, 2017; Pijović, 2021). This hinders the development of coherent global cybersecurity policies to make cyberspace secure.



Practice Code	Practices	Frequency (N=39)
P1CC5	Promote international cooperation and collaboration.	39
P2CC5	Leverage the role of international organizations.	28
P3CC5	Encourage appropriate political vision and commitments.	26
P4CC5	Establish international legal framework for cyberspace to protect digital human rights and privacy.	25
P5CC5	Integrate Security by Design principles.	21
P6CC5	Embed responsible digital behaviors into all levels of society.	21
P7CC5	Empower citizens through education and public awareness.	18
P8CC5	Encourage cyber ethical behavior among actors to respect privacy.	16
P9CC5	Develop specific cyber norms on digital human rights.	14
P10CC5	Establish a global cybersecurity governance authority.	11
P11CC5	Ensure mechanisms are in place to monitor and redress violations of digital human rights and privacy.	08

Practice Code	Practices	Frequency (N=39)
P1CC7	Foster international cooperation and collaboration to build political consensus.	39
P2CC7	Develop and adopt universally accepted cybersecurity norms to minimize the risk of political conflicts.	32
P3CC7	Leverage the role of international organizations to facilitate dialogues.	28
P4CC7	Develop and enforce international cybersecurity legal and regulatory framework.	25
P5CC7	Promote diplomatic negotiations.	24
P6CC7	Adopt confidence building measures.	22
P7CC7	Establish a global cybersecurity authority to facilitate political consensus.	11

Practice Code	Practices	Frequency (N=39)
P1CC10	Foster international cooperation and collaboration.	39
P2CC10	Adopt global cybersecurity norms promoting digital sovereignty.	32
P3CC10	Leverage international platforms such as United Nations.	28
P4CC10	Build political consensus.	26
P5CC10	Develop international cyber law.	25
P6CC10	Adopt crisis and conflict management mechanisms such as norms, cyber law, CBMs.	20
P7CC10	Engage in regional, bilateral or multilateral forums such as NATO, SCO, ASEAN, and ENISA.	19

Figure 5: GCSC challenges and their practices for the Tacit Assumption layer.

Lack of International Political Consensus

Internationally agreed political agreements on the development of global cyber-security frameworks have always been a significant challenge (Australian Strategic Policy, 2022; Pijović, 2021; Prokopyshyn & Trushkina, 2025). Geopolitical differences, including ideological divides, political values, and concerns over digital sovereignty, privacy, and data control, hinder the development of a shared global culture of cybersecurity (Glen, 2021; Kritika, 2025; Riordan, 2018).

International Disputes over the Interpretation of Digital Sovereignty

Cyberspace has no physical boundaries and digital sovereignty is difficult to define because of its borderless nature and the decentralized flow of data. The borderless nature of cyberspace and the decentralized

flow of data make it difficult to define physical boundaries and digital sovereignty (Krishnamurthy, 2025; Pierucci, 2025). In this context, it becomes difficult to balance digital sovereignty, territorial sovereignty, and the free flow of information. Furthermore, states have considerable differences in their approaches to this balance, which hinders global consensus on how sovereignty should be applied in cyberspace (Barrera, 2017; Dunn & Mauer, 2006).

Cluster 3: Espoused Values

The critical challenges in this cluster are related to the values, commitments, governance mechanisms, laws, strategies, and policies that stakeholders formally endorse and promote. The Critical Challenges and their practices mapped to this cluster are illustrated in Figure 6.

Lack of International Cooperation and Collaboration

The lack of international cooperation and collaboration among stakeholders results in fragmented and uncoordinated approaches to make cyberspace secure (Paziuk & Mitsik, 2019; Schjølberg, 2020). This fragmentation creates global vulnerabilities that can be misused by malicious actors. Such issue, thereby hindering the development of global culture of cybersecurity (Anastasiya Kazakova & Droz, 2023; Serrano, 2024).

Lack of a coordinated global cybersecurity strategy

The absence of a comprehensive global cybersecurity approach is a another major challenge in handling the evolving nature of cybercrimes and building trust among nations (Paziuk & Mitsik, 2019; Van Horenbeeck et al., 2018). Hackers and other malicious actors exploit gaps in jurisdiction, international cooperation, and legal enforcement, making it very difficult to hold them accountable (Amoo et al., 2024; Radanliev, 2024).

Limited development and adoption of global cybersecurity norms

Global cybersecurity norms such as developed by the UNGGE provide an important foundation for responsible state behavior. However, their adoption is limited and uneven due to challenges such as limited enforcement mechanisms, varying cybersecurity capabilities across countries, and diverging national interests (Gupta & Singh, 2025; Madnick et al., 2024; Maurer, 2020). Further, the lack of global acceptance make it difficult to ensure adherence to global cybersecurity norms (Gupta & Singh, 2025; Hurwitz, 2013).

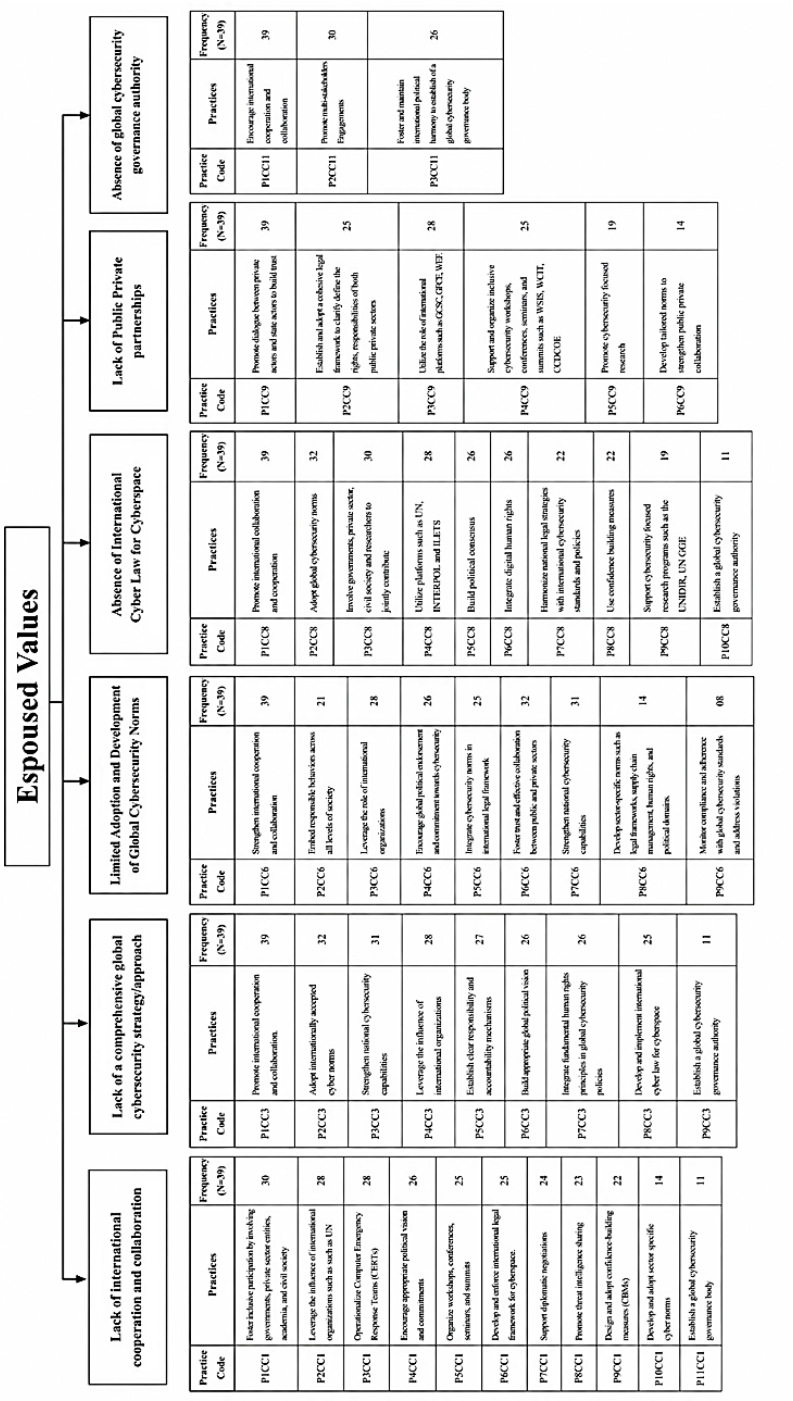


Figure 6: GCSC challenges and their practices for the Espoused Values layer.

Absence of international cyber law for cyberspace

Currently, a globally accepted and implemented unified legislation for cybersecurity does not exist (Pernice, 2018). The absence of international cyber law governing cyberspace is a major challenge in developing a GCSC (Chatinakrob, 2024; Qu, 2026). Existing international law is still unclear about what kinds of cyber actions are allowed and how states should respond to them (Hurwitz, 2013). This deficiency in the digital world not only limits the effectiveness of cybersecurity measures to confront cybercrimes, but also has a negative impact on regulating cyber behaviors and enforcing accountability across borders (Maurer, 2020; Wouters, 2020).

Lack of Public Private Partnerships

The private sector owns and operates the majority of ICT infrastructure. (Camino, 2017; Finnemore & Hollis, 2016). Without cooperation between the public and private sectors, efforts can become fragmented, resources limited and responses to cyber incidents weak which leads to a less secure cyberspace (Paziuk & Mitsik, 2019; Sund, 2007). On the other hand, public private partnerships play a vital role in shaping cyber norms, securing ICT products and building cybersecurity capacity efforts worldwide (Esteve-González et al., 2025; Hurel & Lobato, 2018).

Absence of global cybersecurity governance authority

The absence of a central global authority for cybersecurity is another major problem (Hurwitz, 2013). Without a central coordinating body, states and organizations around the world often work independently, which leads to duplicated efforts and inconsistent practices and standards (Pernice, 2018). International organizations such as the UN, ITU, ISO, NIST, IEEE, W3C, and FIRST are actively working to improve global cybersecurity. However, limited coordination among them makes collective global responses difficult to implement (Australian Strategic Policy, 2022).

Cluster 4: Artefacts

This cluster contains critical challenges associated with visible technical implementations, standards, operational practices, and technologies. The Critical Challenges and their associated practices which are related to this cluster are illustrated in Figure 7.

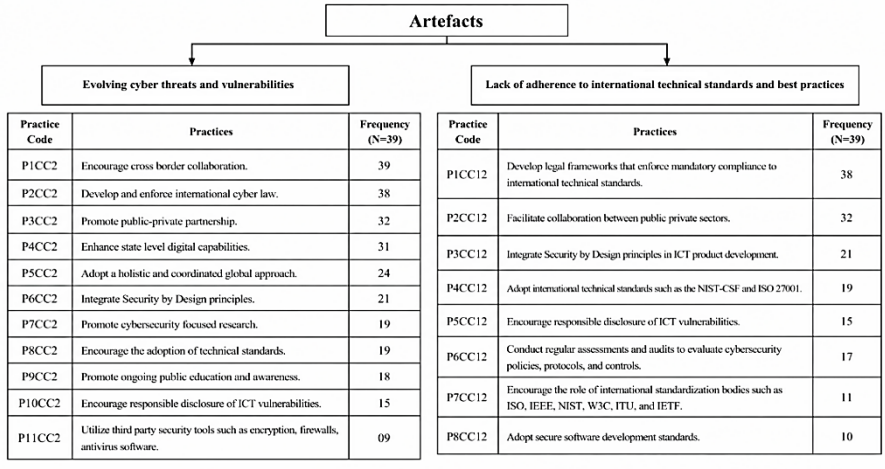
Evolving Cyber Threats and Vulnerabilities

The constantly evolving landscape of cyber threats and vulnerabilities, such as phishing, insider threats, cyber espionage, and

social engineering, pose a significant challenge to global cybersecurity (Mallick & Nath, 2024; Thakur, 2024). Hackers and other malicious actors exploit these vulnerabilities, resulting in personal data breaches, financial losses, and interstate conflicts which contribute to instability in cyberspace (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013; Open-ended Working, 2021).

Lack of adherence to international technical standards and best practices

The lack of compliance with internationally recognized cybersecurity standards, such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), and COBIT, increases the risk of security vulnerabilities and exposes digital infrastructure to cyber threats (Paz, 2023; Shackelford et al., 2015). Without common technical standards, it becomes difficult to implement secure development, protect supply chains, and respond effectively to cybersecurity incidents (Anastasiya Kazakova & Droz, 2023; Schjølberg, 2020).



Practice Code	Practices	Frequency (N=39)
P1CC2	Encourage cross border collaboration.	39
P2CC2	Develop and enforce international cyber law.	38
P3CC2	Promote public-private partnership.	32
P4CC2	Enhance state level digital capabilities.	31
P5CC2	Adopt a holistic and coordinated global approach.	24
P6CC2	Integrate Security by Design principles.	21
P7CC2	Promote cybersecurity focused research.	19
P8CC2	Encourage the adoption of technical standards.	19
P9CC2	Promote ongoing public education and awareness.	18
P10CC2	Encourage responsible disclosure of ICT vulnerabilities.	15
P11CC2	Utilize third party security tools such as encryption, firewalls, antivirus software.	09

Practice Code	Practices	Frequency (N=39)
P1CC12	Develop legal frameworks that enforce mandatory compliance to international technical standards.	38
P2CC12	Facilitate collaboration between public private sectors.	32
P3CC12	Integrate Security by Design principles in ICT product development.	21
P4CC12	Adopt international technical standards such as the NIST-CSF and ISO 27001.	19
P5CC12	Encourage responsible disclosure of ICT vulnerabilities.	15
P6CC12	Conduct regular assessments and audits to evaluate cybersecurity policies, protocols, and controls.	17
P7CC12	Encourage the role of international standardization bodies such as ISO, IEEE, NIST, W3C, ITU, and IETF.	11
P8CC12	Adopt secure software development standards.	10

Figure 7: GCSC challenges and their practices for the Espoused Values layer.

Analysis of the Challenges Across Methodologies

This section examines how the identified Critical Challenges of GCSC are distributed across different research methodologies. This study categorized the selected studies into five methodological approaches including the interdisciplinary analysis, qualitative case studies, comparative analysis, literature review, and Expert Consultation, as presented in Table 11. Chi-square tests (linear by linear associations) were performed to examine the distribution of the identified challenges across

different research methodologies. The analysis revealed that Evolving Cyber Threats and Vulnerabilities (CC2), Absence of Global Cybersecurity Governance Authority (CC11), and Lack of Adherence to International Technical Standards and Best Practices (CC12) were significantly more likely to be investigated using expert-driven methodologies. It is worth noting that none of the selected sources, including both published and GL, employed a systematic review approach. Most studies relied on expert opinions and discussions. These findings underscore the need for more comprehensive Systematic reviews to address the full spectrum of GCSC.

Table 11: Analysis of the critical challenges identified for GCSC challenges based on publication methodologies/ study strategies.

Analysis of the Critical Challenges based on Study Strategies (Both WL and GL)						Chi-square test Results $\alpha = 0.05$, d f= 1	
S.No.	Interdisciplinary Analysis (N = 03)	Qualitative Case Study (N = 03)	Comparative Analysis (N = 01)	Literature Review (N = 12)	Expert Consultation (N = 20)	X^2	P
CC1	3	9	3	1	20	3.414	0.650
CC2	1	10	3	1	20	8.089	0.004
CC3	2	10	3	0	19	1.487	0.223
CC4	1	11	3	1	18	1.487	0.223
CC5	2	11	3	1	16	0.175	0.676
CC6	1	11	1	1	16	0.320	0.572
CC7	2	9	1	1	16	0.469	0.493
CC8	2	7	0	1	17	3.263	0.710
CC9	1	8	1	1	16	2.505	0.113
CC10	2	6	0	0	13	0.560	0.454
CC11	0	5	1	0	15	6.824	0.009
CC12	0	4	1	1	14	7.438	0.006
CC13	2	7	1	0	9	0.754	0.385

Analysis of the Challenges Based on Publication Periods

The identified GCSC challenges were examined across two publication periods: 2000-2015 and 2016-2024. The comparison reveals how the focus of cybersecurity research has changed over time. During the earlier period (2000-2015), studies mainly concentrated on technical and organizational issues, such as malware, data breaches, and other cybersecurity vulnerabilities. In contrast, publications from 2016-2024 emphasized broader cybersecurity challenges, including lack of political consensus over cybersecurity governance, absence of international cyber law, and the lack of cybersecurity awareness. This shift reflects that cybersecurity is not only a technical issue but also a strategic concern with legal, political, and societal dimensions.

Chi-square analysis showed that only the Evolving cyber threats and vulnerabilities, the Absence of global cybersecurity governance authority, and the Lack of adherence to international technical standards and best practices showed significant differences across study strategies, as shown in Table 12. All remaining challenges showed no statistically significant variation. Furthermore, Expert Consultation and Qualitative Case Studies contributed the largest proportion of evidence across most challenges.

Table 12: Analysis of GCSC challenges based on publication Periods.

S.No.	GCSC Challenges Occurrences in MLR, Period of Publications (2000 - 2025), both in WL and GL (N = 39)				Chi-square test Result (Linear by Linear Association) α = 0.05, df = 1	
	2000-2015 (N = 20)		2016-2025 (N=19)		X^2	P
	Frequency	Freq %	Frequency	Freq %		
CC1	17	85	19	100	2.447	0.118
CC2	17	85	18	95	3.356	0.67
CC3	17	85	17	89	4.318	0.038
CC4	16	80	18	95	1.265	0.261
CC5	15	75	18	95	0.296	0.587
CC6	13	65	17	89	0.303	0.954
CC7	14	70	15	79	0.984	0.321
CC8	15	75	12	63	4.979	0.026
CC9	13	65	14	74	0.723	0.395
CC10	11	55	10	53	1.393	0.238
CC11	10	50	11	58	0.293	0.588
CC12	9	45	11	58	0.032	0.857
CC13	9	45	10	53	0.210	0.647

Threats to validity

In this research a multidisciplinary MLR was conducted to understand the different dimensions of GCSC, by synthesizing both WL and GL. These dimensions include technical, normative, governance, and awareness. This topic covers multiple disciplines, making it difficult to collect different types of sources and ensure balanced regional representation. To address these issues, we conducted exhaustive searches across major academic databases and specialized GL sources. Construct validity was ensured by clearly defining key concepts using the PICO criteria and collaborative discussions during study selection and data synthesis. To reduce selection bias, predefined inclusion and exclusion criteria, the Tollgate screening approach, and an inter-rater reliability procedure were applied throughout the study selection process. Internal validity was strengthened by using the Tollgate screening technique, clear inclusion and exclusion criteria, and a structured quality assessment process. To minimize data extraction and coding bias, an inter-rater reliability procedure was also applied during the data extraction, coding, and synthesis processes. The extracted data, identified challenges,

associated practices, and their clustering into the four GCSC layers were independently reviewed by two researchers, and any disagreements were resolved through discussion until consensus was reached. To improve external validity, we included perspectives from academia, policy, and industry sources. However, geographic bias in the available literature and the evolving nature of cybersecurity threats, and the dynamic cybersecurity landscape may limit the generalizability of these findings. Therefore, the results should be interpreted in light of these limitations.

Conclusion and Future Work

This study was undertaken to better understand the challenges that hinder the development and operationalization of a GCSC. To achieve this objective, we conducted a MLR by systematically reviewing both published and GL. The initial search retrieved 3,549 sources, comprising 3,266 published studies and 283 GL sources. These studies were screened in several stages, including title and abstract review, introduction and conclusion review, and full text assessment based on predefined inclusion and exclusion criteria. After applying the QAC on the 44 selected sources, 20 published studies and 19 GL sources, were selected for the final synthesis. The review identified 13 Critical Challenges together with their associated practices for advancing a GCSC. To provide a structured understanding, the identified challenges were further clustered into the four cultural layers of GCSC: Knowledge, Tacit Assumptions, Espoused Values, and Artefacts. The findings show that building a GCSC is a complex task that extends well beyond technical solutions. It is influenced by technological developments, geopolitical interests, legal and regulatory differences, organizational practices, and human behavior. Among the most frequently reported challenges were the lack of international cooperation and coordination, lack of political consensus, evolving cyber threats, lack of national cybersecurity capabilities, and the absence of international cyber law. In contrast, cybersecurity awareness and education, along with adherence to international technical standards, received comparatively less attention in the literature despite their importance for strengthening cybersecurity culture. Overall, this study provides a thorough understanding of the critical challenges and associated practices that shape GCSC. The findings also offer a foundation for researchers, policymakers, and international organizations to strengthen international cooperation and make cyberspace safe and secure. Future research can validate these findings through empirical studies. Comparative studies across countries and regions could provide further insights into how these challenges vary in different contexts and regions. Future research can also examine the impact of emerging technologies,

such as Artificial Intelligence (AI), the Internet of Things (IoT), and cloud computing, on the development and evolution of GCSC.

Appendix A

Table 13: Final list of WL-based on QAC.

S.No.	Title of WL Articles	Article Type	Year	WL_QA1	WL_QA2	WL_QA3	WL_QA4	WL_QA5	WL_QA6	Total Score
W1	An Inclusive Information Society Needs a Global Approach of Information Security	Conference Paper	2009	1	0	1	1	0.5	1	4.5
W2	GCSC in the international discourse: values and principles	Journal paper	2019	1	0	1	1	0	1	04
W3	Analysis of international experience in the formation of a culture of information security in society	Journal paper	2022	1	0	1	1	0	1	04
W4	Towards an international road-map for cybersecurity	Journal paper	2007	1	1	1	1	0.5	0	4.5
W5	Cybersecurity culture as an element of IT professional training	Conference Paper	2016	1	0	1	1	0	0	03
W6	A Dose of Realism: The Contestation and Politics of Cyber Norms	Journal paper	2019	1	1	1	1	0	0	04
W7	The Security Culture of a Global and Multileveled Cyber Security	Book Chapter	2014	1	0	0.5	1	1	0	3.5
W8	The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms.	Conference Paper	2021	1	0	1	1	0	0	03
W9	Cybersecurity: Culture, Norms and Values	Background paper	2018	1	0	1	1	0	0	03
W10	Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives	Journal paper	2021	1	0	0.5	0.5	0	1	03
W11	Global cybersecurity governance: A constitutionalist analysis	Journal paper	2018	1	0	1	0.5	0.5	0	03
W12	Unpacking cyber norms: private companies as norm entrepreneurs	Journal paper	2018	1	0	0.5	0.5	0.5	1	3.5
W13	Constructing Norms for Global Cybersecurity	Journal paper	2016	1	0.5	1	1	0	0	3.5
W14	Norm Entrepreneurship in Global Cybersecurity	Journal paper	2021	1	0	1	1	0	0	03
W15	A Global Treaty on Cybersecurity and Cybercrime	Journal paper	2011	1	0	1	1	1	0	4
W16	Towards a Global Culture of Cyber Security	Book Chapter	2006	1	0	1	1	0.5	0	3.5
W17	A New normal? The cultivation of global norms as part of a cybersecurity strategy	Book Chapter	2013	1	0	0.5	1	0.5	0	03
W18	Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity	Book Chapter	2014	1	0	1	1	0	0	03
W19	International Intergovernmental Organizations	Book Chapter	2009	1	0	1	1	0	0	03
W20	Norms of Responsible State Behaviors in Cyberspace (Book The Ethics of Cybersecurity)	Book Chapter	2020	1	0	1	1	0	0	03

Appendix B

Table 14: Final list of GL-based on QAC

S.No.	Title of GL Sources	Type	Year	WL-QA1	WL-QA2	WL-QA3	WL-QA4	WL-QA5	WL-QA6	WL-QA6	WL-QA6	Total Score
G1	Report by the Secretary General Guidelines for Utilization of The Global Cybersecurity Agenda (CGA)	Report	2020	1	1	0	1	1	0.5	1	1	6.5

G2	The Achievable Multinational Cyber Treaty Strengthening Our Nation's Critical Infrastructure	Report	2017	1	1	0	1	1	0.5	0.5	0.5	5.5
G3	Geneva Declaration of Principles and Plan of Action, World Summit on Information Society at Geneva	Report	2004	1	1	0	0	1	1	1	1	6
G4	Norms For International Peace and Security: The Normative Frameworks Of International Cyber Cooperation	Working Paper	2015	1	1	0	1	1	1	0.5	0.5	6
G5	Georgian Cyber Defense Unit Tallinn University Of Technology	Thesis	2016	1	1	1	1	1	1	0	0.5	6.5
G6	Creation of a global culture of cybersecurity	UN Resolutions	2003	1	1	0	0	1	1	0.5	1	5.5
G7	Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures	UN Resolutions	2009	1	1	0	0	1	1	0.5	1	5.5
G8	International Code of Conduct for Information Security" submitted by China, Russia and other countries to the UN	UN General Assembly Letter	2011	1	1	0	1	1	0.5	0.5	0.5	5.5
G9	Paris Call for Trust and Security in Cyberspace	Report	2018	1	1	0	0	1	1	0.5	0.5	5
G10	Advancing International Cyber Norms: Multi-stakeholder Recommendations (Paris Call 9 Principles)	Report	2020	1	1	1	1	1	0.5	0.5	1	7
G11	The UN norms of responsible state behaviors in cyberspace | (ASPI)	Report	2022	1	1	0	0	1	0.5	1	0.5	5
G12	Five Principles for Shaping Cybersecurity Norms (Microsoft Policy Debate)	White Paper	2013	1	1	0	0	1	1	1	1	6
G13	International Cybersecurity Norms Reducing conflict in an Internet dependent world by Microsoft	White Paper	2014	1	1	0	0	1	1	0.5	0.5	5
G14	Advancing Cyber-stability Final Report of The Global Commission on The Stability of Cyberspace	Report	2019	1	1	0	0	1	1	0.5	0.5	5
G15	OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security	Report	2002	1	1	0	1	1	1	0.5	0.5	6
G16	The UN, Cyberspace and International Peace and Security by UNIDIR	Report	2017	1	1	0	0	1	1	0.5	0.5	5
G17	The Geneva Dialogue on Responsible Behavior in Cyberspace, Implementation of Norms of Responsible Behavior in Cyberspace by Relevant Non-State Stakeholders (Geneva Manual)	Report	2023	1	1	0	0	1	0.5	0.5	0.5	4.5
G18	The Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)	Report	2018	1	1	0	1	1	0	0.5	0.5	5
G19	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	Report	2015	1	1	0	0	1	1	0.5	0.5	5

References

Abdo, J. B., & Hossain, L. (2025). Interdisciplinarity of cybersecurity: Towards convergence science.

Adejumo, A. P., & Ogburie, C. P. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(03), 1527-1541.

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031.

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.

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *Electronic Journal of Information Systems in Developing Countries*.

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205-217.

Anastasiya Kazakova, V. R., Serge , & Droz. (2023). *Geneva manual: On responsible behaviour in cyberspace, implementation of norms by relevant non-state stakeholders*. DiploFoundation. https://genevadialogue.ch/wp-content/uploads/Geneva-Manual.pdf

ASEAN Regional Forum. (2015)*Work plan on security of and in the use of Information and Communications Technologies (ICT)*.

Australian Strategic Policy Institute. (2022). *The UN norms of responsible state behaviour in cyberspace: Implementation and practical guidance for states, with examples from the ASEAN region*. <https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

Barrera, M. A. (2017). *Achievable multinational cyber treaty: strengthening our nation's critical infrastructure* (Air Force Research Institute perspectives on cyber power ; CPP-3, Issue. https://media.defense.gov/2017/Jun/19/2001764798/-1/-1/0/CPP_0003_BARRERA_MULTINATIONAL_CYBER_TREATY.PDF

Ben Amor, H., Abdellatif, M., & Ghaleb, T. (2025). *A comprehensive multi-vocal empirical study of ml cloud service misuses* [Preprint]. https://arxiv.org/abs/2503.09815

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

Chatinakrob, T. (2024). Interplay of international law and cyberspace: state sovereignty violation, Extraterritorial effects, and the

paradigm of cyber sovereignty. *Chinese Journal of International Law*, *23*(1), 25-72.

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy*, *6*(3), 298-317.

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

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214-235.

Council of the European Union. (2017). *Draft council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities, Cyber diplomacy toolbox.* http://www.consilium.europa.eu/en/policies/sanctions/

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.

Dunn, M., & Mauer, V. (2006). Towards a global culture of cyber-security. In *International CIIP Handbook* (Vol. II). Center for Security Studies (CSS).

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.

Esteve-González, P., Axon, L., Creese, S., Dutton, W. H., Saunders, J., Carver, J., & Goldsmith, M. (2025). *Cybersecurity capacities for the application of un cyber norms*. https://ssrn.com/abstract=5089805

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425-479.

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.

Gevorgyan, M. R., Minasyan, S. M., & Manukyan, L. M. (2025). Exploring the role of cybersecurity: Interdisciplinary perspectives and strategies. *Cross-Cultural Studies: Education and Science*, *10*(1), 164-173.

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.

Glen, C. M. (2021). Norm Entrepreneurship in Global Cybersecurity. *Politics & Policy*, *49*(5), 1121-1145.

Government of France. (2018). *Paris call for trust and security in cyberspace*. https://pariscall.international/en/

Gupta, S. K., & Singh, P. (2025). Global Cybersecurity Governance: The role of international norms in cyberspace. In M. Chawki & A. Abraham (Eds.), *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (pp. 113-127). Springer Nature Switzerland.

Gurung, A. (2025). From battlefield to the servers: Cyber warfare and the conflicts. *The Shivapuri Journal*, *26*(1), 29-41.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61-76.

Hurwitz, R. (2013). A new normal? The cultivation of global norms as part of a cybersecurity strategy. In P. A. Yannakogeorgos & A. Lowther (Eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (pp. 233-264). CRC Press.

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (Global Cybersecurity Index, Issue. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Kai Lin, T. (2023). *ASEAN Cyber-security cooperation: Towards a regional emergencyresponse framework*. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf

Kerttunen, M., & Kiisel, S. (2015). *Norms for international peace and security: The normative frameworks of international cyber cooperation* (ICT4PEACE NORMS Project Draft Working Paper, Issue.

Kesler, E. (2024). *A transdisciplinary approach to cybersecurity: A Framework for encouraging transdisciplinary thinking* [Preprint]. arXiv. https://arxiv.org/abs/2405.10373

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 1-13.

Khan, A. W., Saeed, D. S., & Kakar, M. S. (2024). Cybersecurity as a geopolitical tool: The growing influence of digital warfare in

statecraft. *International Research Journal of Social Sciences and Humanities*, *3*(2), 345-357.

Krishna, B., Krishnan, S., & Sebastian, M. P. (2022). Examining the relationship between national cybersecurity commitment, Culture, and Digital payment usage: An Institutional Trust Theory Perspective. *Information Systems Frontiers*.

Krishnamurthy, V. (2025). Anchoring digital sovereignty. *Chicago Journal of International Law*, *25*(2), Article 2.

Kritika, M. (2025). A comprehensive study on cyber diplomacy as a tool for conflict prevention and cybersecurity governance. *International Cybersecurity Law Review*.

Madnick, B., Huang, K., & Madnick, S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective*, *33*(3), 204-225.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.

Marina, K., & Michael, C. (2019). *Advancing Cyberstability Final Report*. https://cyberstability.org/

Maurer, T. (2020). A dose of realism: The contestation and politics of cyber norms. *Hague Journal on the Rule of Law*, *12*(2), 283-305.

McDowell, S. D., Nensey, Z., & Steinberg, P. E. (2014). Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 231-252). Springer Berlin Heidelberg.

Meyer, P. (2020). Norms of responsible state behaviour in cyberspace. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 347-360). Springer International Publishing.

Microsoft Corporation.(2014) *Microsoft international cybersecurity norms: reducing conflict in an internet-dependent world*. https://www.microsoft.com/en-us/cybersecurity/content-hub/reducing-conflict-in-lnternet-dependent-world

Microsoft Corporation. *(2013) Five principles for shaping cybersecurity norms*.https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc9

Muhammad, N., & Khan, S. U. (2024). Global culture of cybersecurity: A multi-vocal literature review protocol. *The Lighthouse Journal of Social Sciences*, *3*(1), 67-88.

Muhammad, N., Khan, S. U., Niazi, M., & Shameem, M. (2026). *An Empirical Study of Challenges for Developing Global Cybersecurity Culture,* International Conference on Evaluation and Assessment in Software Engineering (EASE) 2026, Glasgow, United Kingdom.

Naeem, U., Siffat Ullah, K., & Syed Muhammad Shakir, B. (2025). *Multivocal literature review protocol for theidentification of cybersecurity challenges anditssolutions in the context of vehicle-to-vehiclecommunications from software engineeringperspective. Spectrum of Engineering Sciences*, *3*(2), 58-89.

Niekerk, J. V., & Issa, R. V. S. (2006). Understanding information security culture: A conceptual framework. *Citeseer*.

OECD, (2002). *OECD Guidelines for the security of information systems and networks*. https://legalinstruments.oecd.org/public/doc/116/116.en.pdf

Paris Call for Trust and Security in Cyberspace. (2020). *Advancing international cyber norms: Multistakeholder recommendations* (Paris Peace Forum, Issue. https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf

Paz, S. (2023). Cybersecurity standards and frameworks. *IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)*, 397-416.

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.

Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*, *7*(1), 112-141.

Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking territoriality and governance in cyberspace. *Digital Society*, *4*(1), 27.

Pijović, N. (2021, 25-28 May 2021). The cyberspace 'great game'. the five eyes, the sino-russian bloc and the growing competition to shape global cyberspace norms. 13th International Conference on Cyber Conflict (CyCon),

Portnoy, M., & Goodman, S. (2009). International intergovernmental organizations. In M. Portnoy & S. Goodman (Eds.), *Global Initiatives to Secure Cyberspace: An Emerging Landscape* (pp. 1-22). Springer US.

Prokopyshyn, O., & Trushkina, N. (2025). The geopolitics of cybersecurity: A comparative analysis of national strategies for digital sovereignty. *Politics & Security*, *12*(2), 59-71.

Qu, X. (2026). International law and the regulation of cross-border cyberattacks: Challenges and solutions. *International Journal of Computer Information Systems and Industrial Management Applications*, *18*, 12-12.

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1-51.

Reegård, K., Blackett, C., & Katta, V. (2020). The Concept of Cybersecurity Culture. 4036-4043.

Riordan, S. (2018). The geopolitics of cyberspace: A diplomatic perspective. *Brill Research Perspectives in Diplomacy and Foreign Policy*, *3*(3), 1-84.

Schein, E. H. (2009). *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

Schein, E. H. (2010). Three cultures of management: The key to organizational learning. *Glocal Working. Living and Working Across the World With Cultural Intelligence. Milan, Italy, Franco Angeli*, 37-58.

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

Serrano, A. S. (2024). The challenge of global cybersecurity. In *Global Cybersecurity and International Law* (pp. 1-9). Routledge.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ*, *50*, 305.

Singh, M., Srivastava, S., & Mahanandia, R. (2026). Leadership and cybersecurity governance: building a human-centric protective culture in the digital age. In *The Human Dimension of Cybersecurity: Cultivating a Protective Organizational Culture* (pp. 1-28). IGI Global Scientific Publishing.

Steve, M. (2023). *Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024*. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Sund, C. (2007). Towards an international road-map for cybersecurity. *Online Information Review*, *31*(5), 566-582.

Tabagari, T. (2016). *Georgian cyber defense unit, cyber reserve*

tallinn manual on the international law applicable to cyber warfare. (2013). Cambridge University Press.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, 1-20.

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. (2014). The security culture of a global and multileveled cyber security. In *Cyber-Development and Cyber-Democracy: Challenges, Opportunities and Implications for Theory*.

United Nations Open-ended Working Group. (2021). *Final substantive report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)*. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

United Nations General Assembly. (2003) Creation of a global culture of cybersecurity :resolution.

United Nations General Assembly. (2009) *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*.

United Nations General Assembly. (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. http://digitallibrary.un.org/record/753055/files/A_68_98-ES.pdf

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

United Nations Institute for Disarmament Research (UNIDR). (2017). *The united nations, cyberspace and international peace and security: responding to complexity in the 21st century*.

United Nations General Assembly. (2015). *International Code of Conduct for Information Security*. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf

Van Horenbeeck, M., Kulesza, J., & Paziuk, A. (2018). Cybersecurity: culture, norms and values, Background paper to the IGF Best Practices Forum on Cybersecurity.

https://www.academia.edu/37417784/Cybersecurity_Culture_Norms_and_Values

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,

Wongmahesak, K., Singh, B., & Kaunert, C. (2025). The complex interplay of generational differences, digital literacy, and cybercrime fear. *Asian Crime and Society Review*, *12*(1), 3-3.

World Summit on the Information Society. (2005) *Geneva Declaration of Principles and Plan of Action* https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf

World Bank. (2024). Digital first responders: The role of computer security incident response teams (CSIRTs) in developing countries.

World Economic Fourm. (2025). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Wouters, J. (2020). Filling global governance gaps in cybersecurity: International and european legal perspectives. *International Organisations Research Journal*, *15*(15), 141-172.