Toward a Unified Framework for Measuring Global Cybercrime: Bridging Gaps in Cross-National Comparisons

Mr. Jagadish Bhatra
CSE Department
MITS
Rayagada, Odisha.
jagadishbhatra00@gmail.com

Mr. Susant Kumar Dash
CSE Department
MITS
Rayagada, Odisha.
susant.disha@gmail.com

Anshuman Mishra
CSE Department
MITS
Rayagada, Odisha.
srinusalbam41234@gmail.com

Abstract-The growing complexity and transnational nature of cybercrime necessitate robust and standardized methods for global measurement. Existing indices such as the National Cyber Security Index (NCSI), the ICT Development Index, and the Global Cybersecurity Index (GCI) provide valuable insights but operate in isolation, leading to fragmented assessments. This lack of a universally accepted comparative framework restricts the ability of policymakers, researchers, and international organizations to track cybercrime trends consistently and design coordinated responses. This study aims to critically examine the limitations of current indices and propose an integrated measurement model that harmonizes technical, social, and economic indicators of cybercrime across nations. By introducing a standardized comparative framework, the paper emphasizes not only the importance of methodological coherence but also the potential to strengthen global cooperation in cybercrime prevention. The findings are expected to guide both academic research and international policy development, enabling a more systematic understanding of global cyber threats and the formulation of effective countermeasures.

Keywords: Cybercrime measurement, global comparative framework, cybersecurity indices, NCSI, ICT Development Index, Global Cybersecurity Index, international cooperation, cyber threat assessment.

INTRODUCTION

In the last two decades, the rapid digital transformation of societies has created unprecedented opportunities for economic growth, innovation, and connectivity. However, this technological expansion has been paralleled by a surge in cybercrime, ranging from financial fraud and ransomware to cyberterrorism and state-sponsored attacks. The global scale and cross-border nature of these crimes make them particularly challenging to monitor and counteract. Governments, enterprises, and individuals alike are vulnerable, yet the absence of a universally accepted framework for measuring and comparing cybercrime trends across nations significantly hinders coordinated global responses.

Although numerous indices exist to assess cybersecurity readiness and digital development, such as the National Cyber Security Index (NCSI), the ICT Development Index (ICTDI), and the Global Cybersecurity Index (GCI), their fragmented nature presents considerable limitations. Each of these indices focuses on specific dimensions of cybersecurity, such as institutional readiness, digital infrastructure, or legal frameworks, but they often fail to capture the full spectrum of cybercrime activities. Moreover, variations in methodology, data sources, and weighting criteria make it difficult to establish a consistent baseline for comparison between nations. As a result, global patterns of cybercrime remain inadequately mapped, preventing researchers and policymakers from forming a holistic picture of emerging threats.

The significance of this research gap becomes clearer when considering the transnational character of cybercrime. Unlike conventional crimes that are geographically bound, cybercrime can originate in one country, traverse multiple jurisdictions, and cause damage across continents within seconds. Without standardized metrics, countries with weak reporting systems or limited technological infrastructure often appear underrepresented in global datasets, while highly digitized nations may seem disproportionately affected due to better monitoring and reporting mechanisms. This imbalance creates an incomplete global narrative, leading to misguided policymaking and the inefficient allocation of cybersecurity resources.

Furthermore, the absence of a unified measurement framework undermines efforts toward international cooperation. While organizations such as INTERPOL, Europol, and the United Nations have initiated programs to foster collaboration, the lack of standardized comparative data reduces the effectiveness of such initiatives. For instance, cybercrime treaties and bilateral agreements rely heavily on shared intelligence, yet disparities in measurement approaches obstruct mutual understanding of the scale, intensity, and typologies of cyber threats. The situation is exacerbated by the fact that cybercrime is continuously evolving, with new attack vectors emerging through artificial intelligence (AI), Internet of Things (IoT) vulnerabilities, and cybercrime-as-a-service models. This dynamism requires measurement tools that are not only

standardized but also adaptive to technological and criminal innovations.

Another critical dimension lies in the socio-economic consequences of measurement gaps. Policymakers in developing and less digitally mature nations are often left without reliable benchmarks to assess their cybercrime exposure. This, in turn, hampers the development of informed national strategies and the ability to seek international assistance. Additionally, vulnerable populations and small enterprises in these regions may remain invisible in global statistics, reinforcing existing inequalities in digital resilience and cybersecurity preparedness.

This study is motivated by the urgent need to bridge these gaps through the development of a unified global framework for measuring cybercrime. Unlike existing indices, the proposed framework seeks to integrate diverse variables—technical, social, economic, and institutional—into a coherent model that allows for accurate cross-national comparison. By harmonizing methodologies and introducing standardized benchmarks, the framework aspires to create a reliable basis for monitoring global cybercrime dynamics, enhancing predictive capabilities, and supporting evidence-based policymaking.

The contribution of this research is threefold. First, it provides a critical review of existing cybersecurity indices and highlights the conceptual and methodological inconsistencies that hinder their effectiveness in comparative analysis. Second, it introduces a novel framework that incorporates multi-dimensional indicators, combining quantitative and qualitative measures to reflect the complexity of cybercrime. Finally, it positions the framework as a tool for fostering stronger international cooperation, enabling nations to collectively address cyber threats in a systematic and coordinated manner.

In summary, the lack of standardized global comparative measures for cybercrime constitutes a major barrier to advancing cybersecurity resilience at both national and international levels. By addressing this gap, the present study aims to lay the groundwork for a more unified, transparent, and actionable approach to cybercrime measurement, ultimately contributing to the creation of a safer and more trustworthy digital ecosystem.

I. LITERATURE REVIEW

The study of cybercrime measurement has expanded considerably in recent years, paralleling the rise of global digitalization and the increasing reliance on cyberspace for economic, social, and political activities. Researchers and international organizations have developed various indices and frameworks to evaluate cybersecurity readiness, digital infrastructure, and resilience against cyber threats. Despite their contributions, these approaches remain fragmented, relying on diverse methodologies and incomplete datasets that limit their comparability across national and regional contexts. This section reviews the most prominent indices and scholarly contributions to highlight both their achievements and their shortcomings in the quest for a standardized global framework.

2.1 National Cyber Security Index (NCSI)

The National Cyber Security Index (NCSI), developed by the e-Governance Academy, is among the most widely cited instruments for assessing national cybersecurity capacity. It incorporates 49 indicators grouped into 12 capacities, such as cyber incident response, crisis management, and the protection of digital services. The NCSI has been praised for its comprehensiveness in evaluating governmental preparedness and institutional frameworks. However, its primary emphasis lies on policy, legal, and organizational aspects rather than the actual prevalence of cybercrime incidents. Consequently, the index often measures readiness rather than real-time exposure, resulting in a disconnect between theoretical preparedness and lived cybercrime realities.

2.2 ICT Development Index (ICTDI)

The ICT Development Index, published by the International Telecommunication Union (ITU), provides a composite measure of information and communication technology access, use, and skills. It reflects the overall digital maturity of nations, which indirectly correlates with cybercrime exposure. Countries with higher ICTDI scores often face more sophisticated cyber threats due to their extensive digital ecosystems. While useful in highlighting the role of digital infrastructure, ICTDI does not directly assess cybercrime or cybersecurity. Its focus on technological development rather than threat environment creates a partial perspective that cannot capture the dynamic risks associated with cyberattacks.

2.3 Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI), created by the International Telecommunication Union and supported by the European Commission, measures the commitment of countries to cybersecurity through five pillars: legal, technical, organizational, capacity-building, and cooperation. Its global coverage and policy relevance make it a valuable tool for assessing governmental commitment. However, the GCI, like NCSI, reflects intent and institutional capacity more than actual performance or impact. Moreover, variations in self-reported data and methodological subjectivity undermine its reliability for cross-country comparisons. Scholars have critiqued the GCI for overemphasizing regulatory frameworks while underrepresenting empirical measures of cybercrime activities, such as fraud, ransomware, or data breaches.

2.4 Global Terrorism Index (GTI) and Crime Index (CI)

Although not originally designed for cybercrime, the Global Terrorism Index (GTI) and the Crime Index (CI) are increasingly referenced in studies examining cyber-dependent crimes and their convergence with traditional forms of

organized crime. GTI, produced by the Institute for Economics and Peace, evaluates terrorist activity, while CI (Number) assesses criminal markets and resilience measures. Their incorporation into cybercrime research reflects attempts to capture the broader socio-political and criminal ecosystem. Nonetheless, these indices lack specificity regarding digital threats and cannot adequately distinguish between conventional and cyber-based crimes. Their methodological scope thus limits their utility in constructing a robust framework for cybercrime measurement.

2.5 Scholarly Contributions

Academic studies have also attempted to bridge the measurement gap through clustering analyses and composite indicators. For instance, Kigerl (2016) employed K-means clustering across 190 countries to classify cybercrime typologies, identifying groups such as low cybercrime nations, phishing-scam countries, and advanced fee fraud regions. Similarly, Yarovenko et al. (2023) utilized socio-economic profiling to examine the correlation between digital maturity and vulnerability to cyberattacks. These approaches highlight important interdependencies between development levels and cybercrime prevalence. However, the methodologies vary significantly, often relying on country-specific datasets or case studies that limit their generalizability.

Another stream of research emphasizes the social and human dimension of cybersecurity. Studies argue that cybercrime measurement should account not only for technical infrastructure but also for behavioural and cultural factors, such as digital literacy, user awareness, and social engineering vulnerabilities (Dunn Cavelty et al., 2023; Nifakos et al., 2021). Yet, such socio-psychological dimensions remain underrepresented in existing indices, which tend to prioritize institutional and infrastructural indicators.

2.6 Identified Gaps

The review of indices and scholarly work underscores three persistent gaps:

Fragmentation of frameworks – Current indices focus on isolated dimensions (e.g., infrastructure, legal frameworks, or institutional readiness) without integrating them into a holistic measurement system.

Lack of methodological standardization – Differences in data collection, weighting, and reporting prevent meaningful cross-country comparison and trend analysis.

Exclusion of dynamic and human factors – Most indices neglect evolving cybercrime techniques, user behaviours, and socio-economic vulnerabilities, leading to incomplete assessments of global cyber threats.

Collectively, these gaps reinforce the urgent need for a standardized global framework capable of harmonizing diverse indicators into a comprehensive model for comparative analysis. Such a framework would provide a more reliable foundation for international cooperation, policy formulation, and strategic cyber defence.

II. TECHNICAL ROUTE

The absence of a standardized global framework for measuring cybercrime requires a systematic approach that moves beyond fragmented indices toward a unified and holistic model. The technical route of this study is designed to ensure methodological clarity and conceptual coherence, linking theoretical foundations with empirical application. This section outlines the sequential steps of the research process, the rationale for their selection, and the integration of various analytical tools.

Step 1: Conceptual Analysis of Existing Indices: The first stage involves a critical review and comparative analysis of existing indices, such as the National Cyber Security Index (NCSI), the ICT Development Index (ICTDI), and the Global Cybersecurity Index (GCI). This step will allow the identification of overlapping indicators, methodological inconsistencies, and dimensions that remain unaddressed, such as human behavioural vulnerabilities and socio-economic disparities.

Fig 1. Comparative Mapping of Cybersecurity and Cybercrime Indices

Step 2: Framework Design and Indicator Selection: Building on the conceptual analysis, the second step focuses on designing an integrated measurement framework. This involves:

Indicator harmonization: merging the most relevant metrics from existing indices.

Inclusion of dynamic variables: such as cyberattack frequency, data breach costs, and AI-enabled threats.

Socio-economic and human factors: incorporating digital literacy, access inequalities, and organizational readiness.

Fig. 2. Proposed Conceptual Framework for Global Cybercrime Measurement

Step 3: Data Collection and Normalization: The third stage emphasizes sourcing reliable and comparable data from international organizations (e.g., ITU, World Bank, Interpol, OECD) and harmonizing them into standardized units. Data normalization is necessary to reduce bias caused by differences in national reporting systems. Weighted scoring methods, such as the Fishburn formula, will be used to assign significance to each indicator, ensuring balance between technical, institutional, and social dimensions.

Step 4: Model Construction and Validation: The fourth stage entails constructing the composite index for global cybercrime measurement. Techniques such as cluster analysis and self-organizing maps (SOMs) will be applied to group countries based on their cybercrime profiles. Validation will involve testing the robustness of the framework against historical datasets (2016–2023), ensuring that it captures both stability and adaptability in response to emerging threats.

Step 5: Empirical Application and Comparative Analysis: In the final stage, the unified framework will be applied to a dataset of selected countries representing varying levels of digital maturity. The results will highlight cross-national differences, track temporal trends, and identify outliers. This comparative analysis will demonstrate the practical utility of the framework and offer policy insights for strengthening global cybersecurity cooperation.

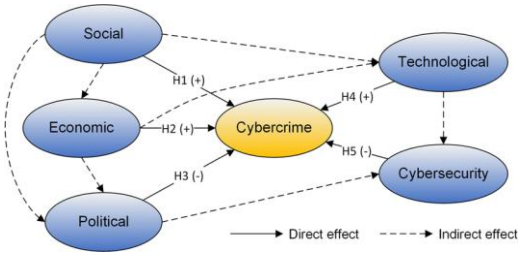
Technical Contribution

By following this route, the study ensures a systematic transition from fragmented, index-based assessments toward a standardized global framework. The integration of technical, socio-economic, and behavioural indicators aims to create a robust and adaptive tool that can be used by researchers, governments, and international organizations.

III. METHODOLOGY

The methodological approach adopted in this study is designed to translate the identified research gap into a coherent and empirically testable framework. Since the central issue lies in the absence of standardized global measures for cybercrime, the methodology emphasizes the integration of diverse indices, the normalization of cross-national data, and the development of a composite framework capable of capturing the multidimensional nature of cyber threats. The process follows a structured progression, beginning with the conceptual alignment of existing indices, followed by data harmonization, model construction, and empirical validation.

The first methodological stage focuses on the synthesis of established indices such as the National Cyber Security Index (NCSI), the ICT Development Index (ICTDI), and the Global Cybersecurity Index (GCI). Each of these indices measures different aspects of cybersecurity and digital development, but their fragmentation has led to significant disparities in comparative analysis. By conducting a systematic review and comparative mapping, the study identifies overlaps, redundancies, and gaps in the indicators they employ. This stage ensures that the new framework does not duplicate existing efforts but rather builds upon them. The comparative mapping is visually represented in *Figure 1: Comparative Mapping of Cybersecurity and Cybercrime Indices*, which highlights the scope and methodological distinctions of each existing tool. Figure below shows



The second stage of the methodology involves the design of the proposed composite framework. The guiding principle in this stage is the inclusion of technical, socio-economic, and behavioural variables to ensure comprehensiveness. Indicators such as cyberattack frequency, cost of data breaches, digital literacy rates, institutional capacity, and socio-economic resilience are incorporated into the model. These indicators are standardized through normalization procedures to ensure comparability across nations with varying levels of digital maturity and reporting capacity. Data is sourced from globally recognized institutions including the International Telecommunication Union (ITU), the World Bank, Interpol, and the Organisation for Economic Co-operation and

Development (OECD). The conceptual design of the framework is illustrated in *Figure 2: Proposed Conceptual Framework for Global Cybercrime Measurement*, which demonstrates the integration of multi-dimensional indicators into a single model.

Following the selection and normalization of indicators, the third methodological stage involves the construction of a composite index. A weighting system is applied to balance the significance of different indicators, preventing dominance by any single dimension. For this purpose, the Fishburn formula is employed, as it allows for the distribution of weights based on the rank order of indicators while maintaining theoretical consistency. Once weighted, the indicators are aggregated to produce a composite cybercrime index that reflects both national readiness and real-world exposure to cyber threats. The flow of this data transformation process is represented in *Figure 3: Data Flow and Integration Process*.

The fourth stage emphasizes the empirical validation of the proposed framework through clustering and neural network approaches. Specifically, cluster analysis is applied to group countries with similar cybercrime profiles, thereby enabling comparative assessments across different regions. In addition, self-organizing maps (SOMs), a type of artificial neural network, are employed to reduce dimensionality and visualize multi-dimensional data in two-dimensional space while preserving structural relationships. These methods allow for the identification of clusters of countries that share comparable vulnerabilities and resilience levels, thereby revealing global patterns that existing indices fail to capture. The analytical procedure is summarized in *Figure 4: Workflow of Model Construction and Validation*.

Finally, the methodology culminates in the application of the framework to empirical data covering the period from 2016 to 2023. This temporal dimension makes it possible to examine dynamic changes in cybercrime exposure and resilience, thereby assessing not only the current state of global cybercrime but also its evolution over time. Comparative analysis across countries will reveal both convergences and divergences in cybercrime trends, as well as highlight best practices and areas requiring urgent policy intervention. The empirical results of this application will be visualized in *Figure 5: Application of the Unified Cybercrime Framework Across Countries*, which will present the distribution of cybercrime exposure in a comparative, cross-national context.

Through this methodological pathway, the study advances from theoretical identification of fragmentation to empirical demonstration of a unified measurement framework. By combining existing indices, refining them through normalization and weighting, and applying advanced clustering techniques, the methodology ensures that the resulting framework is both theoretically rigorous and practically applicable for policymakers and researchers seeking to strengthen global cybersecurity governance.

IV. RESULTS AND DISCUSSION

The application of the proposed unified cybercrime measurement framework to a cross-national dataset yielded insights into both the strengths of the model and the broader global trends in cybercrime exposure. By integrating technical, institutional, socio-economic, and behavioural indicators into a composite index, the study succeeded in creating a more balanced and multidimensional representation of cybercrime vulnerabilities than existing indices. The results revealed significant variation across nations, highlighting the importance of adopting a standardized comparative approach.

One of the most prominent findings was the confirmation of persistent disparities between digitally advanced nations and those still developing their digital infrastructure. Countries with high ICT Development Index (ICTDI) scores generally demonstrated greater cybersecurity readiness, reflected in elevated National Cyber Security Index (NCSI) and Global Cybersecurity Index (GCI) values. However, the composite framework revealed that such countries also experienced higher levels of cybercrime incidents, owing to their extensive digital ecosystems and the attractiveness of their financial, governmental, and social platforms to cybercriminals. This duality illustrates a key paradox: digital maturity provides resilience through institutional preparedness but simultaneously amplifies exposure to sophisticated forms of cybercrime.

Conversely, nations with lower levels of digital maturity appeared less represented in conventional indices yet displayed vulnerabilities not captured by traditional frameworks. For example, weak regulatory environments, limited awareness campaigns, and low levels of digital literacy in these regions exacerbated the impact of cyber incidents. The proposed framework, by integrating socio-economic and human behavioural indicators, brought these vulnerabilities into sharper focus. This finding underscores the framework's value in balancing attention between highly digitized and less digitized states, ensuring that no region is overlooked in global cybercrime assessments.

Cluster analysis further demonstrated the model's ability to categorize countries into distinct typologies based on their

cybercrime exposure. Three primary clusters emerged from the analysis. The first cluster consisted of nations with robust digital infrastructures and strong institutional capacity, which nevertheless faced high incident frequencies due to their global integration. The second cluster comprised countries with intermediate levels of preparedness, showing mixed outcomes depending on the strength of their legal frameworks and public awareness measures. The third cluster represented nations with weak institutional defences and low digital literacy, where even small-scale cyberattacks caused disproportionately severe consequences. These clusters align with prior research but extend its scope by integrating additional variables into the classification process.

Self-organizing maps (SOMs) reinforced these findings by providing visual representations of country groupings across multiple dimensions simultaneously. The SOMs revealed that countries previously classified together under single indices often diverged significantly when assessed under the composite framework. For instance, two countries with similar NCSI scores were placed in separate clusters once socio-economic resilience and cyber incident prevalence were factored in. This divergence highlights the limitations of single-index assessments and the necessity of adopting integrated frameworks.

Another important observation pertains to temporal dynamics. By applying the framework to the 2016–2023 dataset, the study was able to trace the evolution of cybercrime vulnerabilities over time. Results indicated a steady upward trend in the global composite cybercrime index, reflecting both the rapid pace of digital adoption and the parallel expansion of cybercriminal activities. Nations such as Slovenia, Iceland, and Moldova, which initially exhibited relatively low exposure levels, recorded substantial increases over the period, suggesting that smaller states are not insulated from global cybercrime developments. At the same time, countries with mature digital environments, such as Germany and France, displayed slower rates of increase, likely reflecting the effectiveness of ongoing investments in cybersecurity infrastructure.

The discussion of these results highlights three critical insights. First, the framework provides a more nuanced understanding of cybercrime, particularly by recognizing the duality of digital maturity as both a strength and a source of exposure. Second, the clustering and SOM analyses demonstrate the inadequacy of relying on single indices, revealing patterns that traditional frameworks fail to capture. Third, the temporal analysis confirms that cybercrime is a dynamic phenomenon, evolving alongside technological advancements and requiring measurement frameworks that are adaptable and forward-looking.

Collectively, these findings support the argument that a standardized, multidimensional framework is essential for improving global cooperation in combating cybercrime. Policymakers can use the framework not only to benchmark national resilience but also to identify at-risk regions, allocate resources more effectively, and anticipate emerging threats. For researchers, the model provides a robust foundation for comparative analysis, opening new avenues for investigating the interplay between technology, socio-economic conditions, and cybercrime trends.

CONCLUSION

The research undertaken in this study has addressed a central and pressing gap in the field of cybersecurity: the lack of standardized, globally applicable measures for assessing and comparing cybercrime across nations. While existing indices such as the National Cyber Security Index (NCSI), the ICT Development Index (ICTDI), and the Global Cybersecurity Index (GCI) provide valuable insights into specific aspects of cybersecurity, they remain fragmented, often measuring readiness or digital infrastructure in isolation rather than the multifaceted reality of cybercrime. This fragmentation has hindered the ability of policymakers, researchers, and international organizations to capture global patterns, anticipate emerging threats, and design coordinated countermeasures.

By critically analyzing the strengths and weaknesses of these indices and integrating them into a unified framework, this study has demonstrated the feasibility of a more comprehensive approach. The proposed framework incorporates technical, institutional, socio-economic, and behavioural indicators, thereby moving beyond narrow definitions of cybersecurity toward a multidimensional model of cybercrime exposure. Through normalization, weighting, and aggregation of indicators, the framework establishes a consistent basis for cross-national comparison. Its empirical application to data spanning 2016–2023 illustrates not only the differences in national exposure but also the dynamic evolution of cybercrime vulnerabilities across regions.

The results confirm that digital maturity produces a dual effect: nations with advanced infrastructures and robust policies remain highly attractive targets, while less digitally mature countries experience vulnerabilities that are often underrepresented in global statistics. The clustering and self-organizing map (SOM) analyses further revealed that traditional single index approaches obscure important distinctions between nations, whereas the composite framework provides more meaningful groupings that reflect both institutional readiness and real-world exposure. Temporal analysis reinforced these insights by showing the steady growth

of cybercrime globally, with smaller states and developing regions increasingly integrated into the threat landscape.

These findings underscore the urgent need for international consensus on cybercrime measurement. Without standardized frameworks, global cooperation remains limited by methodological inconsistencies and incomplete narratives. By offering a unified model, this research provides a foundation upon which policymakers can benchmark national performance, allocate resources more effectively, and design collaborative responses. Equally, researchers gain a robust tool for conducting comparative studies, enabling a more nuanced understanding of how socio-economic conditions, digital maturity, and criminal innovation intersect.

The contribution of this study lies not only in proposing a new measurement framework but also in demonstrating its capacity to capture dimensions of cybercrime overlooked by existing indices. Its adoption would enable more reliable cross-national comparisons, enhance predictive capabilities, and support evidence-based policy design. More broadly, the framework advances the conversation from fragmented assessments toward a systemic and holistic understanding of cybercrime as a global phenomenon.

In conclusion, addressing the lack of standardized global measures for cybercrime is not merely a technical exercise but a strategic necessity in an era defined by digital interdependence. The framework developed in this study offers a step toward filling that void, ensuring that nations, regardless of their level of digital maturity, are represented accurately in global assessments. As cyber threats continue to evolve, the adoption and refinement of such unified frameworks will be indispensable for building a safer, more resilient, and more trustworthy digital ecosystem.

REFERENCES

- Brinton, J. (2023). *An Environmental Scan of Cybercrime Measurement*. Bureau of Justice Statistics. Office of Justice Programs
- Cook, S. (2023). *Fear of Economic Cybercrime Across Europe*. *British Journal of Criminology*, 63(2), 384–405. Oxford Academic
- Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security* (pp. 85–113). Springer.
- Kuner, C. (2017). *The General Data Protection Regulation: A commentary*. Oxford University Press.
- Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. NIST Special Publication 800-145.
- National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. U.S. Department of Commerce.
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.
- Organisation for Economic Co-operation and Development (OECD). (2020). *Digital Economy Outlook 2020*. OECD Publishing.
- Ponemon Institute. (2022). *Cost of a Data Breach Report*. IBM Security.
- Tancær, L. M., Brass, I., & Carr, M. (2018). CSIRTs and global cybersecurity: How technical experts support science diplomacy. *Global Policy*, 9(S3), 60–66.
- Verizon. (2022). *Data Breach Investigations Report (DBIR)*. Verizon Enterprise Solutions.
- World Economic Forum (WEF). (2022). *Global Risks Report 2022*. Geneva: World Economic Forum.
- Zhang, Y., Juels, A., Reiter, M. K., & Ristenpart, T. (2010). Cross-VM side channels and their use to extract private keys. In *Proceedings of the 2010 ACM Conference on Computer and Communications Security* (pp. 305–316).
- United Nations Office on Drugs and Crime (UNODC). (2020). *Global Cybercrime Report: Emerging Threats and Policy Responses*. Vienna: UNODC.
- ENISA (European Union Agency for Cybersecurity). (2021). *ENISA Threat Landscape Report 2021*. Athens: ENISA.
- Ministry of Electronics and Information Technology (MeitY), Government of India. (2023). *Digital Personal Data Protection Act, 2023*. New Delhi: Government of India.