Journal of Systemics, Cybernetics and Informatics (2024) 22(1), 150-164
https://doi.org/10.54808/JSCI.22.01.150

The Importance of Defining Cybersecurity from a Transdisciplinary Approach

Bilquis Ferdousi

*School of Information Security and Applied Computing
College of Engineering & Technology
Eastern Michigan University*

bferdous@emich.edu

Abstract[1]

This paper presents a transdisciplinary approach to define the field of cybersecurity. The main purpose of this study is to enhance the understanding of the impact of cybersecurity in different aspects of life, improving the interdisciplinary and multidisciplinary relation focusing on the impact of cybersecurity on other disciplines. The more specific purpose is to determine how cybersecurity professionals, including academics and researchers, can *better approach cybersecurity as a transdisciplinary field to ensure data security and privacy. The paper focuses on how cybersecurity affects the different aspects of society, such as legal systems, online business and services, etc., on personal and organizational levels. Additionally, it focuses on how trans-disciplinarity involves academic researchers from different, unrelated academic disciplines as well as non-academic stakeholders or end-users to create new knowledge. Based on the extensive literature review on multidisciplinarity, interdisciplinarity, and transdisciplinarity research in cybersecurity, this study found that a transdisciplinary approach is needed to ensure cybersecurity in organizational and individual level. For that purpose, the academics, researchers, and practitioners from different disciplines must engage with their content extending beyond their traditional academic boundaries and reaching out to non-academic stakeholders or end-users of digital technology.*

Keywords: *Cybersecurity, Privacy, Transdisciplinarity, Interdisciplinary, Multidisciplinary.*

1. Introduction

As organizations increasingly become dependent on digital technology, they are required to address the cybersecurity risks associated with the technology used

[1] Rachel Dick, Lecturer and Writing Consultant, Eastern Michigan University, is the peer-editor who proofread and edited the final version of the paper

by the growing number of people. The cybersecurity risks focus on the threat to people’s data security and privacy when they use digital technology. To reduce these risks and ensure cybersecurity, Information Technology (IT) management often rely on technology-based solutions. Although the technical solutions help improve cybersecurity, relying on them exclusively is not practical enough to eliminate these cybersecurity risks. Empirical and anecdotal evidence suggest that success in safeguarding cybersecurity can be achieved only when efforts invest from both technical and socio-organizational perspectives.

Cybersecurity is traditionally a track or subset of Information Technology (IT) or Computer Science. However, cybersecurity as a field is comprised of different disciplines. One of the main challenges in the cybersecurity field is its interdisciplinary nature that involves fields of computer, technology, engineering, law, business and social sciences in the academic world (Omar et al., 2020). Consequently, it is basically almost impossible in real life to mitigate threats to cybersecurity and defend against cyber-attacks without coordinated efforts from qualified teams with skills in all the aforementioned disciplines. More specifically, the transdisciplinary approach, which requires inclusion of non-academic stakeholders in the process of comprehension, understanding and awareness, is vital in this process.

1.1. Significance of the Study

As organizations and a growing number of people are using digital technology and are reliant on the internet for business, education, services, entertainment, etc., the risk in cybersecurity has become a major issue. The threat to cybersecurity is a major challenge for many organizations because this may have dire consequences including organizational accountability, loss of credibility, reputational and financial damage, etc. Similarly, any threat to cybersecurity may breach people’s privacy and endanger their data security. For that reason, ensuring cybersecurity has become one of the top priorities in many organizations. The advancement of Internet of Things (IoT) in the IT domain has created more serious challenges to cybersecurity that cost millions globally.

While the IoT with its many useful features provides many innovative, productive, and efficient services to people's everyday lives, the IoT can also cause serious threats to people's privacy and data security. In this context, the demand for qualified cybersecurity professionals, academic and non-academic, is continuously increasing at an unprecedented rate (Omar et al., 2020).

1.2. Goal of the Study

This study focuses on the transdisciplinary approach of cybersecurity that will contribute to the direction, content and methods involved in the growth and development of cybersecurity education and training for non-academic stakeholders or end-users. The study also recognizes the impact of other disciplines on the field of cybersecurity discussing relevant literature that contributes to understanding cybersecurity from the legal, business, engineering, criminology, and socio-psychological perspectives in addition to technology.

2. Define Cybersecurity

Cybersecurity is "The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (National Security Presidential Directive-54, 2008, p. 3). As people are living in an increasingly digital world, the ever-advancing cutting-edge pervasive computing technology has made people's privacy and data security risk a serious concern.

2.1. Cybersecurity vs. Privacy

Privacy is people's right, acting on their own behalf, to determine the degree to which they will interact with their environment, including the degree to which they are willing to share their personal information with others (Youm, 2017).

Cybersecurity is usually defined as the composite of three attributes: Confidentiality, Integrity, and Availability (CIA) of data. These core principles of cybersecurity are complemented with further attributes such as reliability, safety, and maintainability when combining security with dependability of data (Ferdousi, 2020). There are some overlapping or common areas between cybersecurity risks and privacy risks as shown in Figure 1.

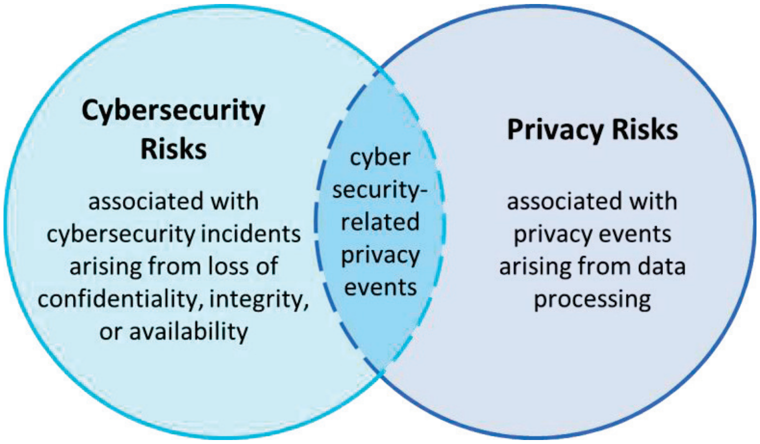
Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Figure 1: Cybersecurity and Privacy Risk Relationship (Source: Boeckl et al., 2021).

2.2. Threat to Cybersecurity in Internet of Things (IoT)

The advanced technology Internet of Things (IoT) incorporates a large set of people’s everyday life, such as healthcare, business, navigation, communications, transportations, etc. With more and more people taking advantages of the services of IoT, because of its efficiency and conveniences, the threat to cybersecurity related to these services are becoming a greater concern (Sharma et al., 2020). Since the IoT devices are increasingly used by people as well as different sectors of businesses and organizations, it is causing a larger number of security challenges (Razzaq et. al., 2017).

In today’s digital world, IoT covers almost every area of peoples’ lives such as home, automation, manufacturing, transportation, health care, infrastructure, etc.

One of the sectors that popularly uses IoT applications is home automation that processes home appliances such as washing machines, thermostats, garage doors, lighting, microwaves, refrigerators, etc. Another important sector is transportation where IoT technology was first used by integrating light sensors, GPS and GSM in automobiles. Sensors in the vehicles can be used to avoid collisions, for traffic management, and to provide space for parking. Another promising sector that is increasingly using IoT is health care. In health care systems, the IoT applications may store and process patients' sensitive health records. Patients' medical records can be transmitted from smart devices to a cloud computing platform to be stored and analyzed (Husamuddin & Qayyum, 2017). The threat to data security could be a serious issue in those health care systems. Whether or not those sensitive data is securely stored in smart medical devices and transmitted over the network following privacy and security acts, such as the government-regulated Health Insurance Portability and Accountability Act (HIPAA), could be a serious concern (Razzaq et. al., 2017).

3. The Continuum of Disciplinarity, Interdisciplinarity, Multidisciplinary, and Trandisciplinarity

The continuum of disciplinarity, interdisciplinarity, multidisciplinary, and transdisciplinarity can be discussed as follow:

Disciplinarity - Disciplines are detailed knowledge areas with distinct boundaries with common research objects, questions, methodological tools and exemplary cases (Japee, 2020).

Multidisciplinary - Consists of two or more different disciplines in which researchers from those disciplines work together on a common problem, but without altering their own disciplinary approaches or developing a common conceptual framework (Uwizeyimana & Basheka, 2017). Thus, a multidisciplinary task or project requires cooperation and skills from specialists who belong to different disciplines.

***Interdisciplinarity* -** Focuses on sharing the relationship between two or more disciplines that have a degree of common context. These disciplines integrate insights, information, and perspectives from more than one disciplinary standpoint (Sulyman, 2021). Thus, interdisciplinarity refers to analysis, synthesis, and harmonization of relations between disciplines, and finally into a coordinated and coherent whole (Fawcett, 2013). To create new knowledge, interdisciplinarity draws information, ideas, and methods from other disciplines. For that purpose, interdisciplinarity opens up new sources, interfaces, and methodologies beyond those found in a single discipline (Sulyman, 2021). For example, Human-Computer Interaction is an interdisciplinary field that uses diverse methods and practices from the fields of Computer Science, Psychology, Sociology, Anthropology, and Design and Arts. One of the basic foundations of Human-Computer Interaction, which has a cross-disciplinary nature, is *Principles* that represent intellectual theories, models and empirical research from different disciplines (Dix, 2017).

Transdisciplinarity - Transdisciplinarity refers to the integration of natural, social, and health sciences, and technology disciplines transcending each of their traditional boundaries (Fawcett, 2013). Transdisciplinarity is a holistic vision with a particular method, concept or theory; a general attitude of openness and aptitude for collaboration; and an essential strategy for solving complex problems. Thus, Transdisciplinarity is a specific form of interdisciplinarity in which boundaries between and beyond disciplines are transcended, and different scientific as well as non-scientific disciplines are integrated with their own knowledge and perspectives (Japee, 2020). Defining the content area of Trans-disciplinarity from an education research perspective, Radakovic et al. (2022) defined four features of trans-disciplinarity: 1) *Traversing* - crossing disciplinary boundaries, 2) *Transcending* - moving beyond disciplinary paradigms, 3) *Transforming* - focusing on socially relevant issues and common good, and 4) *Transgressing* - an openness to defy, question, and transform the established disciplinary boundaries and structures (Radakovic et al, 2022).

Consequently, the Trans-disciplinarity is a product of an evaluation process of knowledge that includes the development of content, methods and techniques. In this evolution process, Disciplinarity goes through Multidisiciplinarity on the way to Interdisciplinarity, which next reaches to Trans-disciplinarity (Japee, 2020).

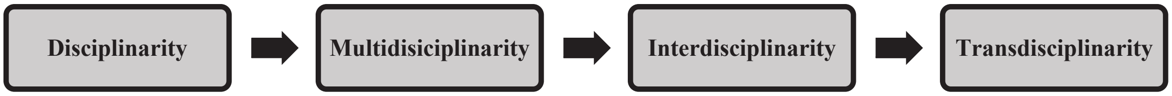

Figure 2: The Evolution of Transdisciplinarity.

The origin of the Transdisciplinarity concept is attributed to Jean Piaget, who in the early 1970s stated that “the maturation of general structures and fundamental patterns of thought across fields would lead to a general theory of systems or structures” (Klein, 2004, p. 515). Another pioneer of this concept, Erich Jantsch, defined Trans-disciplinarity as “the coordination of all disciplines and inter-disciplines in the education innovation system on the basis of a generalized axiomatic and an emerging epistemological pattern” (Jantsch, 1972, p. 106). Building off of Piaget’s structural approach, the terms multidisciplinarity, interdisciplinarity, and transdisciplinarity were created and have been debated since then (Budwig & Alexander, 2020). All Trans-disciplinarity involves interdisciplinarity, but the number of disciplines involved and the differences among them will vary with the problem being addressed. In general, the more dissimilar the disciplines, the more difficult it will be to effectively integrate them (OECD, 2020).

4. The Significant Necessity of Transdisciplinarity

Although theoretically the importance of a multidisciplinary or interdisciplinary approach has been recognized, practically it is still very difficult to transcend the borders of different disciplines (Koizumi, 2000). For example, Science, Technology, Engineering, and Math (STEM) emphasis on interdisciplinarity that integrates pedagogy of these distinctive disciplines to make curriculums more complex nature to create learning activities more engaging, authentic, and equitable. However, this interdisciplinary integration could be superficial because interdisciplinarity lets academics and researchers observe, analyze, and evaluate different ways to connect to different disciplines; whereas, trandisciplinarity focuses on construction of knowledge in a more real-world context where disciplines intersect, combine, and work together blurring their own boundaries (Radakovic et al., 2022) reaching out to non-academic stakeholders.

For instance, Human-Computer Interaction is a problem-solving field that strongly emphasizes constructive solutions to problems addressing challenges created by computer systems and people's interactions with different computer systems in diverse social and psychological contexts (Pargman et al., 2019). Human-Computer Interaction stresses on the fact that people's interaction with any electronic device or computing systems such as desktop, laptop, tablet, smartphone, smartwatch, ATM, Kiosk in airports, etc. is the connection between the end-user (human) and the computer device or application (technology). Therefore, Human-Computer Interaction is a discipline that emphasizes the design and usage of computer technology, focusing on the interaction between people and computers to guide how to design, evaluate, and implement interactive computer systems interfaces that satisfy the end-users (Shneiderman et al., 2017).

As Koizumi (2000) stated, in the ancient Greece, disciplines or fields of knowledge were not so strictly categorized with specific boundaries, and the scholars of that age studied various fields of thought to advance the knowledges. For example, the Pythagorean philosophers during that time studied mathematics, along with philosophy, music, and religion simultaneously to achieve new knowledge (Koizumi, 2000).

5. Trandisciplinarity in Research

In transdisciplinary research, widely differing forms of knowledge from different disciplines are integrated to construct a whole knowledge (Japee, 2020). The Trans-disciplinarity concept proposes a distinctive way of thinking about and engaging with scientific investigation by transcending disciplinary boundaries to illuminate the entanglements of real-world challenges. Consequently, a transdisciplinary approach allows researchers to step out of their disciplinary boundary, removing disciplinary barriers, although they may start their research investigation from a certain disciplinary viewpoint or perspective. The Trans-disciplinarity approach of scientific inquiry encourages researchers reaching out beyond the academic disciplines to weave together seemingly unrelated foundations of knowledge, skills, and experiences (Woods et al., 2021).

The interdisciplinary or multidisciplinary research are not robust enough to overcome the boundary between disciplines; consequently, they have been often based upon only a bundle of closely, or sometimes not so closely, related disciplines. The new breakthroughs in knowledge and research findings are often accomplished only by bridging the gap between completely different disciplines such as technology, math, psychology, philosophy, etc. (Koizumi, 2000). For example, the field of Human-Computer Interaction contributes to the knowledge about designing usable and user-friendly interfaces of computer technology, considering the effects of human, social, and technical factors (Clemmensen, 2019). Derived from the fields of Computer Science, Psychology, Sociology, and Design and Art, Human-Computer Interaction focuses on making connections among people, society, and technology. Therefore, the interdisciplinary research in this field can open transdisciplinary communications between authors and readers.

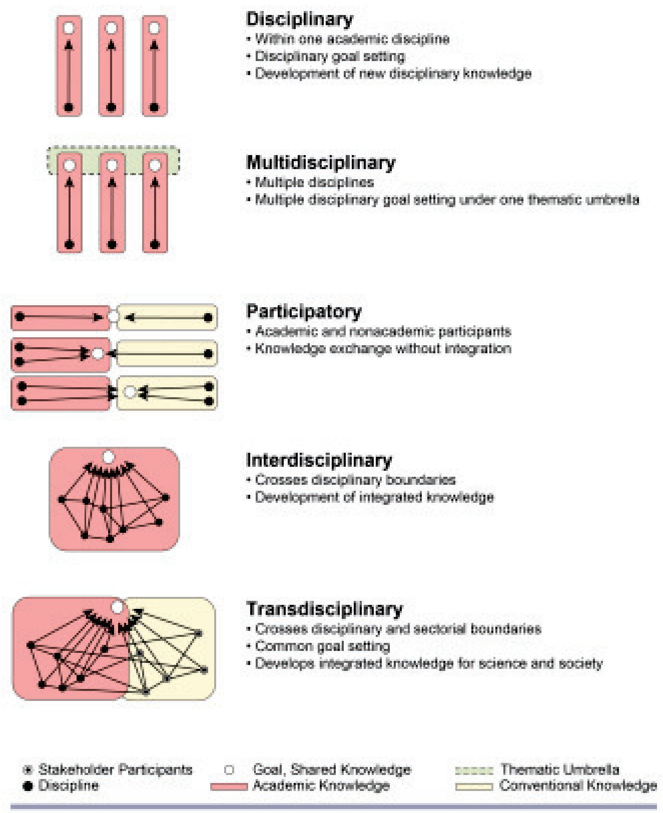
Disciplinary
• Within one academic discipline
• Disciplinary goal setting
• Development of new disciplinary knowledge
Multidisciplinary
• Multiple disciplines
• Multiple disciplinary goal setting under one thematic umbrella
Participatory
• Academic and nonacademic participants
• Knowledge exchange without integration
Interdisciplinary
• Crosses disciplinary boundaries
• Development of integrated knowledge
Transdisciplinary
• Crosses disciplinary and sectorial boundaries
• Common goal setting
• Develops integrated knowledge for science and society
Stakeholder Participants
Discipline
Goal, Shared Knowledge
Academic Knowledge
Thematic Umbrella
Conventional Knowledge

Figure 3. Graphical Representation of Transdisciplinary research (Source: Morton et al. 2015).

The collaboration among different dissimilar disciplines can enhance transdisciplinarity by successfully reaching out to the different audiences. For instance, although fields such as engineering, science, and technology are from disciplines different than the discipline of journalism, the academics and researchers from all these fields can collaborate on the *content* and *form*. In all these dissimilar disciplines, there is always a need to apply their professional expertise and knowledge in various contexts and to communicate with different audiences in the population. The engineers, technologists, and scientists may write research papers, patent abstracts, executive summaries, etc. based on their empirical research. While journalists can interview the engineers, scientists, and technologists on their innovation-based research, and then disseminate that valuable information and knowledge among the wider general population via journalistic articles, press releases, editorials, etc. (Breeze & Guinda, 2017). This type of collaboration among different disparate disciplines shows the importance of trans-disciplinarity.

6. Cybersecurity and Transdisciplinarity

The rapid advancement of IoT has led to an increase in cybercrime and a growing concern for cybersecurity and privacy. The cybersecurity concern involves many important and complicated societal, psychological, and practical factors that cannot be addressed only from the technological perspectives. For example, the field of Human-Computer Interaction plays a vital role in the cybersecurity issues, including many social or cultural challenges that involves humans with unpredictable outcomes. Humans or the end-users are regarded as the weakest link in cybersecurity because although computer security technologies such as anti-virus software, role-based access control, password settings, secure interface design, etc. are the first line of defense to ensure cybersecurity, the success in this regard depends on people's or end-users' online behavior or actions (Zhang-Kennedy et al., 2016). The usual computer technology-based problem-solving techniques alone cannot address the threat to cybersecurity.

As the focus on cybersecurity shifts toward people and organizational perspectives, cybersecurity policies and people's compliance with cybersecurity policies has emerged as a key socio-organizational resource in cybersecurity. Therefore, a robust cybersecurity policy is needed to address the security and privacy challenges (Bada & Nurse, 2019). However, merely having cybersecurity policies with guidelines concerning how to ensure cybersecurity is not enough. Although having the guidelines and policies is an essential starting point, it is not enough to ensure people's compliance with them. The limited awareness or unawareness of cybersecurity risks among end-users allow hackers to exploit the vulnerabilities of technology as well as users. Often there is a significant lack of user-understanding of cybersecurity procedures, which leads to exploited users, causing threats to cybersecurity (Sharma et al., 2020). Therefore, user awareness of cybersecurity is vital to address these threats.

Consequently, the threat to cybersecurity in the real-world needs to be addressed from a transdisciplinary perspective. Cybersecurity can be ensured through technology, policy compliance, and human factors. A transdisciplinary approach to understanding what psychological and social factors affect people's compliance with cybersecurity policies is vital in providing them with ways to solve the behavioral issues affecting the cybersecurity. An integrated approach to the training of cybersecurity awareness among end-users, developing a robust cybersecurity policy, ensuring users' compliance with policy, and improving the security and usability of secure computer technologies is more likely to produce a holistic solution in this regard. For that purpose, the academics, researchers, and practitioners from different disciplines such as computer science, information technology, engineering, business, law, health science, psychology, sociology, criminology, liberal arts, etc. need to engage with their content extending beyond their traditional academic boundaries and reaching out to non-academic stakeholders or end-users of digital technology.

7. Conclusions

The increased usage of digital technologies makes organizations as well as people or end-users vulnerable to various cyber-attacks, threatening the integrity of data at organizational, business, consumer or personal levels. Frequent cyber-attacks cost individual users, businesses, organizations, and other infrastructural entities highly (Jacob, 2020). A transdisciplinary approach is increasingly mentioned as an effective way to enhance knowledge and make the right decisions in this regard. With ever advancing digital technology, the pedagogy, literacy, and learning delivery modes have changed. This advancement is consistent with transdisciplinarity as artificially imposed disciplinary boundaries often create barriers in integration of knowledge and causes fragmentation in understanding (Radakovic et al., 2022). Along with computer security technology, increasing cybersecurity awareness among end-users enables them to make informed decisions and encourages compliance with security policies and advice provided by experts (Zhang-Kennedy et al., 2016). Therefore, ensuring cybersecurity only can be achieved when efforts invest from both technical and socio-organizational perspectives, exceeding academics and researchers' disciplinary boundaries and including end-users.

8. Acknowledgement

a. I would like to express sincere thanks to Rachel Dick, Lecturer and Writing Consultant, Eastern Michigan University, for proofreading and editing the final version of the paper as peer-editor.

b. I would like to express special thanks to Jamal Bari, Professor, School of Engineering, Eastern Michigan University, for reading this paper as a non-anonymous peer reviewer from the perspective of a different discipline.

References

Archibald, M. M., Lawless, T. M., Plaza, P. A. M., & Kitson, L., A. (2023). How transdisciplinary research teams learn to do knowledge translation (KT), and how KT in turn impacts transdisciplinary research: A realist evaluation and longitudinal case study. *Health Research Policy and Systems, 21*(20). 1-24. https://doi.org/10.1186/s12961-023-00967-x.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Boeckl, K., Grayson, N., Howell, G., Lefkovitz, N., Ajmo, J. G., McGinnis, M., Sandlin, K. F., Slivina, O., Snyder, J., & Ward, P. (2020). *Mobile device security: Bring Your Own Device (BYOD)* NIST SPECIAL PUBLICATION 1800-22). U.S. Department of Commerce, National Institute of Standard and Technology. ,

Breeze, R., & Guinda, S. C. (2017). Genre-based strategies for integrating critical and creative thinking in Engineering and Journalism. ESP Today, 5(2), 196–221. https://doi.org/10.18485/esptoday.2017.5.2.4

Budwig, N., & Alexander, J. A. (2020). A transdisciplinary approach to student learning and development in university settings. *Frontiers in Psychology, 11, 1-13*. https://doi.org/10.3389/fpsyg.2020.576250

Clemmensen, T., Rajanen, D., Rajanen, M., & Abdelnour-Nocera, J. (2019). Introduction to the special issue on human-computer interaction in a sharing society. AIS Transactions on human-computer interaction, 11(3), 107-116. https://doi.org/10.17705/1thci.00115

Clemmensen, T., Rajanen, D., Rajanen, M., & Abdelnour-Nocera, J. (2019). Introduction to the special issue on HCI in a sharing society. *AIS Transactions on Human-Computer Interaction, 11*(3), 107-116. https://doi.org/10.17705/1thci.00115
DOI: 10.17705/1thci.00115

Dix, A. (2017). Human-computer interaction, foundations and new paradigms. *Journal of Visual Languages and Computing, 42*, 122-134. https://doi.org/10.1016/j.jvlc.2016.04.001

Fawcett, J. (2013). Thoughts about multidisciplinary, interdisciplinary, and transdisciplinary research. *Nursing Science Quarterly 26*(4) , 376–379. https://doi.org/10.1177/0894318413500408

Ferdousi, B. (2020). Privacy issue in the Internet of Things: Security threats and challenges. *Proceedings of the 60th International Association for Computer Information Systems (IACIS)Conference*, 1-7.*https://iacis.org/conference/proceedings/IACIS_2020_Proceedings*

Hesjedal, B. M., & Heidrun, A. (2023). Making sense of Trans-disciplinarity: Interpreting science policy in a biotechnology centre. *Science and Public Policy, 50,* 219–229. https://doi.org/10.1093/scipol/scac055

Husamuddin, M., & Qayyum, M. (2017). Internet of Things: A study on security and privacy threats. The 2nd International Conference on Anti-Cyber Crimes (ICACC), IEEE, 11-6. https://doi.org/10.1109/Anti-Cybercrime.2017.7905270

Klein, J. T. (2004). Prospects for transdisciplinarity. Futures, 36(4), 515-526.https://doi.org/10.1016/j.futures.2003.10.007

Koizumi, H. (2000). Search for foundations of science & technology in the 21st century. *The Transdisciplinary Symposium on the Frontier of Mind-Brain Science and Its Practical Applications (II)*. Hitachi, Ltd, Tokyo.

Jacob, J., Peters, M., & Yong A. T. (2020). Interdisciplinary cybersecurity: Rethinking the approach and the process. *National Cyber Summit (NCS) Research Track,* . 61–74. https://doi.org/10.1007/978-3-030-31239-8_6

Japee, P. G. (2020). Transdisciplinary research - A paradigm shift in research ecosystem. *Journal of Xi'an Shiyou University, Natural Science Edition, 16*(8), 78-91. ISSN: 1673-064X.

Jantsch, E. (1972). *Interdisciplinarity: Problems of Teaching and Research in Universities*. Paris: OECD.

Omar, T., Amamra, A., Rigden, K., & Ketseoglou, T. (2020). Interdisciplinary cybersecurity projects experience: Developing a market ready workforce. American Society for Engineering Education, June 22-26, 2020. https://peer.asee.org/34861

Morton, L. W., Eigenbrode, S. D., & Martin, T. A. (2015). Architectures of adaptive integration in large collaborative projects. *Ecology and Society*, *20*(4). http://www.jstor.org/stable/26270306

National Security Presidential Directive (NSPD)-54, (January 8, 2008). Cybersecurity Policy, *Homeland Security Presidential Dir-23*. https://irp.fas.org/offdocs/nspd/index.html.

OECD. (June 2020). OECD Science, Technology, and Industry Policy Papers. Addressing societal challenges using transdisciplinary research, *OECD Science, Technology, and Industry Policy Papers*, *88.* OECD Publishing.

Pargman, S. D., Eriksson, E., Bates, O., Kirman, B., Comber, R., Hedman, A., & Broeck, M. (2019). The future of computing and wisdom: Insights from human - computer interaction. *Futures, 113*. https://doi.org/10.1016/j.futures.2019.06.006

Radakovic, N., W. O'Byrne, I., Negreiros, M., Hunter-Doniger, T., Pears, E., & Littlejohn, C. (2022). Toward trans-disciplinarity: Constructing meaning where disciplines intersect, combine, and shift. *Literacy Research: Theory, Method, and Practice, 71(*1), 398-417. https://doi.org/10.1177/23813377221113515

Razzaq, M. R., Qureshi, A. M., Gill, H. S., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6), 383-388. https://doi.org/10.14569/IJACSA.2017.080650

Sharma et al.: Security, privacy and trust for smart mobile-internet of things (m-iot): a survey, special section on internet-of-things attacks and defenses: recent advances and challenges. *IEEE Access, 8, 167123-167163.* https://doi.org/10.1109/ACCESS.2020.3022661

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2017). *Designing the user interface - strategies for effective human-computer interaction* 6th Ed.. Pearson.

Strand, M., Ortega-Cisneros, K., Niner, J. H., Wahome, M., Bell, J., Currie, C. J., Hamukuaya, H., Bianca, L. G., Lancaster, M. S. N. A., Maseka, N. (2022). Trans-disciplinarity in transformative ocean governance research—reflections of early career researchers. ICES Journal of Marine Science, 79(8), 2163–2177. https://doi.org/10.1093/icesjms/fsac165

Sulyman, A. S., Adebowale, S., & Amzat, O. B. (2021). The interdisciplinary, multidisciplinary and transdisciplinary natures of library and information science: An analysis. *Library Philosophy and Practice, 6044*. https://digitalcommons.unl.edu/libphilprac/6044

Uwizeyimana, D. E., & Basheka, B. C. (2017). The multidisciplinary, interdisciplinary and transdisciplinary nature of public administration: A methodological challenge? *The African Journal of Public Affairs, 9*(9), 1-28. https://journals.co.za/doi/epdf/10.10520/EJC-c13a0cbc0

Woods, T., C., Rudd, J., Araújo, D., Vaughan, J., & Davids, K. (2021). Weaving lines of inquiry: Promoting transdisciplinarity as a distinctive way of undertaking sport science research. *Sports Medicine – Open, 7*(55). https://doi.org/10.1186/s40798-021-00347-1

Youm, Y. H. (2017). An overview of security and privacy issues for Internet of Things. IEICE Transactions on Information and Systems., 100 (8), 1649-166. https://doi.org/10.1587/TRANSINF.2016ICI0001

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. International Journal of Human–Computer Interaction, 32(3), pp. 215–257.https://doi.org/10.1080/10447318.2016.1136177