

Systems Thinking in Cybersecurity; Ending with the Beginning in Mind.

Michael Collins^a@

a: Independent Researcher and Chief Information Security Officer, Melbourne, Australia

@: w_michaelcollins@hotmail.com

ABSTRACT: Despite the increasing complexity of the digital landscape and the rise in cyber-attacks, systems thinking has not been widely utilized in cybersecurity. This research paper employs a Systems Literature Review to examine the current state of knowledge regarding the use of systems thinking in cybersecurity and identifies several issues, including the lack of consistency in defining "systems thinking", narrow use cases, and a lack of empirical evidence supporting the reviewed methods. Different researchers and practitioners may have varying interpretations of this concept, leading to confusion and a lack of standardized approaches. This inconsistency hampers the development of a cohesive framework for applying systems thinking in cybersecurity. To address these challenges, future research should focus on developing a common understanding and definition of systems thinking in the context of cybersecurity. This will facilitate communication and collaboration among researchers and practitioners, leading to more consistent and effective approaches. Additionally, there is a need for empirical studies that rigorously evaluate the impact of applying systems thinking in cybersecurity. These studies should assess the effectiveness of different methodologies and frameworks in real-world scenarios, providing evidence-based insights into their benefits and limitations. In conclusion, while the application of systems thinking in cybersecurity holds promise, there are challenges that need to be addressed. Resolving these challenges is crucial for advancing the field and establishing a solid foundation for the application of systems thinking in cybersecurity¹.

KEYWORDS: Systems Thinking | Cybersecurity | Information Security | IT Security | Computer Security

Statement of Significance & Public Understanding

The significance of this academic paper lies in its unique contribution to the field of systems thinking and cybersecurity. To the author's knowledge this paper is the first of its kind, it focuses on providing a snapshot of the condition of knowledge related to systems thinking in addressing cybersecurity challenges. By understanding the current state, a path forward is presented that will provide valuable insights for both academics and practitioners in the field.

¹ Cite this Paper: Collins, M. (2024) Systems Thinking in Cybersecurity; Ending with the Beginning in Mind. Journal of Systems Thinking. (XX) X.

Research Methodology

Research Questions

This study aimed to address the following research questions:

1. What is the condition of knowledge regarding the application of systems thinking in the field of cybersecurity?
2. What theories, models, methods, and frameworks are being used today in the field?
3. What are the specific scenarios in which systems thinking is being utilized in the field of cybersecurity?

Coverage

This Systematic Literature Review utilizes the PRISMA method, as described by Cabrera et al. [1], to employ a quantitative approach for narrowing down the scope of the review to a feasible number of papers, while maintaining the necessary emphasis to address the research questions. The primary advantage of employing this methodology is to guarantee the selection of a comprehensive and unbiased assortment of both scholarly and public works through a methodical, transparent, and replicable procedure.

Search Types

Three types of searches were conducted to ensure a comprehensive view of the condition of knowledge from three different perspectives.

Scholarly Search

The scholarly search was used to understand the scientific community's perspective on the topic.

Hasty Search

The hasty search is used to ensure that publications crucial to the overall understanding of the topic are not overlooked.

Public Search

The public search is used to understand the general population's perspective on the topic of interest.

The following databases were selected to provide the required coverage.

Selected Databases

Database	Type	Benefit	Search Type
Cornell Library	Academic	High quality large collection of papers. Provides access to many paywalled journals.	Scholarly Search
Google Scholar	Academic / Accessible	Accessible to anyone. Generally high-quality collection of publications. Has the ability to search for just literature reviews as well.	Scholarly Search / Hasty Search (most cited criteria)
Semantic Scholar	Academic / Accessible	Accessible to anyone, mainly focuses on journal articles. Uses machine learning techniques to extract meaning and identify connections from within papers. Ability to sort by 'citation count' and 'most influential papers'.	Scholarly Search / Hasty Search (most cited criteria)
Google Search	Search Engine	Popular search engine for resources accessible to the public.	Public Search / Hasty Search

Search Terms

Given the research questions the initial search term selected was "systems thinking" AND "cybersecurity". The Boolean operator 'AND' was applied to indicate that both terms should be present in

the findings, leading to more precise and relevant results. However, the initial search results which were returned also included phrases such as information security, IT security, and computer security. After examining the usage of these phrases using Google Books Ngram Viewer (refer to Figure 1), it was seen that from the early 1960s, each of these four terms has been used to varying degrees, with "cybersecurity" being the most used keyword in recent times.

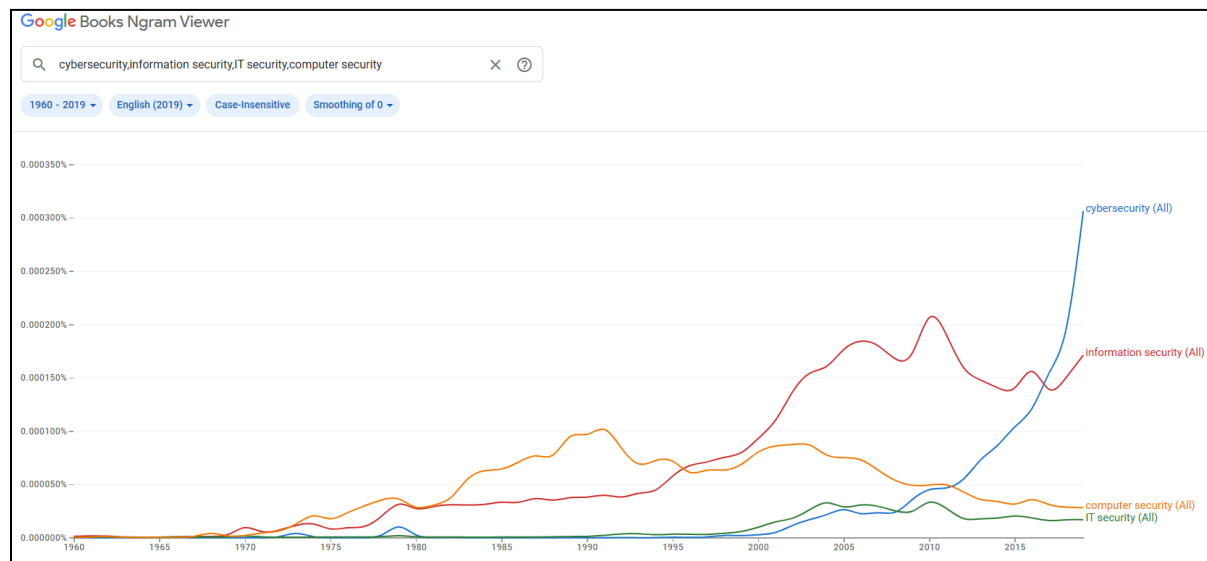


Figure 1 - Google Ngram Search Term Usage

To accurately capture the evolving usage of the terms, the Author made the decision to expand the range of included phrases in the search results to the following.

1. 'systems thinking' AND 'cyber security'
2. 'systems thinking' AND 'information security'
3. 'systems thinking' AND 'IT security'
4. 'systems thinking' AND 'computer security'

The results which were returned from the scholarly databases using the search terms are shown in Table 3².

Level of Review	Acceptance Criteria	Exclusion Criteria
Title	The title of the paper is relevant to the research question(s) and includes the search terms.	The title does not include the search terms and is not relevant, uninformative, or unclear.
Abstract	The abstract of the paper is relevant to the research question(s) and includes the search terms.	The abstract does not include the search terms, is not relevant, explores a different aspect of the topic than

		intended or displays insufficient methodology.
Full Text	The full text of the paper is relevant to the research question(s) and includes the search terms.	The full text does not include the search terms, is not relevant, explores a different aspect of the topic than intended or displays insufficient methodology.

Table 1 - Selection Criteria

In the preliminary stage, all articles that met the requirements of the title were kept for further assessment. In the second round, the articles were then reviewed to identify abstracts that met the specified criteria. The candidates who successfully cleared the second selection process then advanced to the third and final round evaluation, while those who failed to meet the criteria were excluded from further consideration. Subsequently, a comprehensive evaluation of the remaining papers was conducted, and those that satisfied the final criteria were chosen as the final papers for the analysis stage.

The notable aspect of this selection method is the significant quantity of outcomes retrieved from public databases like Google Scholar that despite the narrow search term did not meet the initial inclusion criteria. The main reason for this was the lack of capability to customize sophisticated or numerous filters to efficiently exclude a significant amount of false positive results. Many of the false positive results used terms such as "system theoretic", "thinking in systems", and "a systematic approach", but further analysis revealed that they were not relevant to the topic of interest. In these instances, a meticulous examination of the outcomes was required to pinpoint potential candidates for later evaluation.

Hasty Search

A hasty search is used to identify prominent scholars in the field that may have been overlooked during the scholarly search Cabrera et al. [1]. Where scholarly search employed specific inclusion and exclusion criteria to ensure a methodical approach in selecting relevant literature, the hasty search adopted a time-bound strategy and relied on subjective judgment to choose which authors and their works to include. To begin the procedure, the initial step was entering the search term "systems thinking" AND "cybersecurity" into Semantic Scholar, accompanied by a specific set of filters as seen in Figure 1.

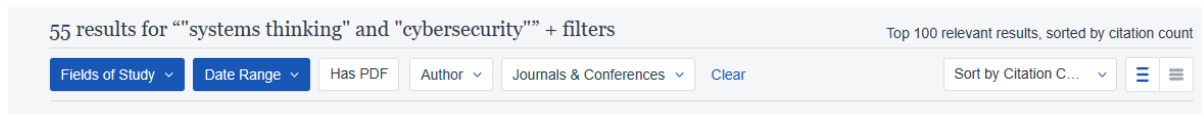


Figure 2- Semantic Scholar Hasty Search by Citation Count

The findings were subsequently sorted based on the number of citations to provide the Top 10 results. These results were then extracted and recorded in Table 4². Subsequently, the identical methodology was employed, however, the outcomes were sorted based on the Top 10 Most Influential Papers as shown in Figure 3.

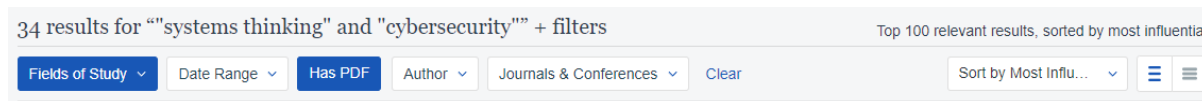


Figure 3- Semantic Scholar Hasty Search by Most Influential Paper

These findings were then retrieved and recorded in Table 4². Subsequently, the papers underwent a review process, during which any duplicates identified through the scholarly search were eliminated. Additionally, publications that were considered irrelevant were also excluded. The authors of the publications were then examined on Google Scholar to analyze their profiles and ascertain the total amount of citations for each author, as well as their affiliation. Subsequently, the table was sorted to determine the Top 5 authors based on their total citations, as presented in Table 2 below. Each author's papers were then evaluated to ascertain their potential contribution to the literature review, as well as any secondary sources referenced by the scholars in the chosen papers.

Scholar	Affiliation	Citations	No. Articles Selected from Publications	No. Articles Selected from Cited Works
Elisa Bertino	Purdue University	56,094	1	1
Igor Linkov	US Army Corps of Engineers	25,045	0	0
Stuart Madnick	Massachusetts Institute of Technology	13,052	0	1
Fabio Massacci	University of Trento	9,801	0	0
Nicola Dragoni	Technical University of Denmark	5,971	0	0

Table 2- Hasty Search of Scholars

Analysis

To address the research questions, a specific set of variables was selected to review and compare each publication. This data is essential for establishing a standardized strategy for analysis. Following is a summary of the analysis of the articles discovered by the Scholarly and Hasty search method according to the following variables.

1. Publication Title
2. Author/s
3. Summary
4. Cybersecurity Discipline
5. Industry
6. Research Method
7. Statistical Significance
8. Systems Thinking Method

In the paper titled “A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education” by Zoto et al. [2] they propose the application of a Socio-technical Systems (STS) approach using simulation-based teaching tools in cybersecurity and risk management education. The main thrust of the research is to promote the usage of systems thinking in cybersecurity education and to bridge the gap between theoretical models and real-world cyber-attacks. The research employs a combination of theoretical models and data from real-world cases to model and build a simulation-based teaching tool in adversarial and systems thinking, aiming to raise awareness of cybersecurity among students and practitioners in the ICT ecosystem.

The research defines systems thinking as “a process that considers the interplay between social and technical constraints to enable assured operations”, where system behavior results from the effects of reinforced processes stemming from environments. Use of systems thinking was limited to the identification of the relevant attributes related to the Social and Technical Systems approach which then formed the basis of the quantitative simulation to estimate key variables of information security risks.

The research also conducted experiments to measure the impact of the tool on students' understanding of concepts related to adversarial and systems thinking, as well as its usability and coverage from the cybersecurity professionals' perspective.

However, out of the students that took part in the simulations, only 2 out of the 8 participants acknowledged that the simulation enhanced their comprehension of systems thinking. During a subsequent simulation, only 3 out of the 10 participants believed that the simulation enhanced their comprehension of systems thinking. Although the authors argue for the application of systems thinking to enhance students' comprehension of cybersecurity, the methodologies employed lack sufficient empirical support.

Burrell et al. [3] undertake a literature study titled "Exploring System Thinking Leadership Approaches to the Healthcare Cybersecurity Environment" to analyze the organizational behavior of healthcare cybersecurity. They specifically focus on how organizations utilize systems thinking to manage project risks and enhance healthcare leadership. The paper emphasizes the complexity of cybersecurity, which encompasses diverse security issues influenced by multiple factors from various fields such as sociology, psychology, and information technology. It highlights the interrelationships between components in cyberspace, emphasizing the need for a systems thinking approach to understand the connectivity and interdependencies within the healthcare cybersecurity environment. The authors also discuss the impact of organizational systems on workers' conduct and the need for adaptive healthcare leadership to manage the dynamic and complex systems within an organization.

It applies the General Systems Theory to outline how this can assist in overcoming organizational behaviors that do not contribute to improved cybersecurity outcomes and highlights the use of Senge's learning culture to think about cybersecurity risks and vulnerabilities from a holistic and rational perspective.

The study has limitations as it does not seek to provide a comprehensive and integrated definition of systems thinking, nor does it present any empirical evidence of how systems thinking would be practically applied in this context beyond the conceptual level.

The paper "Incorporating Systems Thinking Into a Cyber Resilience Maturity Model" explores a methodology pertaining to improving cyber resilience of critical infrastructure. Shaked et al. [4] propose the utilization of systems thinking as a method of "reimagining them as a system of systems". The text proposes investigating cyber resilience as an inherent characteristic of a system, which encompasses many aspects of the sector's operations and distinct areas of practice. The authors highlight the limitations of existing cybersecurity maturity models, claiming "existing maturity models typically lack a holistic view on the subject sector, focusing on the assessment of a single constituent".

Essentially, the purpose of the model is to consider an organization as a part whole system within an industry sector, making the distinction at a sectoral level. The model is entirely focused on resilience as an emergent property of the inter-relationships between the critical factors outlined in the proposed maturity model.

While the study has effectively showcased the conceptual advantages of evaluating cyber resilience from a holistic perspective, it is important to note that the findings are limited by at least two factors. Initially, the work lacks adequate attention to the precise definition of systems thinking. Furthermore, it fails to provide a satisfactory explanation of the practical application of systems thinking. Further investigation is required to determine the empirical basis for the model's efficacy.

Kawade & Yamamoto [5] in their paper “A Method to Analyze Cyber Security Guidelines using System Thinking” discuss the implementation of Boardman Soft Systems Methodology (BSSM), as well as the method and process for developing Systemigrams (system diagrams) within the framework of cybersecurity standards and engineering procedures in the automotive industry. According to Kawade & Yamamoto [5], “Systems thinking makes it possible to systematically analyze who performs system activities, for what purpose, and by what means”. They propose the use of Systemigrams as a method for analyzing and visualizing complex systems in various domains, such as cybersecurity guidelines, service design, engineering processes, and production systems. The paper also proposes to address the gaps between systems engineering and systems thinking, highlighting the potential of Systemigrams as a practical tool for system analysis and design, as well as for articulating stakeholder value.

Kawade & Yamamoto [5] are of the opinion that BSSM and Systemigrams are a valuable tool for analyzing and visualizing complex systems across various domains, offering a practical and comprehensive approach to system analysis, design, and stakeholder value. None of the provided references discuss an empirical basis for these claims or provide a statistical analysis of the results.

The paper “Security from a systems thinking perspective - Applying soft systems methodology to the analysis of an information security incident” by Alsabbagh & Kowalski [6] presents an application of Soft Systems Methodology (SSM) to analyze a real case security incident in an organization. The main thrust of the paper is to demonstrate how SSM can be a beneficial tool for security analysts during security incident management and risk analysis, particularly in dealing with unstructured situations where human beings are part of the socio-technical system. Alsabbagh & Kowalski [6] make a distinction between hard system thinking which perceives the world as systemic and describe soft systems thinking as a distinct set of activities the systems thinker applies to perform an analysis before moving back to verification in the

‘real world’. Alsabbagh & Kowalski [6] promote SSM as an effective method to recognise the mental models of how a security analyst should think systemically to understand the inter-related parts of the system from both a technical and social perspective, and the role that individual cognition plays in determining the security culture of an organization.

The authors advocate for the effectiveness of SSM in enhancing relationships and communication among stakeholders, as well as in capturing stakeholder attitudes towards security incidents. They also identified limitations in applying SSM in this context suggesting that SSM should be viewed as a "managerial tool" that offers comprehensive insights into an organization's security. Additionally, the basis for its effectiveness is limited in that it makes no reference to empirical evidence to substantiate the claims.

The thesis of the paper “Applying Systems Thinking to Healthcare Data Cybersecurity” by Chung [7] centers around the analysis of cybersecurity incidents and the need for a holistic and socio-technical perspective in understanding and addressing cybersecurity risks. The main points include defining accidents in the context of cybersecurity, sharing incident information within communities, the increase in cybercrimes in healthcare organizations, the inadequacy of static cybersecurity strategies, and the importance of understanding cybersecurity risks by management. The approach employed entails the examination of cybersecurity events utilizing the System-Theoretic Accident Model and Processes (STAMP) technique, which was devised by Nancy Leveson at the Massachusetts Institute of Technology, as acknowledged by Chung [7]. The method generates a series of recommendations for improving the control environment to prevent the incident from reoccurring. Based on the provided references, there is no direct mention of statistical significance or statistical analysis in the context of cybersecurity incidents and risk analysis.

“Building Capacity for Systems Thinking in Higher Education Cybersecurity Programs” by Enright et al. [8] collectively focuses on building capacity for systems thinking in higher education cybersecurity programs. The paper proposes "systems thinking" as a holistic and inductive approach to student education, teaching theoretical concepts while reinforcing broad concepts with applied exercises. It emphasizes the need to contextualize instruction on a specific topic by teaching students to situate their learning on the system level. Enright et al. [8] provide many definitions for systems thinking, citing several sources, but do not explicitly state a definitive interpretation, except for acknowledging the significance of context. Given the various interpretations of systems thinking among academics, it is crucial to attempt to resolve the specific usage of the word, particularly in a study advocating for its integration into educational curricula. This study presents a theoretical framework for applying systems

thinking to the establishment of cybersecurity programs in higher education. The conclusions lack empirical proof or statistical significance.

The paper titled "Examining Business Alignment Challenges Arising from the Cybersecurity Culture of the Norwegian Specialist Health Services, Utilizing a Systems Thinking Approach" by Vagle [9] underscores the significance of employing systems thinking to comprehend the drivers behind business misalignment within healthcare systems and the repercussions on the cybersecurity posture of these systems. Vagle's research on cybersecurity and systems thinking in healthcare organizations uses a mixed method of qualitative and quantitative modeling techniques. The author relies on Socio-technical Systems theory and Systems Dynamics to define the term 'systems thinking' in the context of analyzing organizational behavior. Causal loop diagrams are used to create a comprehensive system dynamic model that helps detect issues which arise from the intricate interconnections associated with the cybersecurity culture of key stakeholders. In conclusion, the research on cybersecurity and systems thinking in healthcare organizations provides insights into the complex dynamics that affect cybersecurity culture and business alignment, the need for systems thinking approaches, and the interconnected nature of systems and actors within the healthcare system. Vagle [9] recognizes that the absence of qualitative data influenced the validity of the model and introduced constraints that might hinder the use of the simulation model.

Yan [10] examines the use of systems thinking theories and methodologies for the purpose of constructing cybersecurity models. The paper "A Systems Thinking for Cybersecurity Modelling" elucidates the intricate dynamics of the operational environment in which organizations function, highlighting that the prevailing advantage is clearly tilted towards the attacker due to factors such as complexity, asymmetric information, and the comparative costs associated with attack and defense. Yan [10] concludes that "systems thinking can be considered as one of the powerful tools of cybersecurity modeling to find, characterize, understand, evaluate, and predict cybersecurity". Yan [10] provides a definition of systems thinking as "a holistic approach intended to analyze how the parts of the system interact and how the emergence changes as a whole entity".

The paper briefly references several systems theories and methods to develop mathematical models with a goal of predicting cybersecurity events. The author advocates for the advantages of systems thinking; yet their research is limited to theoretical use without sufficiently explaining its practical implementation in this setting. The results collected did not demonstrate any empirical evidence or statistically significant conclusions.

The paper "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks" by Salim [11] focuses on the application of systems thinking and systems theory in the context of cybersecurity. The main points covered in the paper include the challenges posed by the dynamic and complex Web 2.0 environment, the limitations of traditional technology-centric approaches, and the need for a new method to manage cybersecurity risks effectively. The Cyber Safety approach suggested by Salim is derived from Nancy Leveson's Systems-Theoretic Accident Model and Processes (STAMP) model which is employed for pre- or post-incident analysis. Salim [11] relies on Senge's definition of system thinking as "a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static 'snapshots'". The report employs a case study to showcase its efficacy and asserts that it uncovers many factors that may have contributed to the cybersecurity incident, which were not identified in prior post-incident assessments.

In his work titled "Complex system governance requires systems thinking - how to find systems thinkers," Jaradat [12] argues that there is a lack of comprehensive knowledge about the necessary systems thinking skills for effective system governance. Jaradat's view is that complex systems exhibit characteristics such as emergence of unintended behaviors and patterns which require skills in systems thinking to effectively understand the overall picture of the system prior to governance design and analysis. Although Jaradat acknowledges cyber warfare as a domain of system governance, the article is conceptual in nature and does not provide clear details on its practical implementation. The study draws upon definitions of systems thinking derived from theories such as General Systems Theory, Soft System Methodology, and Systems Dynamics. Jaradat [12] recognizes the need for further research to fully understand the application of systems thinking as a method for enhancing understanding of complex system governance.

"Educating for AI Cybersecurity Work and Research: Ethics, Systems Thinking, and Communication Requirements", by Matei & Bertino [13] investigates the discrepancy between the perceived level of cybersecurity education readiness in professional settings and academic institutions, specifically related to the use of artificial intelligence in cybersecurity. The study specifically concentrates on three important domains: ethics, systems thinking, and communication. Matei & Bertino [13] found "both managers and professors perceive preparedness to use AI tools in cybersecurity to be significantly associated with all three non-technical skill sets". Moreover, the research suggests that people who have a higher level of preparedness in using AI technology also possess greater competence in these areas. Matei & Bertino [13] propose that systems thinking is comprised of four dimensions: "thinking through consequences, trade-off thinking, privileging the whole over the parts, and seeking patterns". Although the authors presented a definition of systems thinking, they did not explicitly reference any of the theories that are related to

systems thinking. The quantitative analysis of the survey results gathered during the research concluded that preparedness to use AI tools to be significantly associated with all three categories.

This section has presented a brief analysis of the chosen literature, with a specific emphasis on the key variables.

Synthesis

In the following section a review of what the selected literature says in its entirety will be synthesized to address the research questions. Particular attention will be placed on the research methodologies employed in the literature, the essential vocabulary utilized, and the specific disciplines and areas of study that have been the focus of the research. This will offer opportunities for acquiring novel insights that might serve as the foundation for subsequent research efforts.

Research Methods

The condition of knowledge is a critical factor that guides the selection of research methods. It refers to the current state of understanding or awareness about a specific topic. The author chose to employ a simple heuristic framework, shown in Figure 4 below, known as the Knowledge-Method Matching Matrix (K-MMM). Proposed by Cabrera & Cabrera [14] this matrix serves the purpose of identifying the relationships between the condition of knowledge and the type of methods used in the selected papers. The K-MMM operates on a continuum, moving from a nascent stage, where knowledge is just beginning to form, through a developing phase, to a mature stage, where knowledge is well-established and widely accepted.

Method

- Observation (Theorizing)
- Questioning (Interview, Survey)
- Experimental Design (Quasi-Experimental Designs, Modeling, Experimental Designs, Randomized Designs, Random Control Trials Designs)
- Meta-analysis (Type 1, Type 2)

Knowledge

- Nascent
- Developing
- Mature

When the condition of knowledge (about a specific phenomenon, in a topical area, for a discipline, or for society and science as a whole) is low (Nascent), the types of methods that are best used fall on the left side of the X-axis continuum. As the condition of knowledge develops, the best methods move toward the right side of the X-axis.

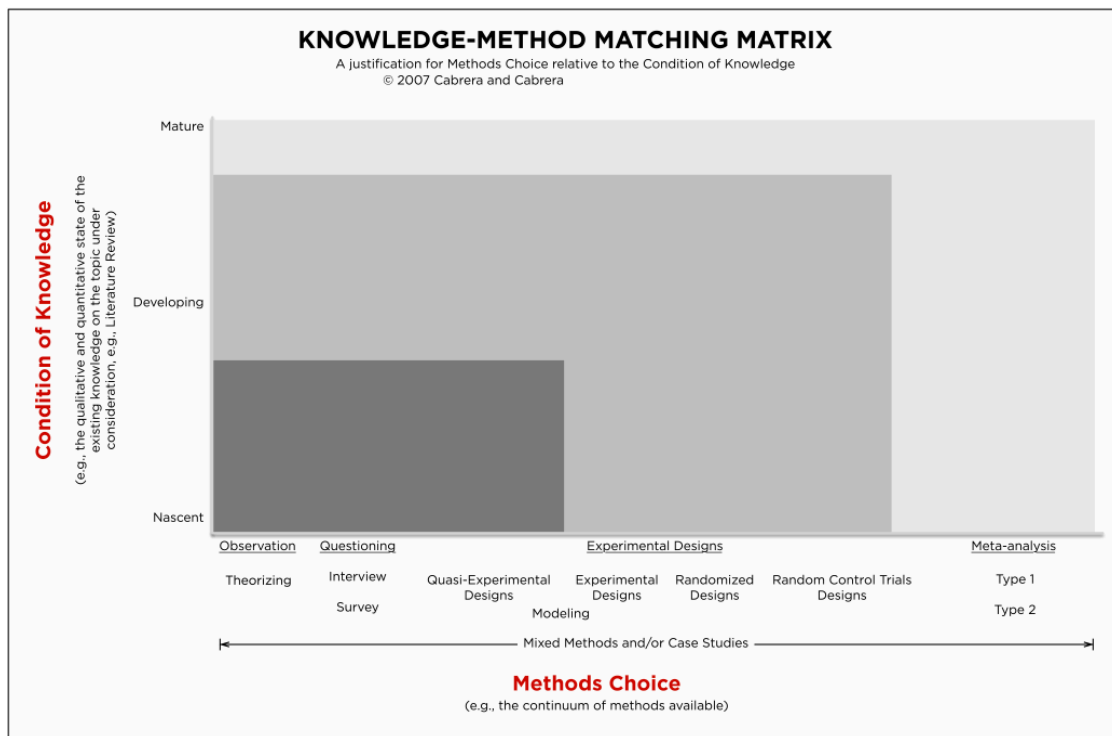


Figure 4- Knowledge Method Matching Matrix

Utilizing the K-MMM, each paper was classified according to the method employed and results are shown in Figure 5 below.

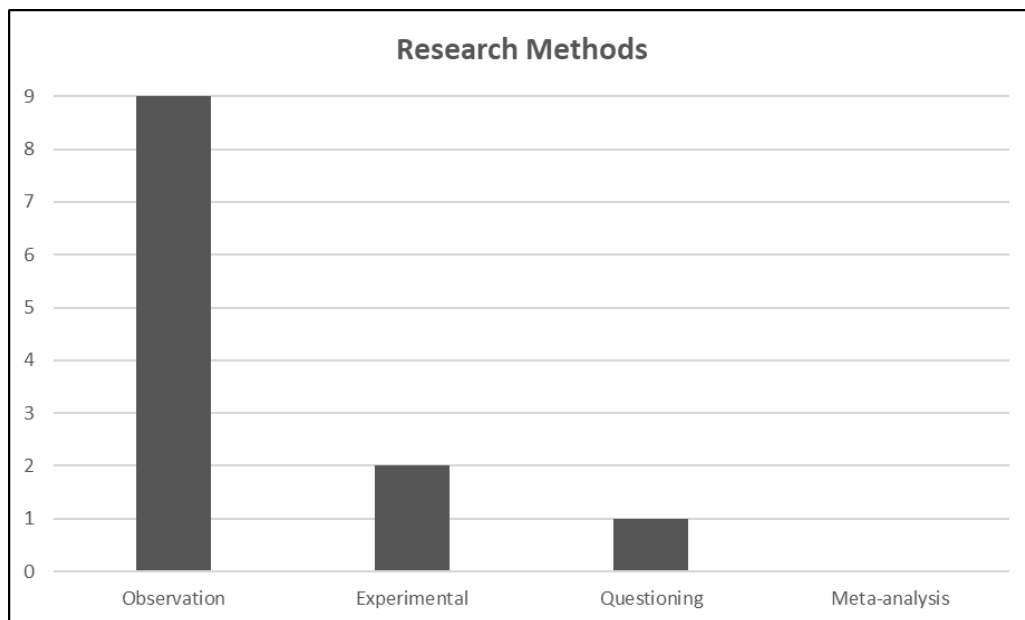


Figure 5- Research methods employed.

As can be seen, the predominance of observational methods in the reviewed papers suggests that the condition of knowledge regarding the application of systems thinking in cybersecurity is still at a nascent or developing stage. The limited use of experimental methods suggests a lack of mature knowledge that could provide a solid basis for hypothesis testing and controlled experiments.

As shown in Figure 6 a qualitative methodology was employed in all the selected literature using this study except for Zoto et al. [2], Matei & Bertino [13], and Vagle [9] where both qualitative and quantitative modeling methods were employed.

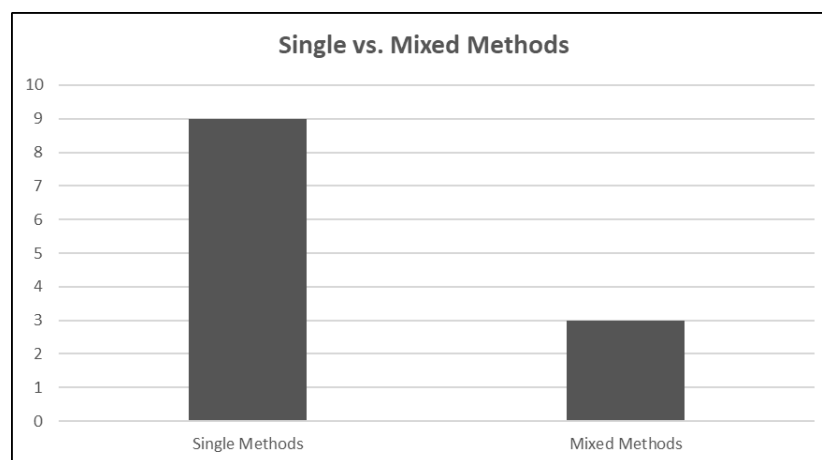


Figure 6- Single vs. Mixed Methods

Statistical Significance

Except for one study by Matei & Bertino [13] shown in Figure 7, the absence of statistical significance in the other evidence supports the idea that knowledge is still developing and lacks definitive conclusions. Therefore, the maturity of the knowledge in this context may be characterized by a need for further empirical validation and the development of more advanced research methods to progress towards a more mature and established state.

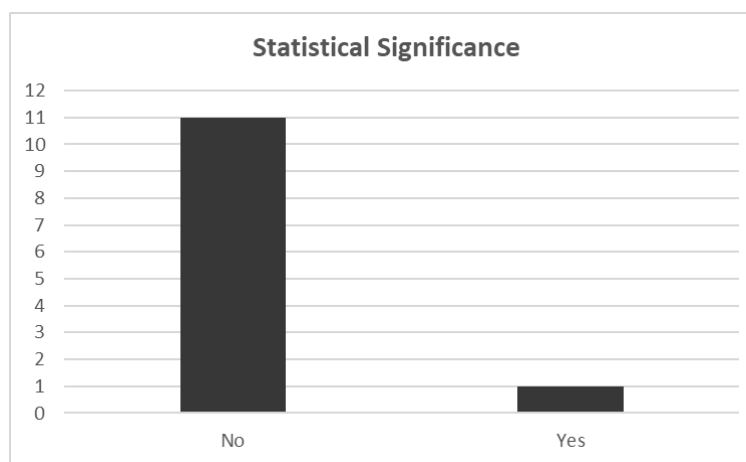


Figure 7- Statistical Significance

Furthermore, the scarcity of such methods in the reviewed literature suggests that the field is still grappling with defining the key variables and understanding their interplay. There is a clear need for more robust research to advance our understanding of this complex field.

To mature the condition of knowledge, researchers in this field should focus on:

- Developing clear and operational definitions of key concepts and variables.
- Conducting exploratory studies to identify potential causal relationships among key variables.
- Moving towards experimental methods as knowledge advances.
- Conducting meta-analyses to synthesize findings from multiple studies and draw more robust conclusions.

Vocabulary Synthesis

Despite its common usage, systems thinking is used in different disciplines to mean different things. The phrase "systems thinking" has shown substantial variability throughout the research, with each paper presenting a unique meaning, often based on the specific discipline of systems thinking that underpinned the approach. Although all the authors support the benefits of adopting a systems thinking approach to cybersecurity a precise definition has remained elusive. Much of the selected literature characterizes systems thinking as a lens through which to view a specific issue related to cybersecurity. As the challenges associated with the cybersecurity domain are highly interconnected and complex in nature, systems thinking is proposed as a perspective from which to better understand the whole rather than the parts within the whole. None of the studies carried out has genuinely investigated the theoretical basis of the cognitive process that leads to systems thinking. This gap is substantial if the field is to advance in its implementation of systems thinking.

Some examples of the definitions presented in the publications are as follows:

For Al Sabbagh & Kowalski [6] systems thinking means “a system of interrelated parts or subsystems that interact with each other and with their surrounding environment.” This definition is close to that of Yan [10] who defines systems thinking as an “holistic approach intended to analyze how the parts of the system interact and how the emergence changes as a whole entity”.

Chung [7] does not offer a precise definition of systems thinking, but instead proposes the adoption of a "systems perspective using a holistic approach" as a strategy. In contrast, Vagle [9] presents systems thinking as “a paradigm, a language, and a method”. According to Jaradat [12] “systems thinking is a framework of thought that helps in dealing with complexity in a holistic way.”

Given the varying interpretations of systems thinking among academics, it is crucial to establish a cohesive and universal definition of systems thinking to prevent further confusion and ensure the domain maintains a high level of construct validity.

This would not only benefit the scientific community in maturing the condition of knowledge but may also contribute to greater adoption of system thinking by cyber security practitioners.

The following section performs an examination of previous works cited in the selected literature to identify seminal papers in addition to any literature that reflects the historical background of the field of systems thinking. This is conducted to situate future research within the context of earlier work.

The present study employs a Citation Assisted Background (CAB) method to ascertain the seminal papers cited in the chosen papers. The CAB concept, developed by Kostoff & Shlesinger [15], is a widely employed technique for determining the most influential publications in a research field through a review of citations. The CAB methodology is based on the premise that a prominent work in a certain research field would generally be cited frequently by a significant proportion of current scholars in that field. Implementation of the CAB method is undertaken using the following steps:

- The research area of interest must be defined clearly.
- The documents that define the area of interest must be identified and retrieved.
- The references most frequently used in these documents are identified and selected.
- These critical references are analyzed and integrated in a cohesive manner to form a comprehensive view of historical context and seminal works.

The first and second steps of the CAB method were completed as part of the PRISMA process described earlier. The subsequent phase of the process entailed recording all the citations mentioned by the authors that were related to systems thinking. The citations extracted from the various papers were entered into Google Scholar and subsequently verified by using the title, author, and date as validation criteria. Subsequently, the citation statistic was obtained by using the value of the "cited by n..." reference, which denotes the frequency of citations recorded by the article.

Several discrepancies occurred when the citations provided by the authors did not yield any matching results in Google Scholar. Where available the URLs of the original file sources were examined to ascertain whether citation metrics were available in the original source file library. References that were not listed in English language were removed due to the author's inability to accurately translate or discover a match for them in Google Scholar.

Simple statistical analysis of the data² gathered using the CAB method was used to identify seminal works that served as the building blocks for the present-day condition of knowledge related to the application of systems thinking in cybersecurity. The material to be included was specifically selected by identifying the earliest publications or highly cited works, and publications regularly referenced. This selection aimed to locate seminal literature and authors within a historical context.

² Reference the Data Availability Section.

While Citation-Assisted Background is a highly systematic approach for identifying critical references, it is not a substitute for the judgment of the researchers, but rather complements their expertise.

The literature review indicates that systems thinking may be traced back to its origins in systems theory. Much of the selected literature explicitly cites system theories from the mid-1900s as influential publications that guided their research. Burrell et al. [3], Enright et al. [8], Vagle [9], Yan [10], Salim [11], and Jaradat [12] all cite the theory of System Dynamics as presented by Jay Forrester or Peter Senge. Another notable illustration is the Socio-technical Systems theory, as cited by Al Sabbagh & Kowalski [6], Chung [7], Shaked [4], Vagle [9], and Zoto et al. [2]. Renowned academics like Ludwig von Bertalanffy and his General Systems Theory, as acknowledged by Chung [7], Burrell et al. [3], Yan [10], Jaradat [12] and Checkland's Soft System Methodology, or its adaptations by Boardman and Sauser, are highlighted in the works of Al Sabbagh & Kowalski [6], Kawade & Yamamoto [15], and Jaradat [12].

It is noteworthy that certain studies, such as Enright et al. [8] and Burrell et al. [3] explicitly referenced Bertalanffy's General System Theory, but in other papers, such as Yan [10], the broader phrase "systems theory" was employed without further explanation. However, upon conducting additional research, the connection to the primary sources was established using secondary sources.

Figure 8 depicts the prevailing theories and academics that were cited in primary or secondary sources by the various authors.

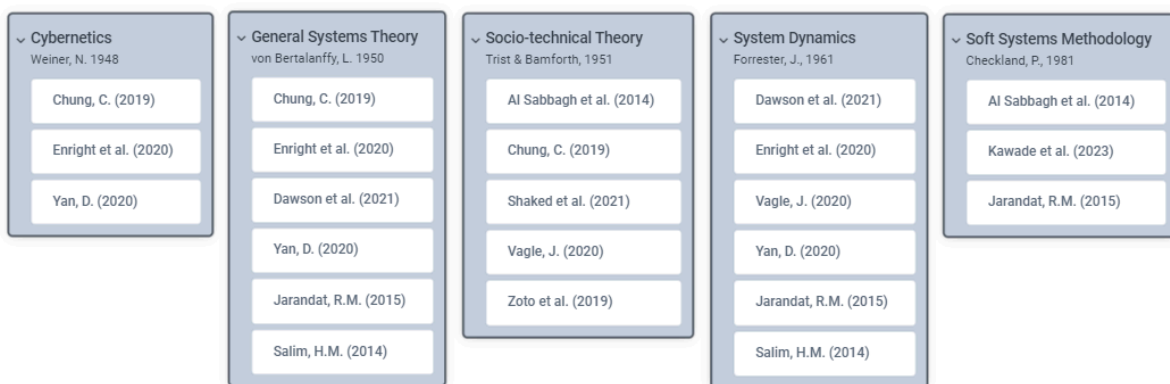


Figure 8- Seminal Theory and Scholars

This progression is consistent with the use of similar system thinking methodologies in sectors beyond cybersecurity, and the continued development of these techniques, as described in this research, correlates to the "Four Waves of Systems Thinking" as articulated by Cabrera, Cabrera, & Midgley [16].

Psychologist Kurt Lewin [17] is often quoted as saying “there is nothing as practical as a good theory”. The objective of this section is to evaluate the degree to which the selected literature was grounded in systems thinking theory and to analyze how this was demonstrated in the research.

Due to the preponderance of qualitative literature, it was determined that the most suitable approach for this enquiry would be to employ the QUANTUM typology, as outlined by Bradbury-Jones et al. [18], who propose it as a methodical way for identifying the consistent implementation of theory in qualitative research. The method seeks to critically evaluate the visibility and description of theory by asking two questions. Firstly, “How well are you able to see theory?” Secondly, “How do authors describe their use of theory?”

Table 7 displays the results derived by assessing each publication according to the criteria for each subject area, with the aim of determining the degree to which the literature answers the two questions. The results obtained from the QUANTUM typology indicate that the visibility and description of theory varied significantly among the evaluated literature.

By way of example Shaked et al. [4] refers to a “systems thinking” perspective without explicit reference to theorists in the field and with limited discussion describing their use of systems thinking theory in their work. Examining further secondary sources likewise proved unsuccessful in providing a clear and comprehensive description for systems thinking. The study may have been more valuable if the authors had provided explicit distinctions and cited the theoretical foundations of the terms “systems thinking”, “system of systems”, and “socio-technical systems” to aid in understanding the interaction between theory and method.

On the other hand, the papers authored by Al Sabbagh & Kowalski [6], Jaradat [12], and Salim [11] all provide a comprehensive and explicit explanation of the theoretical framework that supports the approach. The theory is consistently and clearly articulated throughout all aspects of the research process.

This Author contends that to increase the adoption of systems thinking among a broader audience, it is essential for scholars to build a direct link between the theory and its practical implementation. This will result in a deeper understanding of systems thinking among practitioners.

The literature presents a diverse range of industries where systems thinking in cybersecurity has been applied, as illustrated in Figure 9. It is reasonable to infer that in any organization where cybersecurity is important, the application of systems thinking to cybersecurity is as important. This presents a significant opportunity for advancing the application of systems thinking in this field, particularly considering the

substantial influence that cybersecurity threats are currently exerting on businesses, as indicated by all the authors.

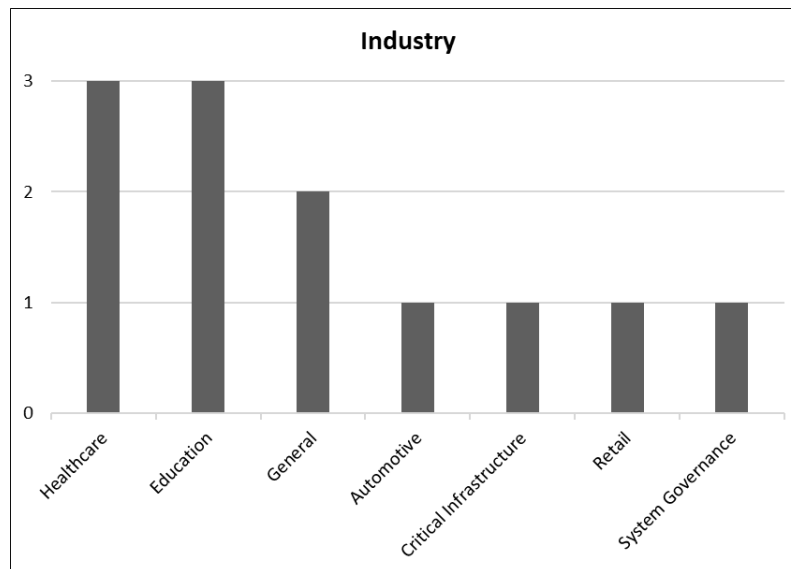


Figure 9- Industries Employed

Figure 10 displays various cybersecurity disciplines that were referenced in the research. A quarter of the papers were dedicated to exploring the integration of systems thinking in higher education. Zoto et al. [2] emphasize the significance of instructing students to consider systemic elements while contemplating cybersecurity and advocate for the use of simulations to effectively illustrate the value of this methodology. Enright et al. [8] argue that the implementation of a comprehensive framework for teaching systems thinking in cybersecurity programs and courses can effectively address the existing gaps within the academic system responsible for preparing the cybersecurity workforce. Furthermore, 25% of the papers examined the utilization of systems thinking to either analyze the causative elements behind cybersecurity issues or as a proactive approach to identify areas of concern and avoid incidents. The literature indicates that the term 'systems thinking' is commonly employed either as a general concept to represent a systemic approach to problem-solving, or in a more specific context where it is applied with a prescribed methodology to address domain-specific issues.

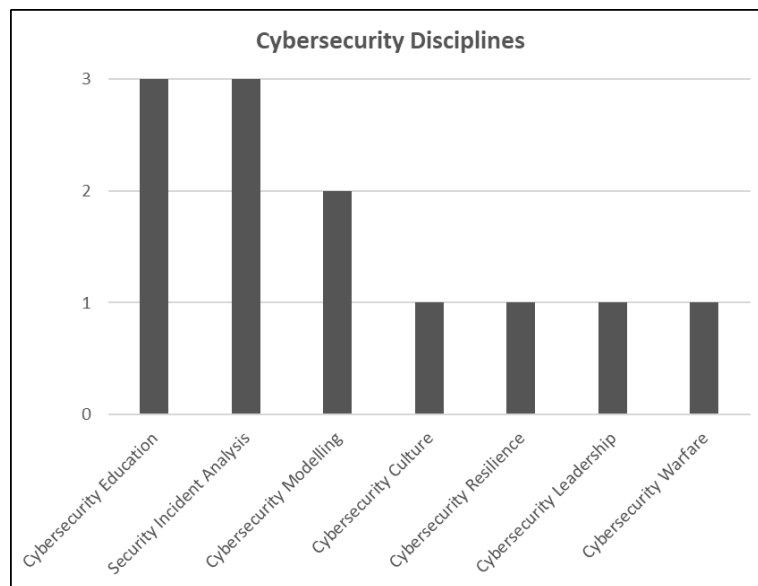


Figure 10 - Cybersecurity Disciplines

By way of illustration, Al Sabbagh & Kowalski [6] explain that, if a system thinker were to utilize the Soft System Methodology independently, they would need to possess a comprehensive understanding of information security management and the workings of attack techniques. Additionally, they note that the method is not technical in nature, but rather serves as a management tool.

The Author acknowledges the usefulness of custom developed tools for expert practitioners, but questions whether the complex nature of some of the techniques available to novice practitioners hinders the broader adoption of systems thinking within the cybersecurity community. This may also reinforce the argument that substantial theoretical foundations are necessary to provide a robust approach for practical implementation.

Public Search

To achieve a thorough examination of the research subject, the Author made the decision to incorporate a public search across websites and books. The benefit of this technique is its exploration of the collective knowledge of the public regarding the topic area. The public's comprehension of a scientific or research topic is crucial in determining the societal significance of the research according to Cabrera et al. [1].

Websites

Websites were located by a Google search using the previously specified search phrases as used in the Scholarly search. The selection of websites was based on their inclusion of the search terms and their relevance to the research questions. Search results were excluded where they contained academic research articles, PDFs, and books. Furthermore, the results were purged of advertisements, sponsored content, and training courses. Table 5¹ shows the results returned from the relevant search terms. A sample of the websites was then examined to assess the extent to which they demonstrated alignment with the research questions. The following content presents an examination of the selected websites.

The Medium article [20] "Systems Thinking Applied to Cybersecurity" authored by Aung (Steven) Thu Rha Hein provides an introductory exploration of systems thinking within the realm of cybersecurity. It highlights the significance of understanding the interconnections between system components and how they impact overall security and references scholarly works by Dingyu Yan. The article focuses on essential elements, influential aspects, and their interplay within the field of cybersecurity and highlights the System Dynamics concept of feedback loops inside the cybersecurity system to improve understanding of overall security. It also links to a Systems Engineering Body of Knowledge site which is funded by the International Council on Systems Engineering (INCOSE), the Institute of Electrical and Electronics Engineers Systems Council (IEEE-SYSC), and Stevens Institute of Technology and was established to provide a guide to the key knowledge sources and references of systems engineering. To make the existing knowledge more informative about systems thinking and relevant to general users, it should include practical examples of how systems thinking can be applied more broadly in the field, as well as the specific benefits and outcomes that can be achieved through its application. Additionally, providing clear explanations of key concepts and terminology would enhance understanding for general users.

The second website [21] studied discusses the application of systems thinking in the field of cybersecurity. The article highlights the teachings of W. Edwards Deming, a renowned expert in quality management, who advocated for a holistic approach to problem-solving. Deming's System of Profound Knowledge, comprising appreciation for a system, knowledge of variation, theory of knowledge, and psychology, is presented as a framework for understanding and addressing cybersecurity challenges. The article raises questions about the balance between technical training and understanding system dynamics in cybersecurity education. It also compares the root cause analysis methods used in cybersecurity with those in other disciplines. Overall, the article critiques the limited perspective of some cybersecurity

professionals who fail to recognize the complexity and interconnectedness of systems in the modern business landscape.

Phil Venables is a renowned cybersecurity expert who presently holds the position of Chief Information Security Officer (CISO) at Google. The central theme of the blog piece "Thoughts from the Field" [22] revolves around the systems concept. It emphasizes the significance of understanding that while simplicity at the component level is crucial, attempting to eliminate complexity at the systems level is often futile, and instead suggests developing techniques to manage and harness system-wide complexity. The website conveys the idea of complex systems and their unpredictable behavior by making references to various theories and laws related to systems. It draws upon literature in systems-thinking and control theory, such as John Gall's "*Systemantics. The Systems Bible*" to support its arguments. By highlighting the potential failures that can arise when simple systems are combined, the website underscores the need for a holistic approach to cybersecurity. Venables' prominent reputation in the domain of cybersecurity enhances the use of systems thinking in this subject, lending it greater legitimacy.

TechTarget [23] is a technology website that offers news commentary, tutorials, how-tos, tips, in-depth features, and vendor product comparisons. The author discusses the application of system of systems (SoS) in various domains such as business, education, government, healthcare, media, and transportation. It provides examples of SoS in these areas, such as banking systems, universities, and air traffic management. The author suggests that the design of system of systems necessitates the use of systems thinking, which is described as "a holistic approach to analysis that focuses on the way constituent parts interoperate, work over time, and function within the context of a larger, evolving system". The author might enhance the accessibility of the concepts by elaborating further on real-world scenarios, thus enabling people who are unfamiliar with the principles to comprehend the advantages of using this strategy more effectively.

In summary, it has been shown from this analysis that the state of knowledge in the public domain is in its early stages of development. Whilst the advantages of adopting a systems thinking approach are regularly mentioned, it is often without providing sufficient elaboration to convincingly advocate for its adoption by a wider audience. Several websites encounter similar problems as scholarly literature, in that they lack a clear and unified understanding of systems thinking.

Books

A search was performed on Google Books and results were evaluated based on the previously specified terms in the academic search. Only publications that had the search terms inside their text were

considered for the analysis. Books comprising academic papers presented at conferences or symposiums were excluded as they were considered within the scope of the scholarly search. The maximum number of results considered was limited to 100 to establish a threshold for evaluating the results. Results of the book search can be found in Table 6¹.

A sample of the books was then selected to assess the extent to which they demonstrated alignment with the research questions. The following content presents an examination of the selected books. In many respects the books reflect a similar approach as outlined in the previous search scopes. Authors like Lacey [24] advocate for the advantages of adopting a systematic and comprehensive approach to problem-solving to comprehend complex network architectures. According to Shoemaker et al. [25], they consider systems thinking a key concept in overall cybersecurity theory, and a component of a comprehensive cybersecurity framework that aids systems engineers in adopting a holistic approach. D'Anna & Collier [26] suggest that Senge's approach to systems thinking is essential for entrepreneurs and for tackling intricate global issues like cybersecurity. In his work, Furnell [27] explains the potential application of General Systems Theory and Soft Systems Methodology to enhance IT security by providing a more effective approach to safeguarding IT systems and applications. Troskie [28] compares and contrasts “Hard” and “Soft” systems approaches referencing Viable Systems Model, Soft System Methodology, Systems Dynamics and the Vanguard Method and how they might be applied to effectively manage cybersecurity using Environment, Social and Governance (ESG) frameworks.

Public Synthesis

The texts provide insights into the application of systems thinking in cybersecurity, which is an increasingly important area for public safety and economic stability. By promoting a holistic and interconnected view of the systemic factors that contribute to the present issues in cybersecurity, they enhance the public's understanding of the complexities involved in cybersecurity challenges. The texts indicate a maturing field of research that recognizes the limitations of traditional, reductionist or component-focused approaches to cybersecurity. They suggest that systems thinking is gaining traction as a necessary paradigm for addressing the complexity of modern cyber threats and underscore the potential for systems thinking to revolutionize cybersecurity strategies. By highlighting the interplay of various components, including human behavior and organizational collaboration, they advocate for a more integrated and adaptive approach to cybersecurity. The use of practical examples, case studies, and references to recognized authorities in the field like Deming and Venables contributes to a better public

understanding of systems thinking in cybersecurity. However, to further enhance public knowledge, the texts could include more accessible explanations of key concepts and terminology for general audiences. While the texts make significant strides in explaining systems thinking in cybersecurity, they may still be challenging for the layperson to fully grasp.

In summary, they make a strong case for the importance of systems thinking in cybersecurity. The societal impact is significant, as better-informed professionals and members of the public can lead to more resilient and effective cybersecurity practices. However, for these ideas to have the broadest impact, they should be presented in a manner that is accessible to a wider audience, ensuring that the value of systems thinking in cybersecurity is fully appreciated and implemented across society.

Conclusion

In conclusion, this Systems Literature Review sought to understand the condition of knowledge related to the application of systems thinking in cybersecurity, what theories, frameworks and methods are used in the field today and what specific scenarios it is being used in.

“You can know the name of a bird in all the languages of the world, but when you’re finished, you’ll know absolutely nothing whatever about the bird. So, let’s look at the bird and see what it’s doing – that’s what counts. I learned very early the difference between knowing the name of something and knowing something.”

– Richard P. Feynman [29]

In most of the literature analyzed for this study, the term systems thinking was used to describe thinking in a variety of ways. Furthermore, these studies often fail to provide a comprehensive definition of systems thinking, limiting their practicability, and there is a lack of empirical evidence to support their efficacy. Thinking systemically, holistically, and seeing interconnections are all synonyms for systems thinking, but they are not comprehensive. They are incomplete in the same way that expecting a medical doctor to think "medically" does not provide them with the abilities needed to undertake intricate heart surgery. In the same way that a medical student studies the core physiological structure of the body before understanding how to treat it, a cybersecurity practitioner should understand the basic tenets of system thinking before applying it to a broad range of scenarios.

Simply asking cybersecurity practitioners to "think" in a specific way does not mean that they will become "system thinkers". On the opposite end of the spectrum are numerous approaches designed for a specific use case, which some authors concede, requires a certain amount of cybersecurity experience to implement. So, does adhering to a specified methodology enhance the user's proficiency as a systems thinker, or would it be more preferable for the user to first acquire the skills of a proficient systems thinker before learning a specific methodology?

This Author believes that further research is needed to establish broad, practical applications of systems thinking in the cybersecurity domain that are based on strong empirical data, to provide the best opportunity for broad adoption.

And so, having arrived at the end of this research it appears inevitable that, in many ways, we must go back to the beginning and redefine what systems thinking in cybersecurity means to make it accessible to the broadest possible audience.

Data Availability Statement

The data that support the findings of this study are openly available in “STinCybersecurity_SLR” folder at <https://drive.google.com/drive/folders/1NlIP3vZ6nJZtBmMW0OENehntUYuagE-z?usp=sharing>

References

1. D. Cabrera, L. Cabrera, E. Cabrera, The Steps to Doing a Systems Literature Review (SLR). *Journal of Systems Thinking*, 6 April 2023.
2. Zoto, Erjon, Mazaher Kianpour, Stewart James Kowalski, and Edgar Alonso Lopez-Rojas. A Socio-Technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. *Complex Systems Informatics and Modeling Quarterly*, no. 18 (30 April 2019): 65–75.
3. Burrell, Darrell Norman, Amalisha Sabie Aridi, Quatavia McLester, Anton Shufutinsky, Calvin Nobles, Maurice Dawson, and S. Raschid Muller. ‘Exploring System Thinking Leadership Approaches to the Healthcare Cybersecurity Environment’. *International Journal of Extreme Automation and Connectivity in Healthcare* 3, no. 2 (July 2021): 20–32.
4. Shaked, Avi, Lior Tabansky, and Yoram Reich. ‘Incorporating Systems Thinking Into a Cyber Resilience Maturity Model’. *IEEE Engineering Management Review* 49, no. 2 (1 June 2021): 110–15.
5. K. Kawade, S. Yamamoto, A Method to Analyze Cyber Security Guideline using System Thinking, JSAI Technical Report, Type 2 SIG, 2023, Volume 2023, Issue KSN-033. https://doi.org/10.11517/jsaisigtwo.2023.KSN-033_05.
6. B. AlSabbagh & S.J. Kowalski, Security from a Systems Thinking Perspective - Applying Soft Systems Methodology to the Analysis of an Information Security Incident. Proceedings of the 58th Annual Meeting of the ISSS - 2014 United States, 1(1). Retrieved from <https://journals.iss.org/index.php/proceedings58th/article/view/2305>.
7. K. Chung, Applying Systems Thinking to Healthcare Data Cybersecurity. *Doctoral Dissertation*, 2015. <https://dspace.mit.edu/handle/1721.1/105307>.
8. E. Enright, C. Justice, S. M. Loo, E. Taylor, C. Sample, C. Shelton, Building Capacity for Systems Thinking in Higher Education Cybersecurity Programs. *Journal of The Colloquium for Information Systems Security Education* 8, no. 1 (2020).
9. J. Vagle, Investigating Business Alignment Issues Rooted in the Norwegian Specialist Health Services, Cybersecurity Culture, Through a Systems Thinking Approach. *Master's Thesis*, 2020. <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2781150>.

10. D. Yan, A Systems Thinking for Cybersecurity Modeling. 16 January 2020. [Preprint]
<https://doi.org/10.48550/arXiv.2001.05734>.
11. H. Salim, Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks. *Masters Thesis*, 16 May 2014.
12. R. Jaradat, Complex System Governance Requires Systems Thinking - How to Find Systems Thinkers'. *International Journal of System of Systems Engineering* 6, no. 1/2 (2015): 53.
13. S. Matei, E. Bertino, Educating for AI Cybersecurity Work and Research: Ethics, Systems Thinking, and Communication Requirements. [Preprint] arXiv:2311.04326., 7 November 2023.
14. D. Cabrera, L. Cabrera, The Knowledge-Method Matching Matrix (KMMM). *Journal of Applied Systems Thinking* 20, no. 5 (23 June 2021): 1–3.
15. R. N. Kostoff, M. F. Shlesinger. 'CAB: Citation-Assisted Background'. *Scientometrics* 62, no. 2 (January 2005): 199–212.
16. D. Cabrera, L. Cabrera, E. Cabrera. The Steps to Doing a Systems Literature Review (SLR). *Journal of Systems Thinking Preprints*. 2023. DOI: 10.54120/jost.pr000019.v1
17. K. Lewin, The Research Center for Group Dynamics at Massachusetts Institute of Technology. *Sociometry* 8, no. 2 (May 1945): 126.
18. C. Bradbury-Jones, O. R. Herber, R. Miller, J. Taylor, Improving the Visibility and Description of Theory in Qualitative Research: The QUANTUM Typology. *SSM - Qualitative Research in Health* 2 (December 2022): 100030.
19. D. Cabrera, L. Cabrera, G. Midgley. The Four Waves of Systems Thinking. *Systems Thinking*. 2023. Vol. 3:1-51. DOI: 10.54120/jost.000051
20. U. Rōnin, Systems Thinking Applied to Cybersecurity - Unrivaled Rōnin - Medium. (2023). Available: <https://atrhein.medium.com/systems-thinking-applied-to-cybersecurity-b69e2a12643a>. Accessed 20 January 2024.
21. Deming Systems Thinking and Cyberwarfare - The W. Edwards Deming Institute. Available: <https://deming.org/deming-systems-thinking-and-cyberwarfare/>. Accessed 20 January 2024.
22. P. Venables, Handling Complexity. Risk and Cyber, Thoughts From the Field (2023). Available: <https://www.philvenables.com/post/handling-complexity>. Accessed 21 January 2024.
23. A. S. Gillis, system of systems (SoS). App Architecture (2022). Available: <https://www.techtarget.com/searchapparchitecture/definition/system-of-systems-SoS>. Accessed 27 January 2024.

24. D. Lacey, Managing the Human Factor in Information Security. John Wiley & Sons, 2011.
25. D. Shoemaker, A. Kohnke, K. Sigler, The Cybersecurity Body of Knowledge. CRC Press, 2020.
26. G. D'Anna, Z. A. Collier, Cybersecurity for entrepreneurs. SAE International, 2023.
27. S. Furnell, Securing Information and Communications Systems. Artech House, 2008.
28. H. J. Troskie, The 4Th Competitive Force for Good. Partridge Publishing Singapore, 2020.
29. R. P. Feynman, What Do You Care What Other People Think? Penguin UK, 2007.