Doctoral theses at NTNU, 2022:357

Mazaher Kianpour

Cybersecurity Economics: A Multiparadigmatic Inquiry into Theory and Practice

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Information Technology and Electrical
Engineering
Dept. of Information Security and
Communication Technology

NTNU
Norwegian University of
Science and Technology

Mazaher Kianpour

Cybersecurity Economics: A Multiparadigmatic Inquiry into Theory and Practice

Thesis for the Degree of Philosophiae Doctor

Gjøvik, November 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

ISBN 978-82-326-6045-2 (printed ver.)
ISBN 978-82-326-5418-5 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2022:357

Printed by NTNU Grafisk senter

Contents

List of Tables

List of Figures

Out beyond ideas of wrongdoing and rightdoing there is a field.
I'll meet you there.

Rumi (1207-1273), Persian Poet

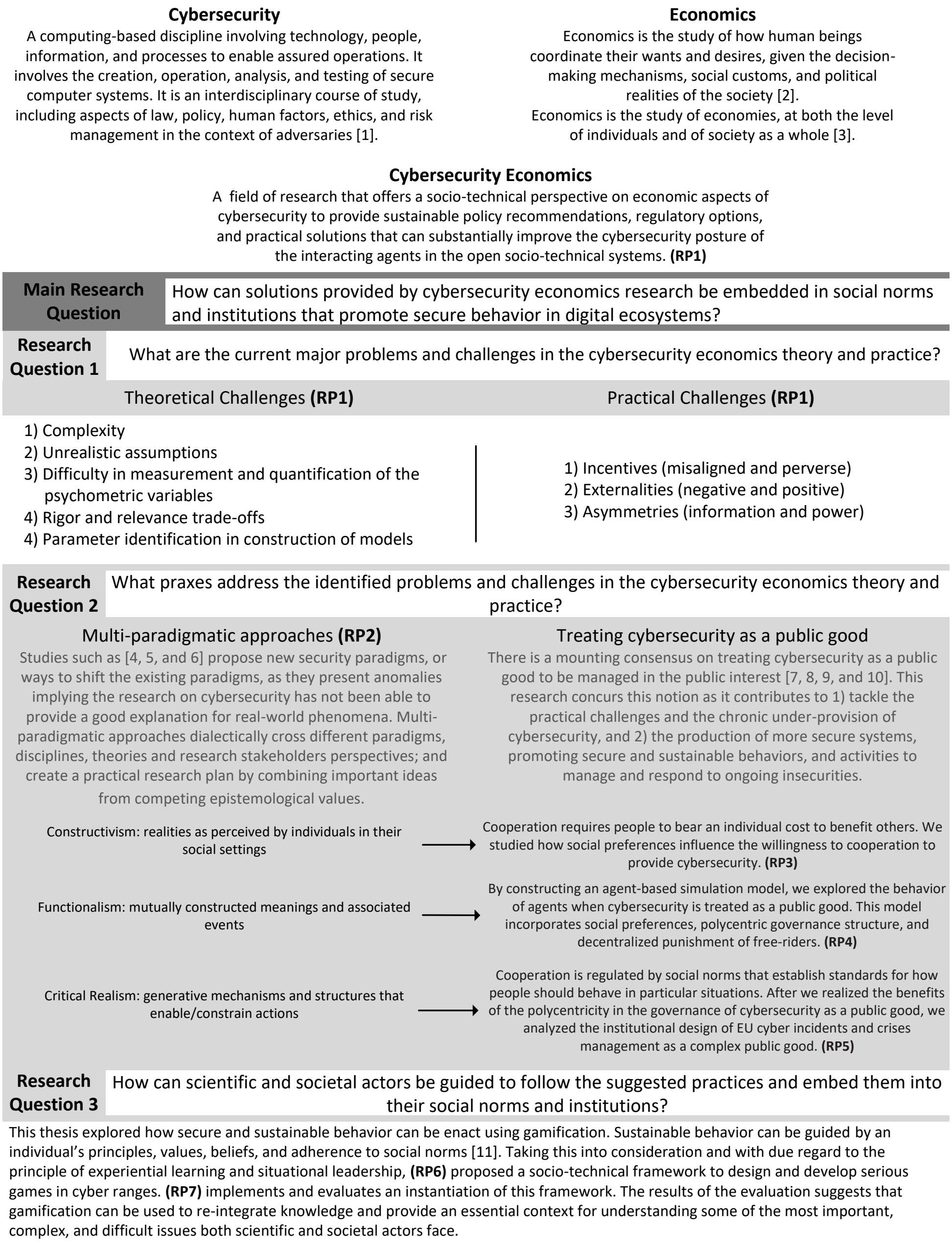
Abstract

Digital ecosystems are continually confronted with increasing number, sophistication, and complexity of cybersecurity threats and incidents. Cybersecurity researchers have been acutely aware of this challenge for many years, and it led them to look for solutions to bridge the gap between their empirical data and macro-level realities. In the early 2000s, economic models, or in general economics language, were hailed to explain, predict, and manage many cybersecurity problems more clearly and convincingly. Over the past two decades, the close collaboration between cybersecurity economics researchers and economists, sociologists, lawyers, politicians, and psychologists led to tremendous advances towards attaining these goals. This collaboration enabled us to identify, collect, and interpret existing and emerging issues that could impact the cybersecurity posture of agents operating at different levels of open, complex socio-technical systems. However, recent findings indicate that cybersecurity economists still struggle to factor in various issues, such as human and institutional governance and dominance structures, complexity and uncertainty of the digital ecosystems, and the rapidly changing dimensions of cybersecurity issues, to suggest practical and sustainable solutions.

These issues have made various challenges in theory and practice of cybersecurity economics that hinder the proposed solutions within this field to be embedded in social norms and institutions that promote secure behavior in digital ecosystems. After identification of these challenges, this research project explores and advocates multi-paradigmatic approaches to tackle the theoretical challenges in cybersecurity economics research. We argue that these approaches provide appealing theoretical and practical frameworks

to understand and interpret known and unknown cybersecurity problems. Regarding the practical challenges, however, this thesis supports the notion of cybersecurity as a public good. Although this notion has been proposed repeatedly by scholars, it has not been substantiated by qualitative and quantitative analysis and studies. Therefore, in this thesis, we take up the challenge of employing a range of paradigms including functionalism, constructivism, and critical realism within one research investigation: cybersecurity as a public good. This thesis outlines a research project in which several studies were conducted to investigate this topic from perspectives of individuals, groups, and institutions. Results were obtained through using theories and methods from multiple paradigms as the basis for research. In seven research papers, details of the studies are given, research findings are presented, and the validity of the methods is discussed.

Following transdisciplinary research strategy that supports co-creation of knowledge by participatory inclusion of scientific and societal actors, this research project suggests gamification and policy games to re-integrate knowledge and provide an essential context for understanding some of the most important, complex, and difficult issues both scientific and societal actors face. We proposed a socio-technical framework to design and develop serious games and developed and evaluated an instantiation of this framework. The evaluation results show a promising outlook on how gamification can be effectively used for promoting secure and sustainable behavior in digital ecosystems.



Cybersecurity

A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries [1].

Economics

Economics is the study of how human beings coordinate their wants and desires, given the decision-making mechanisms, social customs, and political realities of the society [2].
Economics is the study of economies, at both the level of individuals and of society as a whole [3].

Cybersecurity Economics

A field of research that offers a socio-technical perspective on economic aspects of cybersecurity to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems. **(RP1)**

Main Research Question How can solutions provided by cybersecurity economics research be embedded in social norms and institutions that promote secure behavior in digital ecosystems?

Research Question 1 What are the current major problems and challenges in the cybersecurity economics theory and practice?

Theoretical Challenges **(RP1)**

1) Complexity
2) Unrealistic assumptions
3) Difficulty in measurement and quantification of the psychometric variables
4) Rigor and relevance trade-offs
4) Parameter identification in construction of models

Practical Challenges **(RP1)**

1) Incentives (misaligned and perverse)
2) Externalities (negative and positive)
3) Asymmetries (information and power)

Research Question 2 What praxes address the identified problems and challenges in the cybersecurity economics theory and practice?

Multi-paradigmatic approaches **(RP2)**

Studies such as [4, 5, and 6] propose new security paradigms, or ways to shift the existing paradigms, as they present anomalies implying the research on cybersecurity has not been able to provide a good explanation for real-world phenomena. Multi-paradigmatic approaches dialectically cross different paradigms, disciplines, theories and research stakeholders perspectives; and create a practical research plan by combining important ideas from competing epistemological values.

Treating cybersecurity as a public good

There is a mounting consensus on treating cybersecurity as a public good to be managed in the public interest [7, 8, 9, and 10]. This research concurs this notion as it contributes to 1) tackle the practical challenges and the chronic under-provision of cybersecurity, and 2) the production of more secure systems, promoting secure and sustainable behaviors, and activities to manage and respond to ongoing insecurities.

Constructivism: realities as perceived by individuals in their social settings → Cooperation requires people to bear an individual cost to benefit others. We studied how social preferences influence the willingness to cooperation to provide cybersecurity. **(RP3)**

Functionalism: mutually constructed meanings and associated events → By constructing an agent-based simulation model, we explored the behavior of agents when cybersecurity is treated as a public good. This model incorporates social preferences, polycentric governance structure, and decentralized punishment of free-riders. **(RP4)**

Critical Realism: generative mechanisms and structures that enable/constrain actions → Cooperation is regulated by social norms that establish standards for how people should behave in particular situations. After we realized the benefits of the polycentricity in the governance of cybersecurity as a public good, we analyzed the institutional design of EU cyber incidents and crises management as a complex public good. **(RP5)**

Research Question 3 How can scientific and societal actors be guided to follow the suggested practices and embed them into their social norms and institutions?

This thesis explored how secure and sustainable behavior can be enact using gamification. Sustainable behavior can be guided by an individual's principles, values, beliefs, and adherence to social norms [11]. Taking this into consideration and with due regard to the principle of experiential learning and situational leadership, **(RP6)** proposed a socio-technical framework to design and develop serious games in cyber ranges. **(RP7)** implements and evaluates an instantiation of this framework. The results of the evaluation suggests that gamification can be used to re-integrate knowledge and provide an essential context for understanding some of the most important, complex, and difficult issues both scientific and societal actors face.

Figure 1: The thesis at a glance. The reference to the cited studies and details of highlighted research papers are in the next page.

List of Research Papers (RP)

- **RP1.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. 2021. "Systematically Understanding Cybersecurity Economics: A Survey" Sustainability 13, no. 24: 13677
- **RP2.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. "Multi-Paradigmatic Approaches in Cybersecurity Economics." Proceedings of the 7th Workshop on Socio-Technical Perspectives in Information Systems, October 14-15, 2021, Trento, Italy.
- **RP3.** Kianpour, Mazaher, Harald Øverby, Stewart J. Kowalski, and Christopher Frantz. "Social preferences in decision making under cybersecurity risks and uncertainties." In International Conference on Human-Computer Interaction, 2019, Florida, USA.
- **RP4.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. "Advancing the concept of cybersecurity as a public good." Simulation Modelling Practice and Theory (2022)
- **RP5.** Kianpour, Mazaher and Christopher Frantz. "Analysis of institutional design of EU cyber incidents and crises management as a complex public good." Under review in Policy Studies Journal
- **RP6.** Kianpour, Mazaher, Stewart Kowalski, Erjon Zoto, Christopher Frantz, and Harald Øverby. "Designing serious games for cyber ranges: a socio-technical approach." In 2019 IEEE European symposium on security and privacy workshops (EuroS&PW), IEEE, 2019.
- **RP7.** Kianpour, Mazaher and Stewart Kowalski "Promoting Secure and Sustainable Behavior in Digital Ecosystems Through Gamification" In Handbook of Research on Gamification Dynamics and User Experience Design, 2022.

List of cited papers in Figure 1

- **[1].** Bishop, Matt, et al. "Cybersecurity curricular guidelines." IFIP World Conference on Information Security Education. Springer, Cham, 2017
- **[2].** Colander, D.; Holt, R.; Rosser, B., Jr. The changing face of mainstream economics. Rev. Political Econ. 2004, 16, 485–499

- **[3].** Krugman, Paul, and Robin Wells. 2004. Microeconomics. New York: Worth.

- **[4].** J. M. Spring, T. Moore, and D. Pym, “Practicing a science of security: a philosophy of science perspective,” in Proceedings of the New Security Paradigms Workshop, 2017

- **[5].** O. Pieczul, S. N. Foley, and V. M. Rooney, “I’m ok, you’re ok, the system’s ok: Normative security for systems,” in Proceedings of the New Security Paradigms Workshop, 2014

- **[6].** H. Vescent and B. Blakley, “Shifting paradigms: Using strategic foresight to plan for security evolution,” in Proceedings of the New Security Paradigms Workshop, 2018

- **[7].** Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. Daedalus, 140(4), 70–92.

- **[8].** Schneider, F. B., Elain, S. M., & Deirdre, M. K. (2016). Public cybersecurity and rationalizing information sharing. Lausanne: Opinion Piece for the International Risk Governance Center (IRGC).

- **[9].** Weber, S. (2017). Coercion in cybersecurity: What public health models reveal. Journal of Cybersecurity, 3(3), 173–183.

- **[10].** Taddeo, Mariarosaria. "Is cybersecurity a public good?." Minds and Machines 29.3 (2019): 349-354.

- **[11].** White, K., Habib, R., & Hardisty, D. J. (2019). How to SHIFT consumer behaviors to be more sustainable: A literature review and guiding framework. Journal of Marketing, 83(3), 22-49

Acknowledgement

Before you read a short summary of my PhD journey, it is important that I acknowledge the people who have supported, encouraged and motivated me throughout that journey and made it one of the most memorable experiences of my life. First and foremost, my utmost thanks go to my parents, wife, and siblings for all their support and encouragements through my life.

I would like to express my sincere appreciation for my supervisor, Harald Øverby. I am extremely grateful for your trust in my abilities and for the freedom that allowed me to explore my scientific interests. Given the socio-technical perspective of this thesis, my PhD project would not have gone smoothly without the help and support of my co-supervisor, Stewart James Kowalski who sometimes, by talking to him, saved me tons of work and sometimes gave me TONS of work. Next, special thanks go to Christopher Frantz for the academic support, mentorship, and guidance.

I would also like to acknowledge the help and support of the administration and human resource of the Department of Information Security and Communication Technology (IIK) from the beginning till my last days at NTNU.

I would like to thank my colleagues and fellows at IIK. Having started to live in Norway with almost zero knowledge, I am delighted by what I learned and what we have done together with Martin Stokkenes, Grethe Østby, Adam Szekeres, Shao-Fang Wen (Steven), Ali Khodabakhsh, Kyle Porter, Parisa Rezaei, Hareesh Mandalapu, Jan William Johnsen, Amir Zarei, Siamak Khatami, Majid Ansari, Ali Bozorgian, and many other who made my PhD exhilarating and pleasant.

Part I

Introduction Chapters

Chapter 1

Introduction

This chapter provides an introduction to the thesis subject area and problem statement. To this end, it describes the research motivation, research questions, research outcomes, key contributions, and overall outline of the thesis.

1.1 Research Motivation

When I started this project in May 2018, WannaCry (3) and its shocking effects were still the hot topics of the debates among academic researchers, industrial practitioners, and technology journalists. Within 8 hours, WannaCry had spread around the world, infecting thousands of computers in 150 countries (4) and had an impact that was estimated to range between $4 and $8 billion (5). In 2019, according to the news sites Insider and The Washington Post, the personal information of over 533 million Facebook users in 106 countries was posted in a low-level hacking forum for free after a data breach in August (6, 7). Although Facebook decided not to notify users, security researchers said hackers could use the data to impersonate people and commit fraud. In 2020, many businesses, service providers, and governments witnessed a surge in cyber-attacks, including phishing, social engineering, and spamming, due to the changes caused by the COVID-19 pandemic. However, the year ended with a significant and large-scale supply chain attack targeting the IT infrastructure company SolarWinds. The SolarWinds hack gave the attackers access to the computer networks of over 18,000 of SolarWinds's customers, including sensitive and high profile targets such as the U.S. government agencies, American nuclear research labs, government contractors, IT companies, and non-governmental agencies around the world (8). According to The New York Times (9), new evidence from the security firm CrowdStrike suggests that the SolarWinds hackers used companies that sell software on behalf of Microsoft as a conduit to break into customers' software (10). Finally, by the time I started to write this thesis, the Log4j vulnerability was making the headlines. The vulnerability has been labeled as the "most serious vulnerability in decades" which could impact the entire internet and hundreds of millions of devices in the world (11).

The previous paragraph highlighted a few significant, large-scale cyber-attacks in the last four years. This list could be appended by thousands of other cyber-attacks targeting single or groups of national and international entities and ordinary people around the world (12). Whereas deficient cybersecurity technologies deserve considerable blame for inadequate cyber-defense, seeing and accepting the problem only as a technical shortcoming is to miss the bigger picture (13, 14). Governance structures which enable misaligned incentives (15), uncontrolled spillovers and endogenous uncertainties (16), and dominating powers unwilling to engage in negotiations on cybersecurity-related subjects are also part of the problem. Besides cybersecurity is not a technology in itself, but rather a technology-driven problem that spans across multiple jurisdictions within regulatory institutions (17). Fast changing technologies have created and changed dimensions of cybersecurity issues (18).

Challenges to remedy these problems, and also their negative impacts, exacerbate when digital societies are being shaped locally and globally. The complexity, interdependencies, and innovation-driven growth of the socio-technical systems which such societies rely upon have created obstacles to provide sustainable solutions to mitigate cybersecurity risks (19, 20). A review (Research Paper 1) of the literature focused on cybersecurity economics shows that researchers are well aware of these problems. However, have their research outcomes been successful to deal with the problems efficiently? The answer to this rhetorical question is indeed: "we do not know!". Each and every attempt within the research field of cybersecurity economics makes a contribution toward a solution. However, the underlying problems and questions are "What is the adequate level of cybersecurity and how much should we spend to provide this level?", "How and for whom to provide cybersecurity?", "Who needs to pay for interdependent and cascaded risks?"

These questions show that cybersecurity economics is challenged by several problems which their solutions require fundamental changes in structures, paradigms, behavior, and institutions. The presence of these problems leads to trade-offs and dilemmas such as not-in-my-backyard dilemma and public goods dilemma. These dilemmas require proper conceptualization to adequately address the specificities of cybersecurity. Therefore, the absence of proper understanding of numerous factors and causalities will lead to missed opportunities and empowers those who are willing to discredit the essence of the fundamental changes (21). As a result, we observe that today organizations and governments are caught in a vicious circle[1] in which various elements intensify and aggravate each other, leading to a worsening of the situation. This research project seeks to understand these elements (i.e., major problems, issues, and challenges in cybersecurity economics research) and to explore praxes and mechanisms that creates knowledge that is solution-oriented, sustainable, and transferable to both scientific and societal practices.

1.2 Problem Statement

This section presents the problem that this thesis focuses on. This is a hard task as cybersecurity has become a scientific and societal concern in the last decades due to digital transformation (24). Digital transformation has created massive and complex interacting digital ecosystems. Various interesting socio-technical transitions are expected to emerge from strong interactions in these ecosystems under adopting new technologies and changing business models (25). These transitions can only develop, be managed, and evolve when the focus is not limited to technical aspects, but also includes social and institutional aspects. They are multi-level in terms of governance, and they cut across the individual, organizational, national, regional, and global levels. A significant consequence of these cross-cutting interactions is the emergence of collective action problems because of misaligned incentives, information asymmetry, externalities, and other issues that can be explained more clearly and convincingly using the language of economics. Since 2000, a stream of research, known as cybersecurity economics, has investigated the effect of these problems on the cybersecurity posture of agents operating at all these levels.

[1] Vicious circle refer to complex chains of events that reinforce themselves through a feedback loop. In the absence of appropriate measures, the elements of the vicious circle reinforce each other and lead to detrimental results (22, 23).

We observe that many of the mixed-methods and insights from other fields of study such as economics, sociology, psychology, and politics have been employed in cybersecurity economics. The studies conducted within cybersecurity economics research emphasize the relevance and complexity of the interrelationship between social and technical dimensions in the analyses of cybersecurity topics. The inclusion of 1) human agency, reflected by the interests, behavior, and preferences of humans, 2) organizations, reflected by the information flow, resource allocation, and strategy implementation, and 3) institutions, reflected by societal practices, norms, and values in the literature of cybersecurity economics sets the stage for the multi-level analysis. This analysis needs to be navigated through a different type of thinking than the ones which created the problems. There are two reasons behind this statement.

First, as argued by Fazey (26), many of the problems that societies are currently facing like climate change and including the cybersecurity problems, need new ways of reasoning and assessment that go beyond dominant disciplines and paradigms, exploring new insights and responses. Second, since there are increasing calls for exploring pathways for societal transformations towards sustainability, the solutions need to be systematic, long-term, and adapt to non-linear changes, spanning across the different sectors of societies. To this end, this thesis advocates multi-paradigmatic approaches and transdisciplinary research that support co-creation of knowledge by participatory inclusion of scientific and societal actors to address the following main research question:

> *How can solutions provided by cybersecurity economics research be embedded in social norms and institutions that promote secure behavior in digital ecosystems?*

The main research question is twofold: (a) finding and developing societally relevant solutions; and (b) communicating the designed and created research outcome to relevant actors to be implemented in a way that brings about a significant improvement in the current situation. The former stresses on that greater attention in cybersecurity economics theory is required to propose solutions and processes for change that expand beyond simply understanding the problem. This includes focus on aspired outcomes and how they are expected to be achieved. The latter is a fundamental point in cybersecurity economics practice when it comes to deciding how cybersecurity actors and their interrelations should be governed by social rules and institutions. Therefore, this research explores both theory and practice of cybersecurity economics to answer this question and the research questions defined in the next section.

1.3 Research Questions

To answer the main research question the work has been broken down into three sub-questions:

RQ1. What are the current major problems and challenges in the cybersecurity economics theory and practice?

RQ2. What praxes address the identified problems and challenges in the cybersecurity economics theory and practice?

RQ3. How can scientific and societal actors be guided to follow the suggested practices and embed them into their social norms and institutions?

The research questions follow a sequential order in which the study of one relies upon the results of the former. RQ1 aims to ground the research by exploring contemporary research approaches and outcomes to identify major problems and challenges in the cybersecurity economics theory and practice. The answers to this question introduces an important query to find out what praxes can be suggested to address the identified problems and challenges in cybersecurity economics theory and practice. Praxis means the process by which the relationship between reflection and practice or theory and practice can transform society, organizations, and individuals (27). Therefore, RQ2 aims to explore a variety of methodological procedures that empower both scientific and societal actors to resolve epistemological and practical tensions in tackling the identified challenges. Lastly, RQ3 seeks to realize how these procedures can be developed and evaluates a mechanism through which they influence the cybersecurity of digital ecosystems and promote sustainable cybersecurity solutions.

1.4 Research Strategy

As mentioned in the previous sections, cybersecurity challenges can be categorized as socio-technical challenges. Transdisciplinarity has been proposed as one important way for researchers to respond to this type of challenges, particularly when sustainable solutions are needed to develop and drive secure digital ecosystems (28, 29, 30). Transdisciplinary research is a comprehensive, multi-perspective, problem- and solution-oriented approach to a societally relevant issue that integrates scientists from a wide range of academic disciplines as well as non-academic actors (31, 32). A transdisciplinary research is needed to understand the structure and processes of the socio-technical systems as well as the paradigms, values, and goals of different actors within the problem field, and to identify methods and means of achieving secure and sustainable digital ecosystems.

There are several frameworks that can be used for transdisciplinary research (33, 34, 35, 36). Each framework has its particular benefits and a researcher can choose one that is most relevant for their research. This research employs the framework proposed by Lang et al. (35). As Figure 1.1 shows, this framework is composed of three phases. The phases are linked and iterative, where feedback is always obtained from one phase to the others. The first phase starts with the identification of societal problems. The researcher formulates research objectives, societally-relevant research questions, and the design of a research study to navigate our inquiry. These three are presented in Sections 1.2, 1.3, and 3, respectively.

The second phase of this framework is the actual doing of the research by adopting a set of integrative (scientific) paradigms and methods to further develop and integrate different bodies of knowledge in the process. This phase aims at generating knowledge which is meaningful to practitioners and which creates a comprehensive problem understanding. In transdisciplinary research, knowledge is conceptualized as being of three types: systems, target, and transformation knowledge. Systems knowledge is analytical, descriptive or explanatory knowledge about specific problems, challenges, and ideas. Target knowledge is normative knowledge about values and norms related to more desirable futures. Transformation knowledge is practical knowledge about how to transform an existing, problematic situation into a better one (37, 38). These are gathered, exchanged, compared, and synthesized from various sources, including from academic and non-academic stakeholders while defining strategies to address real-world problems. This transdisciplinary process yields co-produced knowledge which provides a holistic problem understanding across different scales and levels of abstraction.

Knowledge systems are differentiated according to three levels of abstraction: most abstract level, intermediate level, and most concrete level (39). Each level is characterized by its content and its connections. Theories form the middle level of abstraction, and they contain specific proposi-

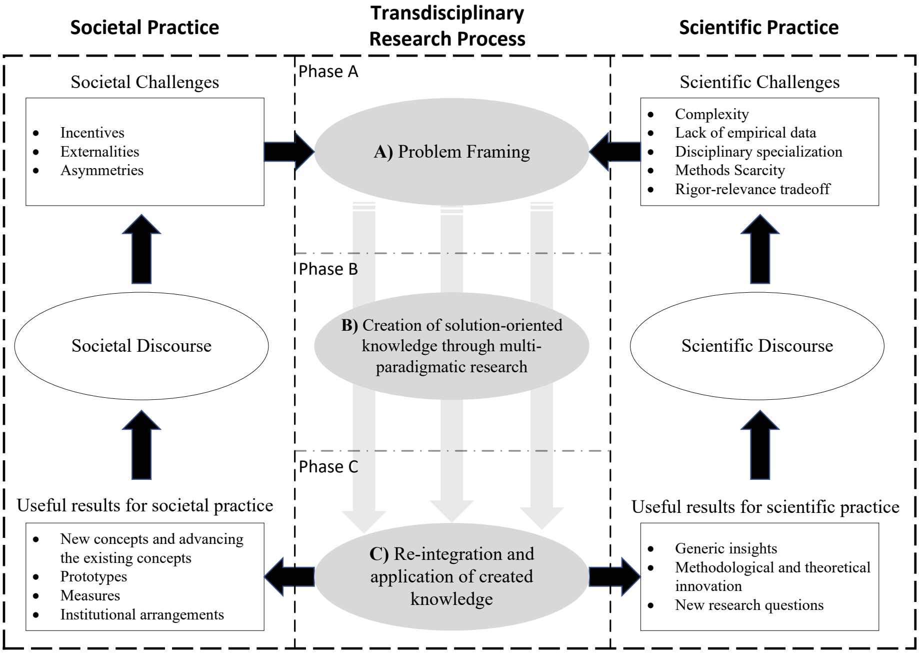

Societal Practice
Transdisciplinary Research Process
Scientific Practice
Phase A
Societal Challenges
Incentives
Externalities
Asymmetries
A) Problem Framing
Scientific Challenges
Complexity
Lack of empirical data
Disciplinary specialization
Methods Scarcity
Rigor-relevance tradeoff
Phase B
Societal Discourse
B) Creation of solution-oriented knowledge through multi-paradigmatic research
Scientific Discourse
Phase C
Useful results for societal practice
New concepts and advancing the existing concepts
Prototypes
Measures
Institutional arrangements
C) Re-integration and application of created knowledge
Useful results for scientific practice
Generic insights
Methodological and theoretical innovation
New research questions

Figure 1.1: Transdisciplinary research process as the research strategy of this project. Adapted from (35). This strategy is comprised of three phases. Each phase interrelates with both societal and scientific practices. For example, after re-integration and application of created knowledge in Phase C, we present our generic insights (e.g., how to benefit from multi-paradigmatic approaches in cybersecurity economics research, advancing the concept of cybersecurity as a public good, and how gamification can be used as a promotion and behavior change strategy), methodological innovation (e.g., using Institutional Grammar to analyse the institutional designs within the domain of cybersecurity) theoretical innovation (e.g., incorporation of social preferences in the decision models and utility functions in cybersecurity economics models) and new research question outlines in Section 4.2. In the societal practice, we proposed a multi-layer perspective to treat cybersecurity as a public good, developed a prototype of a policy game that can be used to promote secure and sustainable behavior in digital ecosystems, and new insights and suggestions for the institutional arrangements within the context of cyber incidents response and crises management.

tions about constitutive concepts (elements of the theories) and causal connections between these concepts (the relational structure of the theories). On a higher, more abstract level, there are paradigms. They contain cognitive signifiers, which function as anchor points for the organization of knowledge (in other words, as focal points for the scientific discourse). Paradigms provide the connections between theories in specific fields of research and more generic ontological and epistemological perspectives. On the lowest, most concrete level, there are the observable implications that we deduce from theories (predictions). They form the connecting points between abstract systems of knowledge and the empirical world. As presented in Section 3.2, different forms of inference enable us to move from concrete to abstraction. In addition, Chapter 3 describes the theoretical rationale, research approach, research methodology, and research methods adopted in Phase B.

Phase C focuses on the use, application, and implementation of the research outcomes. As different paradigms and research methods are integrated over the entire process of transdisciplinary research, this phase is different from the classical form of knowledge transfer from science to practice (40, 41). It is, instead, (re-)integration and application of results into the societal practice and scientific practice. In our research, this integration aims 1) to enhance decision-making capacity of the practitioners involved by empowering and motivating them to contribute more actively to the implementation of provided solutions, and 2) to suggest new changes to the current institutional design of cybersecurity policies and regulations to alter the structure of incentives.

1.5 Research Outcome

This chapter discusses how our findings during this project contributed to answer the research questions. The chapter is organized according to research questions defined in Section 1.3. Finally, the section ends with the classification of the research papers based on type of knowledge and levels of abstraction.

1.5.1 Main Research Question

> *"How can solutions provided by cybersecurity economics research be embedded in social norms and institutions that promote secure behavior in digital ecosystems?"*

As we mentioned in Section 1.2, the main research question is twofold. It concerns both theory and practice of cybersecurity economics research. In theory, the solutions should extend actors' view of cybersecurity to comprehend the complexity of their implementation in practice. It is foolhardy to assume that just because two or more factors have been incorporated in a model to determine the optimal investment in cybersecurity, the cybersecurity posture will automatically enhance.[2] There may be other factors (e.g., a perception that underinvestment will never be discovered by the regulators; market rewards corporations for risk-taking when those risks are largely borne by other parties; or there are conflicting interests involved) that will influence intentions, behaviors, and outcomes. To realize theoretical benefits in practice, the proposed solutions should be multi-pronged and have the potential to be deployed as a social norm embedded in institutions and implemented by actors. This thesis puts forward employing multi-paradigmatic approaches in research within the domain of cybersecurity economics contributes to obtain this potential.

In practice, however, actors face with various issues such as incentives (misaligned or perverse), asymmetries (information or power), and externalities (negative or positive) that make barriers to implement the proposed solutions. This research project concurs the doctrine of cybersecurity as a public good to deal with such challenges. Public goods contribute to social inclusions and they strengthen a shared sense of participation. Such characteristics enable the actors to diffuse information, co-produce solutions, share in anticipation of the future, and coordinate in different forms. However, due to externalities and misalignment of incentives, not all cybersecurity functions, products, and services should be treated as public goods. This distinction matters for actors and policy-makers. Therefore, a multi-layered perspective that distinguishes utility, supply, and production is suggested to improve the understanding, translating and deploying solutions to create

[2] This statement does not mean that theory can have a very weak impact on practice. Conversely, this thesis acknowledges that scientific models and academic research can have a tremendous influence even if not embedded in transdisciplinary research and co-created with many societal actors. As John Maynard Keynes states in his book, The General Theory of Employment, Interest and Money (42), "Practical men, who believe themselves to be quite exempt from any intellectual influences, are usually the slaves of some defunct economist". However, he questions restrictive assumptions and shows the limitation of such approaches by putting at the centre of his analysis the role played by uncertainty in shaping economic outcomes. As he pointed out: "It would be foolish, in forming our expectations, to attach great weight to matters which are very uncertain". Therefore, this thesis encourages cybersecurity economics research to lay stress on studies that take account of complexity, interdependencies, uncertainty, and diversity of factors that contribute to a result.

and sustain secure and resilient environment.

Finally, to meet theory and practice needs, this thesis suggests gamification from a instrumental perspective to modulate the behavior of individuals and groups. Gamification, as a participatory approach, enables us to reintegrate knowledge, close the gaps, and communicate the designed and created research outcomes to relevant actors. Through gamification we can identify actors' needs, disentangle their problems, and gather a comprehensive understanding of the problem context. We can also enable, engage, and empower them to actively implement the solutions proposed within the scientific practices.

In the following sections, we represent the details of challenges, suggested praxes to deal with these challenges, and mechanisms to develop and implement these suggestion.

1.5.2 Research Question 1

Research Question: What are the current major problems and challenges in the cybersecurity economics theory and practice?

Related Research Paper:

- RP1. Systematically Understanding Cybersecurity Economics: A Survey

Main Contribution:

- Improved understanding of the problems and challenges in cybersecurity economics theory and practice

Answer to the research question: The identified major problems in the theory and practice of cybersecurity economics include scarcity, uncertainty, change, and dominance. RP1 and Section 2.1 of this thesis discuss these problems in detail. Table 1.1 outlines these problems with an example of each in theory and practice. For an instance, scarcity in theory can be attributed to scarcity of research methods or knowledge to holistically understand and assess the situations and propose efficient solutions. Scarcity in practice, on the other hand, is featured by scarce cyber-physical technologies and skilled workers to deploy in networks and cyber infrastructures.

Table 1.1: The identified major problems in theory and practice of cybersecurity economics with anecdotal examples (the examples are based on individual experience rather than rigorous or scientific analysis).

	Theory	**Practice**
Scarcity	Scarcity of research methods or knowledge	Scarcity of skilled worker or cyber-physical technologies
Uncertainty	Uncertainty in scientific measurements and prediction	Uncertainty in technological developments
Dominance	Dominance of neoclassical economics in cybersecurity economics research at the early stages	Power imbalance in the EU to influence the governance structure
Change	Change in political structure of a country (e.g., Brexit)	Change in scientific collaborations

In the literature of cybersecurity economics, different solutions have been suggested to these problems. We classified these solutions into groups of budgeting, economic efficiency, interdependent risks, information asymmetry, governance, and sustainability. The diversity of these solutions indicates that cybersecurity economics research is not limited to determine optimal investment in cybersecurity, but also covers politics, coordination, and other organizational and institutional topics.

After identification of major problems, we highlighted five major challenges that have been pointed out in the literature of cybersecurity economics. The first challenge that has been extensively recognized in the literature is complexity. If organizations, societies, and markets are viewed as complex and out-of-equilibrium systems, understanding non-linear, adaptive, and evolutionary patterns which emerge from system dynamics and agents' behavior in network structures is important for researchers. To tackle this challenge, the researchers need to reconsider the dominant equilibrium thinking in their models and shift from focusing on proposing models to optimize and predict system equilibrium to manage the complexity of cybersecurity better.

The second challenge is that most economic models rest on a number of assumptions that are not entirely realistic[3]. For example, we inductively

[3] The debate on acceptability of unrealistic assumptions as the simplifying assumptions became

derived from our observation that at the early stage of research on cybersecurity economics, scholars often assumed that the decision makers are rational and have perfect information. After two decades of research, there is a growing literature in cybersecurity economics that shows humans do not have the processing capacity to be perfectly rational (i.e., bounded rationality), even if they had perfect and complete information. Therefore, any analysis of the results and application of the proposed models must consider the inaccuracies that compromises the model based on these assumptions. Additionally, the model overlooks issues that are important to the question being studied, such as externalities and interdependencies[4].

The third challenge is the difficulty in measurement and quantification of the psychometric variables, such as the perceived value of cybersecurity, perceived cyber risks, and willingness to pay/collaborate. When the researchers neglect these variables, their model cannot provide full explanations or correct predictions of the phenomenon under study. The lack of reliable instruments to determine the indicators of these latent constructs contribute to the difficulty in measuring them. Another important challenge is the tension between rigor and relevance across cybersecurity economics models. On one hand, the models that are purely theoretical or expressed mathematically are prone to poor relevance and applicability. One the other hand, the models that are purely based on practitioner concerns are prone to poor theoretical coherence and rigor. The main question here is if a trade-off must exist between rigor and relevance. If yes, what is the right balance between rigor and relevance in the study? To answer these questions, the researchers need to understand the system, identify the significant constructs,

heated after Friedman (43) pointed out that assumptions used in economics need not be realistic; as long as the conclusions (especially predictions) stand up to the test of empirical verification, unrealistic assumptions are acceptable as simplification for analysis (44). This thesis acknowledges that simplifying assumptions or methods of simplification may or may not be acceptable depending on the context. Exactly the same assumption may be acceptable for a certain analysis but not in another. Some very successful theories are based on assumptions that appear hard to justify (45). For example, invisible hand theory that involves self-interested who choose rationally. The main point differentiating acceptance and rejection should be whether the results (conclusions and predictions) are distorted to be misleading or not. This makes realism, at least in terms of the relevance of results, important. However, some assumptions may be acceptable as harmless simplifications, or even useful simplification to allow focus on the important relationships. For example, while pure risk neutrality is unrealistic (46), assuming agents to be risk-averse can be considered as a simplifying assumption (e.g., (47)).

[4] One of the unrealistic assumptions in neoclassical economics is that agents act independently on perfect (full and relevant) information. Relying on this assumption, the Gordon-Loeb model neglects all forms of interdependence that can arise among firms (48).

and use scientific methods that promote the systematic uptake of research findings and other evidence-based practices into routine practice.

Finally, the fifth challenge is the arising problem of parameter identification in construction of models using econometrics. Econometrics is the application of statistical and mathematical methods using observational and empirical data to develop new theories or test hypotheses. There are a multitude of parameters which affect the behavior of actors, operation of socio-technical systems, and structure and characteristics of the environment. When the value of these parameters and how they effect on the outcomes is uncertain, the reliability of constructed models to predict decreases when it comes to empirically test the models. The next research question attempts to suggest solutions that empower both scientific and societal actors to deal with these challenges.

In addition to the theoretical challenges identified in this research project, there are significant practical challenges in cybersecurity economics as well. In this research project we categorized these challenges into three groups of economic incentives, asymmetries, and externalities. This categorization is based on the fundamental concepts highlighted in (49). In simple terms, incentives are means that influence people to act in certain ways. The joint influence of social norms and economic incentives on individuals' choices are recognized in the literature of sociology and economics (50, 51, 52). The literature of cybersecurity economics has been focused on two challenges regarding the economic incentives: misaligned incentives and perverse incentives. The former occurs when individuals, groups, divisions, or organizations are rewarded for behaviors that would conflict with others within and across organizations (53). The latter are those incentives that have unintended and undesirable results that are contrary to the intentions of their designers (54, 55). Misaligned and perverse incentives are increasingly becoming important now that cybersecurity is not merely used to protect against malicious attacks, but also to protect monopolies, product differentiation and market segmentation (56).

Asymmetries, the second category of these challenges, can be separated into information asymmetry and power asymmetry. The finance literature show theoretically that informational asymmetries can have a profound impact on a agents financing and investment decisions and on managerial incentive compensation contracts (57, 58, 59). The problems of information asymmetry have also received considerable attention in the literature of cybersecurity economics; however, studies on power asymmetry are limited. Social interactions involve most of the times power asymmetric relationships (60). Power stems from various sources and takes several forms. For instance, people or organizations are powerful when they can administer punishments or rewards, when they are in a hierarchically higher position than others, when they have knowledge, expertise, and technology, when they are admired and respected, and when they have alternative options which enable them to make choices. As Anderson stated "information security is about power and money (56)", power asymmetry is a decisive factor in how all kinds of relationships develop and how conflicts are handled and resolved.

The third category of practical challenges involves externalities and spillovers. Externalities occur in an economy when the production or consumption of a specific good or service impacts a third party that is not directly related to the production or consumption of that good or service. For example, under-investment in cybersecurity by SolarWinds threatened the security of customers that were using commercial software application made by SolarWinds and incurred them external costs. Spillover effect, on the other hand, refers to the impact that seemingly unrelated events in one agent (e.g., nation, organization, or even individual) can have on the cybersecurity posture of other agents. For example, geopolitical and geo-economic tensions among the countries are increasingly expressed in cyber and information warfare which have wide-ranging impacts in the private sector due to state-sponsored cyber-attacks against them.

Martinez–Carrasco separates spillovers into either technological or social in nature (61). Technological spillovers can be thought of as the mechanical response of rational agents responding to stimulus generated in the environment, where their answer to these stimuli is independent to the identity of other agents. Social spillovers, by comparison, emerge from the social preferences of the agents. Social spillovers may activate based on the mere presence of someone else (as in the peer pressure or pro-social behavior literature) or it may depend on the characteristics and the type of interaction with other agents. Social spillovers may appear even if agents are technologically independent and there is no interaction among them. While externalities and spillovers have both positive and negative effects, the literature of cybersecurity economics mostly has been focused on the negative effects (62, 63).

The combined, or even separated, effects of these practical challenges in cybersecurity encourage problematic self-interested behavior among the actors. Moreover, some of these challenges such as misaligned incentives and information asymmetry reinforce themselves through a feedback loop. These challenges are not new to the economists and they have been extensively studied in the literature of economics. However, within the context of cybersecurity economics, the researchers face with important questions regarding the design of research projects and methodologies that address these challenges. This research project acknowledges that these challenges can be overcome by taking individual and structural factor into account. As a governance system can affect the degree of information asymmetry between the agents (64), the true preferences and intention of individuals can also cause asymmetric information (65). The next research question investigates the praxes that can address the identified problems and challenges in the theory and practice of cybersecurity economics.

1.5.3 Research Question 2

Research Question: What praxes address the identified problems and challenges in the cybersecurity economics theory and practice?

Related Research Papers:

- RP2. Multi-paradigmatic approaches in cybersecurity economics
- RP3. Social preferences in decision making under cybersecurity risks and uncertainties
- RP4. Advancing the concept of cybersecurity as a public good
- RP5. Analysis of institutional design of EU cyber incidents and crises management as a complex public good

Main Contributions:

- A set of recommendations that aim to support a transdisciplinary, reflective, collaborative, and integrative research within the field of cybersecurity economics
- Examining the doctrine of cybersecurity as a public good through a multi-paradigmatic research

Answer to the research question: This thesis recognizes that the aforementioned problems and challenges cannot be dealt with through a single paradigm. Therefore, in RP2, we sought to explicate and contextualize multi-paradigmatic approaches to deal with the highlighted challenges in theory. Multi-paradigmatic approaches enable the researchers to manoeuvre in between and across a mixture of disciplinary boundaries as the first step towards transdisciplinary research. Transdisciplinary research does not require a fundamental reorientation of the science. Rather, in our understanding, it is a synthesis of different paradigms, each with a clear orientation, function, and methodology. A researcher can cross these paradigms to identify transformative discourses and thus represent an important and irreplaceable contribution to complex issues. To date, no work has been published explicitly describing the methodological approaches that might be used to integrate the range of paradigms present in most cybersecurity economics research. However, in this research we discussed the desirability and feasibility of this approach along with some guidelines that can be followed to initiate a multi-paradigmatic research project.

We describe the multi-paradigmatic approach in cybersecurity economics research as a process of i) examining critically personal and professional values and beliefs, ii) exploring how worldviews have been shaped and governed by largely invisible social and cultural norms, iii) appreciating and understanding the intertwined role of institutions in reducing uncertainties and establishing sustainable, secure cyberspace, and iv) delineating future scenarios as a way to anticipate challenges, opportunities, and threats for organizations and governments' contingency planning. This process produces a style of research that synthesizes divergent insights and contributed to deal with the outlined challenges in theory of cybersecurity economics. In practice, however, we supported the doctrine of cybersecurity as a public good to address the challenges such as incentives, asymmetries, and externalities.

Public goods are costly to produce but benefit everyone, thus creating a social dilemma: individual and collective interests are in tension. Ignoring this dilemma leads to the under-provision of cybersecurity as a public good. Understanding how to motivate stakeholders to pay these costs is therefore of great importance for policy-makers. Our studies (RP3 and RP4) show that voluntary cooperation is fragile, even if most actors are not free riders. Other mechanisms like punishment, rewards, communication, or good institutional design are necessary to sustain cooperation. By employing multi-paradigmatic approaches, cybersecurity economics can significantly contribute to the formulation and deployment of such mechanisms. In our research, we employed two paradigms of constructivism and critical realism to examine the concept of cybersecurity as a public good in different perspectives. We studied this topic initially by testing several hypotheses to show how the assumptions and parameters of behavioral models of social preferences relate to the willingness to cooperate within the context of cybersecurity. The moderating effect of social preferences on willingness to cooperate was supported by the collected data from societal stakeholders. The results of this study are presented in RP3. This led us to incorporate social preferences into the utility function that predicts observed decisions. It also motivated us to study critical paradigm where perceives human nature as cooperative, collective, and social.

With these results, we constructed an agent-based model in which a group of heterogeneous agents participate in provision of several cybersecurity measures as public goods. Heterogeneity of the agents is based on their resource level, other-regarding preferences, reciprocity, and experience of cyber-attack. Analyzing the influence of different parameters of this model showed that with possibility of punishment, the agents adopt an evolutionary strategy towards the provision of cybersecurity as a public good and create a robust environment. In other words, the simulation results for our baseline model suggested that the environment forms a dominant strategy which promotes the cooperation efficiently. Furthermore, our simulations have been able to exhibit altruistic punishment and inequity aversion preferences in the agents' decisions. In this connection, it is important to mention that the success of providing cybersecurity as a public good was predominantly enabled by the dynamic level of contributions based on the agents' experience of being a victim, punished, or number of existing free-riders.

In view of the common collective action problems, including free-riding, it is crucial to understand the forces shaping actors' cooperation. In RP4 we showed that the neglect of other-regarding preferences may induce cybersecurity economics researcher to largely misunderstand the nature of many collective action problems. A key to the understanding of collective action problems is the interaction between selfish actors and actors with other-regarding preferences. We illustrated the impact of other-regarding preferences on cooperation for the case of reciprocal or inequity averse actors. First, reciprocal actors are willing to cooperate if they are sure that the other actors who are involved in the collective action problem will also cooperate. If the others cooperate, despite pecuniary incentives to the contrary, reciprocators are conditionally cooperative. Likewise, inequity averse actors are also willing to cooperate if they can be sure that others cooperate. Second, reciprocal, inequity averse, and altruistic actors are willing to punish free-riders because free-riders exploit the cooperators. Thus, if potential free-riders face reciprocators they have an incentive to cooperate to prevent being punished.

The coexistence of conditional cooperators and selfish subjects has important implications. It implies that institutional designs may cause large behavioral effects and constrain or shape the actors' incentives (15). Institutional designs reflect the shared rules, norms, and belief systems that are established as guidelines for social behavior, which shape the nature of decision making, coordination, and information-sharing processes (66). Institutional designs can take different forms and structures (e.g., polycentric, centralized, or decentralized). Our results in RP4 indicated that polycentric configurations of institutions for addressing collective action problems and contribution to provide cybersecurity as a public good has been successful. With such insights, we suggested that polycentric governance structure should be used to promote active participation that empowers stakeholders to be critical in understanding their problems and enables them to reflect on their situations that help them to objectively decide on trade-offs. Therefore, we advanced our research to study how polycentricity is conceptualized and operationalized in cybersecurity policies and institutions. In RP5, we employed Institutional Grammar 2.0 to investigate whether the EU's cybersecurity strategies and policies establish a polycentric governance structure to respond and manage cyber incidents and crises as a complex public good. Moreover, we analyzed the EU cybersecurity policies to identify what sanctions are prescribed as part of the regime and to what extent the sanctioning is centralized or decentralized. Since the scope of this study has been narrowed down to cyber incident response and crisis management across the EU, we also explored to what extent policies signal actors' commitment to ensure efficient coordinated response to large-scale cybersecurity incidents and crises.

The results of this study uncovered the variation in polycentricity within specific cybersecurity regulations in the EU governance system and the variation in authorities of different actors across those regulations. However, our study found weak evidence of punishment and signals of commitment to common goals in the analyzed policies. Although the policies of punishment depend on cultural, political, and legal values, the neglect of proportionate punishment immensely influences the active participation of agents in the achievement of common goals. One of the reasons that policy-makers have failed to adequately address these two concepts in cybersecurity policies is that the policy-makers have been unable to perceive the complexity of human behavior and the systems in which we live. This led us to inquire into the third research question to come up with approaches that enable policy-makers to identify the issues that are most relevant to their specific context and needs.

1.5.4 Research Question 3

Research Question: How can scientific and societal actors be guided to follow the suggested practices and embed them into their social norms and institutions?

Related Research Papers:

- RP6. Designing serious games for cyber ranges: a socio-technical approach
- RP7. Promoting secure and sustainable behavior in digital ecosystems through gamification

Main Contributions:

- A new framework to design and develop serious games to raise security awareness, teach hands-on skills, and develop key competencies
- A game design process to promote secure and sustainable behavior in digital ecosystems and understand the needs and characteristics of the players through gamification experiences

Answer to the research question: The third research question concerns through what mechanisms research outcomes become societally relevant and influence cybersecurity posture of digital ecosystems. Researchers produce knowledge as a potential. Actualization of knowledge requires its use (67). This thesis showed that gamification is a plausible method that can be utilized to instill key competencies (e.g., system thinking, adversarial thinking, integrated problem-solving, and anticipatory competencies) to advance secure and sustainable behavior in digital ecosystems. Furthermore, games

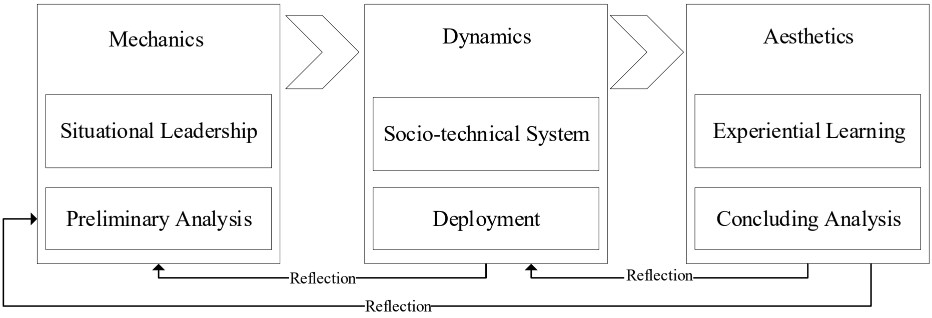


Figure 1.2: Proposed framework to design and develop cybersecurity serious games (1)

enable the researchers to benefit from practitioners' experience and knowledge. When seeking to understand the experiences and behaviors of humans, gamification plays an important role in co-production of knowledge and retroductive inference of what experience must have been.

Considering the complex nature of the cyber domain, the knowledge and motivation of participants, and the necessity of reflection in action, RP6 proposed a new framework to design and develop serious games that raise security awareness, teach hands-on skills, and develop key competencies. As illustrated in Figure 1.2, the framework was built based upon the existing body of literature on gamification, situational leadership, and experiential learning. To assess this framework, we designed, developed, and evaluated an instantiation of it in RP7 to investigate whether gamification can be used to promote secure and sustainable behavior in digital ecosystems. With emphasis on practical relevance, we built a game-based model to gamify the tasks (e.g., cybersecurity resource allocation, adoption of cyber insurance, information sharing, and incident response) related to sustainable, secure behaviors. Our approach to gamifying the interactions was to metrify the tasks with additional frame mechanics and elements of play. Metrification of tasks involves incorporating a measure of attainment upon which a concept of goal-directed movement is predicated.

The results of our evaluation show significant qualitative evidence of security and sustainable behavior in terms of developed system thinking, anticipatory and problem-solving competencies. In RP7, we created and followed the game design process depicted in Figure 1.3. This process enabled us to both understand the needs of the players and formulate the training of key competencies in the game more efficiently.

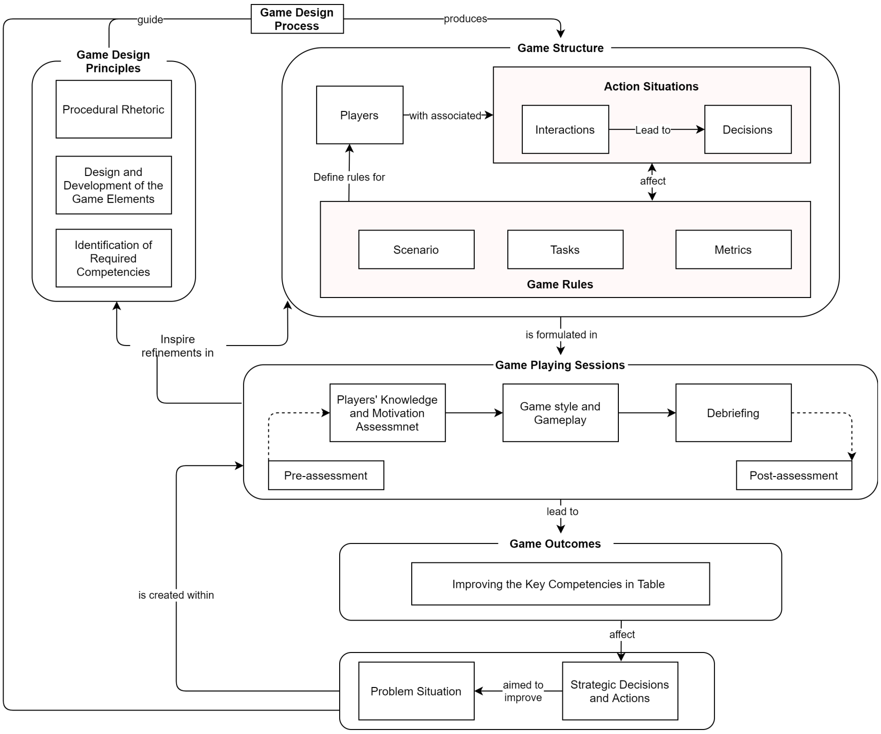


Figure 1.3: Game design process in RP7

1.5.5 Classification of the Research Papers

Previous sections highlighted how the findings of this research project contributed to answer the research questions. This section classified the research papers based on type of knowledge and levels of abstraction described in 1.4. Figure 1.4 depicts this classification. It should be noted that this figure shows no mapping between the type of knowledge and levels of abstraction. However, it illustrates the mapping of research papers to these two classifications.

- **RP1.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. 2021. "Systematically Understanding Cybersecurity Economics: A Survey" Sustainability 13, no. 24: 13677
- **RP2.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. "Multi-Paradigmatic Approaches in Cybersecurity Economics." Proceedings of the 7th Workshop on Socio-Technical Perspectives in Information Systems, October 14-15, 2021, Trento, Italy.
- **RP3.** Kianpour, Mazaher, Harald Øverby, Stewart J. Kowalski, and Christopher Frantz. "Social preferences in decision making under cybersecurity risks and uncertainties." In International Conference on Human-Computer Interaction, 2019, Florida, USA.
- **RP4.** Kianpour, Mazaher, Stewart J. Kowalski, and Harald Øverby. "Advancing the concept of cybersecurity as a public good." Simulation Modelling Practice and Theory (2022)
- **RP5.** Kianpour, Mazaher and Christopher Frantz. "Analysis of institutional design of EU cyber incidents and crises management as a complex public good." Under review in Policy Studies Journal
- **RP6.** Kianpour, Mazaher, Stewart Kowalski, Erjon Zoto, Christopher Frantz, and Harald Øverby. "Designing serious games for cyber ranges: a socio-technical approach." In 2019 IEEE European symposium on security and privacy workshops (EuroS&PW), IEEE, 2019.
- **RP7.** Kianpour, Mazaher and Stewart Kowalski "Promoting Secure and Sustianble Behavior in Digital Ecosystems Through Gamification" In Handbook of Research on Gamification Dynamics and User Experience Design, 2022.

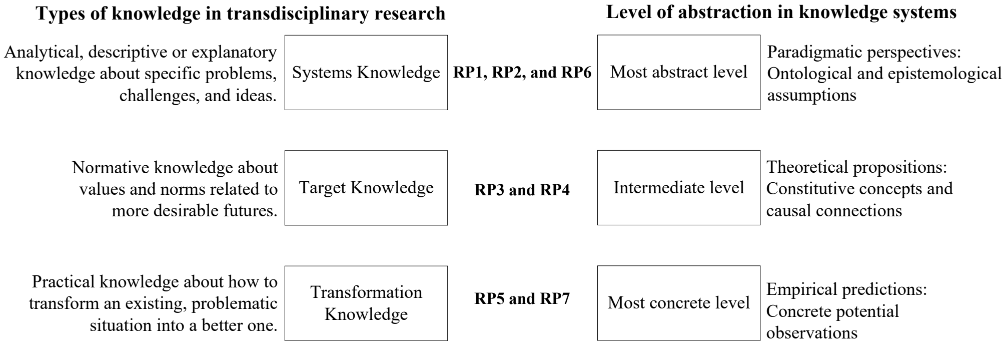

Types of knowledge in transdisciplinary research
Level of abstraction in knowledge systems
Analytical, descriptive or explanatory knowledge about specific problems, challenges, and ideas.
Systems Knowledge
RP1, RP2, and RP6
Most abstract level
Paradigmatic perspectives: Ontological and epistemological assumptions
Normative knowledge about values and norms related to more desirable futures.
Target Knowledge
RP3 and RP4
Intermediate level
Theoretical propositions: Constitutive concepts and causal connections
Practical knowledge about how to transform an existing, problematic situation into a better one.
Transformation Knowledge
RP5 and RP7
Most concrete level
Empirical predictions: Concrete potential observations

Figure 1.4: Classification of research papers based on types of knowledge and levels of abstraction.

1.6 Structure of Thesis

This thesis is structured in two parts. In the first part, after this introduction, Chapter 2 highlights the theoretical foundations of this research project. The theoretical foundations support the employed theoretical models of this project. To build the foundations, we synthesized the literature on cybersecurity economics to understand the outcomes and challenges of the scholarly research in this field. Chapter 3 represents the theoretical rationale, research approaches, and research methodology of this project. Chapter 4 concludes this part and outlines the limitations of our work and the suggestions for the future work. The second part of this thesis includes the full text of research papers listed in Section 1.5.5.

Chapter 2

Theoretical Foundations

This chapter provides an introduction to the concepts discussed in this thesis. It reiterates how we understand the intricacies of cybersecurity economics research aiming to propose sustainable cybersecurity solutions. Linking the debate of cybersecurity economics with the studies of sustainability is challenging task. Therefore, this chapter presents clear definitions of the key concepts and continues to look at how factors such as scarcity, path dependence, emotions, and paradigms play a role in this discourse.

2.1 An Introduction to Cybersecurity Economics

The study of cybersecurity economics is developing as a field of research in which it becomes essential to determine the kind and soundness of models to build in the future, to explore and observe how to implement them in practice, and to understand how these models affect the systems within which agents interact. This field is strongly motivated to explain substantive and considerable real-world phenomena in the cybersecurity area. Since there is no consensus on the definition, this research contextualizes cybersecurity economics as a field of research that offers a socio-technical perspective on economic aspects of cybersecurity to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems[1].

[1] The concept of the socio-technical systems originated with the insights of Tavistock Institute researchers in the early 1950s (68). A socio-technical system is the synergistic combination of humans, machines, environments, work activities and organisational structures and processes that comprise a given enterprise (69). A socio-technical system has two inter-related sub-systems (70):

In addition to fast changing technologies, the global system's architecture is complemented by fragmented decision-making that often leads to gaps that are still being conceptualized and understood (74, 75). Therefore, a socio-technical perspective in adoption of systematic approaches that employ multiple disciplines and methodologies is essential for understanding and managing the state of cybersecurity today, and to better achieve the goals of cybersecurity economics research. The systematic approaches identify the different units of analysis to understand the processes within such units, their interactions with other units, the dynamics defining their interconnectivity, and the resulting positive and fatal synergies of such interactions. For example, a triggering event may initiate a tipping point as this event may cross the boundary of units and what actors can accept, or this event may initiate a cascading effect that further blurs causalities between exogenous and endogenous factors. This event can either be a significant game-changing occurrence (e.g., Russian military intervention in Ukraine leading to the power grid hack in 2015), or a relatively unimportant event (e.g., the Estonian government's decision to move a Soviet memorial of World War II from its previous location in central Tallinn to a military cemetery, leading to other events such as a campaign of politically motivated cyber-attacks against Estonian governmental and commercial organizations in 2007).

Analyzing the related dynamics, synergies, and triggers is a highly complex endeavor. It requires not only a comprehensive and integrated understanding of past and present events, but also the identification and usage of adequate methodologies for context analysis, the definition of units of analysis and for data interpretation, both in terms of theories and in terms of its practical meaning and usability. Nevertheless, a shared understanding of the drivers behind one's own decisions and the decisions made by others is beneficial, especially when different actors can align their key goals, paving the way for a more collectively acceptable joint agreement. This is

the technology sub-system includes not only equipment, machines, tools and technology but also the work organisation; the social sub-system includes individuals and teams, and needs for coordination, control and boundary management. (71). An open socio-technical system can be defined as one in which there is flow ("import" and "export") and or interaction between components and the environment, resulting in the modification or evolution of system components (72). Consequently, with respect to the environment, the socio-technical perspective acknowledges that a system's success (prosperity) is affected by the way it interacts with its environment, and its evolution and responsiveness to any changing conditions. This implies that environmental factors will influence the way the system behaves, and therefore, to resolve complex issues, the dynamics between psychological, economic, technical, cultural, and political aspects need to be understood (73).

why since 2000, researchers have been employing economic models and theories to present reasoned arguments to these issues and establish argumentative frameworks for applying logic and mathematics to explain, manage, and predict complex processes within the cybersecurity domain. This stream of research introduced a new field of research known as cybersecurity economics. This field, originated by the seminal work of Ross Anderson (56) in 2001, has been fueled by many contributions over the years. Anderson convincingly argued that one solution to the problem of cybersecurity is to focus on economic and market aspects of the issue rather than only on technical protection mechanisms.

One year after this work, in 2002, Gordon and Loeb (GL) presented one of the fundamental models aiming to determine an optimal cost-benefit relation to cybersecurity investments (76). The model has been widely referenced in the academic and practitioner literature. A survey by Fedele and Roner (48) highlights that GL Model originated a stream of literature that examines firms' incentives to invest in cybersecurity using one-firm frameworks and, therefore, neglecting all forms of interdependence that can arise among firms. The predictions of this literature might not be of general applicability from a policy perspective in real-world situations in which firms operate interdependently with others. Moreover, although the GL model is considered a baseline for cost optimization in the cybersecurity, it is not able to handle dynamic ecosystems, i.e., mapping decisions and outcomes in a single period, and not considering the time factor (77).

The importance of interdependent security originated another stream of research on cybersecurity investment. Kunreuther and Heal show that firms with identical security profile in a system of interdependent security would either all invest in equal amount of protection or none at all (78). Moreover, Ogut and Menon theoretically found that the interdependency of risks reduces the firms' investment in information security to a level below optimum (79). The topic of interdependent security is not limited to the investment. It also spans over other topics such as cyber insurance (80, 81, 82). A theoretical analysis by Shim investigates the interplay between IT security investments and cyber insurance. A key finding of Shim's study is that organizations experiencing interdependent risks with different types of cyber attacks use different strategies in making IT security investment decisions and in purchasing cyber insurance policies for their information security risk management than firms that are facing independent risks (83).

As discussed in RP1, the literature of cybersecurity economics is not limited to cybersecurity investment and insurance. It also covers other issues such as information sharing (84, 85), policies and regulations (86, 87, 15), and cybercrime (88). As the literature of cybersecurity is growing, there are several surveys that have investigated some of these topics in more detail. For example, a survey by Fedele and Roner (48) has studies the theoretical literature on the firms' incentives to invest in cybersecurity. Laszka et al. presented a survey of interdependent information security games (89). Cybercrime and cyber risk information sharing are also studied in (90) and (91), respectively.

An informal look at the literature of cybersecurity economics and topics and published papers in the annual Workshop on the Economics of Information Security (WEIS)[2] suggests that this field is a synthesis between various scientific disciplines such as computer sciences, economics, system sciences, sociology, psychology, and political science. It combines knowledge from these disciplines to gain an in-depth understanding of the trade-offs and misaligned incentives in the design and deployment of socio-technical security policies and mechanisms. Trade-offs highlight the human factor in decision-making, particularly in cases that touch upon various policy goals (21). For example, trade-offs between international cooperation and sovereignty, or the trade-offs between the delay due to achieving collective consensus and timely unitary decision-making become relevant in case of cyber crises which cross the borders of countries. Without adequate tools to understand the complexity and uncertainty of these trade-offs, and without proper coordination and facilitation when managing these trade-offs, new conflicts will most likely emerge which may lead to system failures (69).

When looking at trade-offs, or other decisions which affect a range of cybersecurity issues, there are several central problems that actually matter. As Figure 2.1 illustrates, we identified these problems as scarcity, uncertainty, change, and dominance. Scarcity refers to the most basic economic problem; the gap between limited resources and theoretically limitless wants. Scarcity means that the available resources to satisfy agents' desires are too few. The shortage of skilled cybersecurity staff is one of the most well-known scarce resources. However, the list is not limited to the labour shortage. Laboratory studies in psychology indicate that attention is

[2] WEIS (`https://econinfosec.org/`) is recognized as a leading forum for interdisciplinary scholarship on information security and privacy, combining expertise from the fields of economics, social science, business, law, policy, and computer science.

also a limited resource (92, 93). In given situations, individuals selectively concentrate on some information while ignoring other perceivable information. These situations embody two main elements: our desires and the resources to fulfill those desires. In the context of cybersecurity, these desires are constantly changing, developing, and partially determined by both society and technological advances. Moreover, the resources and means we employ to fulfill desires can affect those desires. For example, self-driving vehicles can help reduce driver errors. The very innovations that aim to enhance the way we move from place to place entail cybersecurity challenges (e.g., appropriate encryption for all communications, or access control) that threaten the most sensitive assets (e.g., human life).

The second problem is uncertainty. Uncertainty refers to a situation in which outcomes are known, but there is a poor basis for assigning probabilities to these outcomes. Uncertainty is different from risk (i.e., situations in which there is moderate knowledge about calculating probabilities for different outcomes), ambiguity (i.e., situations in which there is poorly defined characterization of outcomes), and ignorance (i.e., situations that combine poor knowledge about both outcomes and likelihood) (94)[3]. When an organization invests in cybersecurity, the return on investment and cyber costs cannot be measured certainly as it depends on stochastic variables and processes that are not easy to deal with [4]. One of the important factors that makes this difficult is *the change*. Digital ecosystems are dynamic. They grow and evolve as new entities join the ecosystem, new technologies emerge, and topological structures of the system change. Changes can be:

- exogenous (e.g., regulations, political reforms),
- intended endogenous (e.g., technological innovations, reconfigura-

[3] In classical decision theory, it is common to distinguish among certainty, risk, and uncertainty. Knight (95) is credited with the distinction between risk and uncertainty. Stirling (94) goes beyond these two classes and adds two other classes: ignorance and ambiguity. While ignorance has long been recognized as a concept which is symmetrical with (and implied by) the most formal and rigorous definitions of 'risk' and 'uncertainty' in decision theory (96), Stirling argues that ignorance is a condition under which it is possible neither to resolve a discrete set of probabilities along a scale of outcomes (as is possible under risk proper), nor even to define a comprehensive set of outcomes (as under uncertainty) (97)

[4] The high degree of uncertainty and variability surrounding cost estimates for cybersecurity incidents has made the quantification of the costs difficult (98) which, therefore, has consequences for policy-makers (99). Agrafiotis et al. structured a taxonomy of the harm that can be expected to result from consequences of cyber incidents (100). This taxonomy not only includes economic harm, but it also includes physical or digital harm, psychological harm, reputational harm, and societal harm.

tion processes),

- unintended endogenous (e.g., a company becomes so over-leveraged that it can no longer make investments in cybersecurity), or/and
- changes of preferences and objectives (e.g., shifting from self-interested behavior to cooperative behavior).

Many significant changes that occur to digital ecosystems, both at the macro and micro levels, are often associated with sudden shifts in the socio-technical regimes or modes of operations. In the perspective of cybersecurity economics, examples of regime shifts include the introduction of disruptive technologies, new or modified cybersecurity regulations, policies, and laws, and changes brought by every new presidential administration. A regime shift can be anticipated to some extent. Such anticipation affects the behavior of agents prior to the actual occurrence of the shift. For example, following Brexit, many firms in UK predict new data protection regime impact their activities and operations. Some of the changes are also associated to gradual directional shifts especially one leading to a more advanced or complex form. These changes are more considered as the evolution. The growing reliance of businesses on information technologies, better cybersecurity capacity-building at local and national levels, or advancement of cyber threats to become more potent and sophisticated are several examples of evolution that cybersecurity economics studies need to capture in addition to the sudden changes.

Finally, dominance is the fourth problem that is central to cybersecurity economics. Dominance emerges because of asymmetric power relations. It occurs when actors, under conditions of complex interdependence and economic integration, are excluded from decision-making processes but not from the effects of those decisions. There are different laws that prohibits the abuse of a dominant position. For example, within the context of GDPR, data controllers that refuse to move data to another controller can be subject to Article 102 Treaty on the Functioning of the European Union (TFEU) investigations for the abuse of a dominant position. Market power (i.e., the ability of a firm to influence the price at which it sells a product or service to increase economic profit), locked-in effect (customers are dependent on a vendor for products and services, unable to use another vendor without substantial switching costs), and segmentation (i.e., there is a lack of a higher-level consensus on procedures. Instead, specific tasks are

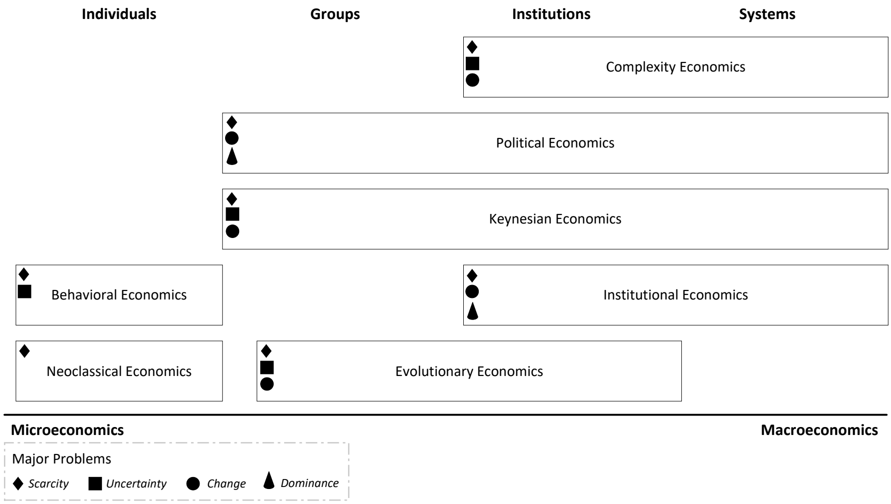


Figure 2.1: Scarcity, uncertainty, change, and dominance problems are central to different economic schools of thought. The schools can provide useful instruments to deal with these problems. Each school concerns specific level(s) of society (e.g., individuals, groups, institutions, and systems) Source: compiled by the author.

handled by particular institutions, technologies and actors) are examples of dominance.

Research in cybersecurity economics has led to suggestion of various solutions to these problems. As Figure 2.1 shows, different economic schools of thought have various instruments to address these problems and the researcher can rely on the theoretical foundations of these schools to design and develop their solutions. The figure also shows what is the most important in each perspective. For example, in behavioral economics, individuals and their motivations, relations, and actions are in focus. In institutional economics, on the other hand, systems and institutions are more important than individuals.

In some cases, the answer to problems of scarcity, uncertainty, change, and dominance from a specific perspective and school might be clear and straightforward. However, a peculiar complexity emerges when these problems are intertwined or the role of individuals, groups, institutions, or systems in the creation and development of these problems is highly interrelated. For example, accurate behavioral information of decision-makers (e.g., CEOs, CISOs, or Members of BoD) is necessary, but currently scarce, to adequately assess the impact of socio-technical regime shifts and reduce the uncertainty. Or, the way agents allocate scarce resources and how scarcity derives their interactions influence the uncertainty and dominance in the ecosystem. Research studies that do not consider or undervalue such complexities could lead to unsustainable recommendations that are not able to uphold or defend security of dynamic digital ecosystems. Therefore, turning back to our problem statement, we require praxes that can approach these problems by finding and developing societally relevant solutions and communicating the designed and created research outcome to relevant actors and authorities to be implemented in a way that brings about a significant improvement in the current situation. Hence, this research project addressees this problem within two discourses: scientific and societal.

Within the scientific discourse, we identify the challenges in the cybersecurity economics theory and practice and investigate why cybersecurity economics research has not been able to overcome these challenges. Then, we propose a set of guidelines that can approach these challenges. Societal discourse, as the other epistemic end of this process that significantly contributes to the effectiveness and sustainability of the proposed solutions, focuses on how the solutions can be embedded in social norms and institutions. The knowledge created through this process needs to be re-integrated to effectively contribute both to the solution of the initial societal problems and to scientific progress. This project explores gamification as a potential method for knowledge re-integration and to generate practice-oriented solutions to current problems of both discourses.

Referring back to the research design of this project, this chapter reflects on some of the theoretical considerations we should consider before embarking on our research project. In section 2.2, we start by describing how cybersecurity economics is distinguished with other domains including information security economics and cyber-crime economics. Next, Section 2.3 focuses on scientific practices and how the problems and challenges of cybersecurity economics research can be overcome by employing multi-paradigmatic approaches. Section 2.4 outlines the building blocks of the public goods theory and discusses how it can be applied to our research project. Finally, Section 2.5 describes how gamification can be used to promote secure and sustainable behavior in digital ecosystems.

2.2 Why not ”Information Security Economics”?

As we discussed in the previous section, cybersecurity economics is of high relevance across various issues within the context of cybersecurity. However, it is important to distinguish this field of research with information security economics and cyber-crime economics. While there are many overlaps between the former and cybersecurity economics, cyber-crime economics (a.k.a attacker economics) exposes cost-benefit analysis of attackers to exploit vulnerabilities in the security of the victim target, to subsequently formulate protective countermeasures for law-abiding entities (101, 102, 103). Moreover, cyber-crime economics focuses on understanding how cyber criminals apply security to defend their systems and operations against disruption from law enforcement (104, 105, 106), or how the specialization, commercialization, and cooperation for cyber-attacks form among the cyber criminals (107, 23). Information security economics, on the other hand, covers a significant part of the same area of interest in cybersecurity economics studies. Although the terms cybersecurity and information security are often used as though they mean the same thing, they are different, have a different purpose and should be addressed separately (108). Hence, this next section highlights the differences between information security economics and cybersecurity economics.

This study distinguishes the terms "cybersecurity" and "information security" by what they specifically protect. According to NIST, Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Cybersecurity, on the other hand, is the ability to protect or defend the use of cyberspace from cyber-attacks. As a result, in cybersecurity, the assets that need to be protected extend beyond the the information per se as defined for information security. In cybersecurity, assets include the personal or physical aspects, both tangible and intangible, of a human being, societies, and governments. For example, the patients data is stored in information systems. Protection of the devices and systems used to store, manage, and transfer those data that are important to ensure patients safety should be considered part of cybersecurity.

The seminal work by Ross Anderson in 2001 initially explored the ties between economics and information security (56). Then, various economic models were constructed to analyze the optimal investment in information security (76), the externalities (109), and information asymmetries (110). However, the literature has little to say about how the differences in definitions and conceptions of "cybersecurity" and "information security" make differences in articulation and development of these models to deal with cybersecurity threats and risks. These differences have important implications for the policies, practices, and procedures that emerge as a result. And since these differences stem from the assets that are being protected by these policies have different values, it is important that the studies in this field determine the domain and provide a contextual definition, based on one that is relevant and fits. ENISA surveys a number of definitions for both information security and cybersecurity (111). Additionally, it is common that National Cybersecurity Strategies provide a definition of cybersecurity in their documents to avoid vagueness in their plan of actions. For example, the UK National Cybersecurity Strategy (112) defines cybersecurity a the protection of information systems, the data on them, and the services the provide, form unauthorized access, harm or misuse. This includes harm caused internationally by the operator of the system, or accidentally, as a result of failing to follow security procedures. This a succinct definition and this project relies on it as it expresses the breaths of coverage within the topic of our research.

In this thesis we focus on cybersecurity economics for several reasons: 1) cybersecurity goes beyond the boundaries of information security (108), 2) cybersecurity concerns a societal context whereas information security would appear to be cultivated in organizational context (113), 3) As digitalization continues to proliferate and new technologies are introduced infrastructure breakdown due to a cyber-attack has become a major concern of decision-makers, and 4) cybersecurity contributes to overall governance of information, systems, enterprises, and other entities including the states, private entities, and critical infrastructure providers (114). As a result, cybersecurity economics covers a broader range of topics than market challenges (e.i., externalities, information asymmetry, and incentives). Cybersecurity economics research involves the description, explanation, prediction and control of complex interplay among issues, actors, structures, processes, and outcomes over time and at different levels. Cybersecurity economics research is thought to ensure that it copes better with the dynamism, uncertainty, complexity of digital ecosystems than information security economics. Cybersecurity economics research enables governance processes that learn more easily from changing circumstance and empowers decision-makers by enhancing their capacity to resolve challenges and promote secure and sustainable digital innovations.

Yet, despite the promise of these functionalities, it is uncertain whether they can be achieved in practice. As we discussed in Chapter 1, cybersecurity economics research has faced a series of challenges that has hindered an inclusive development within this field of research as well as prosperity in society at large. RP1 highlights five categories of these challenges: complexity, assumptions, unobservable variables (e.g., expectations, beliefs, and psychometrics), the tension between rigor and relevance in suggested solutions, and parameter identification in construction of models using econometrics. Considerable empirical and theoretical research is still required to tackle these challenges as the practical outcomes are what will determine successful cybersecurity economics studies to be impactful. Nevertheless, the next section will suggest that the first step to tackle these challenges is to rethink the basic assumptions about how the world is perceived, understood and explained.

2.3 Multi-paradigmatic research on cybersecurity economics

One particularly fruitful area of research regarding the aforementioned issues, and other general issues within the domain of cybersecurity, has focused on work that challenges the dominant approaches, perspectives, and paradigms in cybersecurity. Such challenges have taken the form of critiques of existing practice as well as novel, sometimes controversial, approaches. Studies such as (115, 116, 117, 118) propose new security paradigms, or ways to shift the existing paradigms as they provide objective facts that present anomalies implying the research on cybersecurity has not been able to provide a good explanation for real-world phenomena. For example, Spring et al. (115) focus on the question "why is this scientific process producing unsatisfactory results" from a philosophy of science perspective. They put forward that cybersecurity is a science with its own unique challenges. Cybersecurity must learn from challenges common with other sciences while at the same time pushing forward with novel solutions to those challenges and approaches in fact unique to cybersecurity.

Other studies argue that to respond the anomalies we need to shift our research paradigms (117, 118). The concept of paradigm shift has become a cliché with many meanings, including the several meanings of the word “paradigm” as used by Kuhn in his original publication. While the introduction of new technologies, including Internet and Artificial Intelligence, has created paradigm shift in the way business is conducted or research is directed (119), the discourse on paradigm shift has been incoherent in economics and social science literature because of the different uses of the term and the different levels of sophistication in its application (120). Moreover, there are three elements required for a paradigm shift: 1) a dominant paradigm in the discipline studied, 2) crisis-inducing anomalies, 3) an alternative paradigm to solve the alternatives. The first element is evident: for a paradigm shift to occur requires a paradigm to exist. To our knowledge, since 2000, no scholar has speculated about whether there is a dominant paradigm in cybersecurity or information security economics. It has been observed that cybersecurity economics is in a pre-paradigmatic phase which is a typical of emergent fields (121), as there is a multiplicity of schools of economic thought such as neoclassical economics, behavioral economics, and evolutionary economics, employed in individual studies.

The second and third elements addresses the crisis-inducing anomalies which must be accompanied by an alternative paradigm. It means that in case of presence of such anomalies, the dominant paradigm will be called into question by the research community only if another solution exists. The alternative paradigm must solve both previously observed phenomena and the anomalies to prosper. We have not found any study which has explored such alternatives as well. Therefore, at this stage of maturity, it is clear that cybersecurity economics research can benefit from multi-paradigmatic approaches by confronting multiple paradigms rather than ignoring them. Such approaches allow researchers to gain richer knowledge on a given subject and improve the predictability of outcomes (122, 123, 124). In Section 3.1, we discuss how this approach is employed to advance the concept of cybersecurity as a public good. The next section presents the theoretical foundation of this concept in more detail.

2.4 Cybersecurity as a Public Good

The major objective of this thesis is to provide theoretical and practical knowledge on how the solutions proposed by cybersecurity economics research can be embedded in social norms and institutions to promote secure behavior in digital ecosystems. As we mentioned in Section 2.1, over the last several years, incentives (misaligned or perverse), externalities (negative or positive), and asymmetries (information or power) (125, 86, 110, 126) have been known as practical challenges in implementation of solutions proposed within cybersecurity economics research. This project supports the notion of cybersecurity as a public good to help reduce deal with challenges from a collective point of view, as well as lead to the creation of methodologies to ultimately integrate cybersecurity economics solutions into social norms and institutions. This section will describe the concept of public goods. Then, a recent literature review of providing cybersecurity through a public goods perspective is offered in Section . Section and discuss two concepts of social preferences and polycentric governance structure. These two concepts are central to our research project as they are incorporated to our basic agent-based model to advance the concept of cybersecurity as a public good.

2.4.1 An Introduction to Public Goods Theory

In economics, goods are items, including objects and services, that satisfy human wants and provide utility (127). In contrast to free goods, economic goods have a degree of scarcity and therefore an opportunity cost to society. That is to say, agents value an economic good and are willing to pay for it. An individual, organization, or a government values cybersecurity and pays for it because they expect their utility increase by utilizing it. They do not pay for cybersecurity per se. They might be willing to pay more for products or services that are provided with top ranked companies and vendors. Rosenzweig argues that cybersecurity is not a singular good. Rather it is a bundle of various goods, some of which operate independently and others of which act only in combination (128).

Economic goods, hereafter just goods, can be classified into different categories based on distinctive characteristics, such as tangibility, relative elasticity, or exclusivity and competitiveness. In this research, we focus on the latter classification. Goods can be classified based on their degree of excludability and rivalry (competitiveness). These two characteristics are defined as (129):

- Excludability is defined as the degree to which a good, service or resource can be limited to only paying customers, or conversely, the degree to which a supplier, producer or other managing body (e.g. a government) can prevent consumption of a good.
- A good is said to be rivalrous or a rival if its consumption by one consumer prevents simultaneous consumption by other consumers, or if consumption by one agent reduces the ability of another agent to consume it.

Table 2.1: Typology of economic goods with general and cybersecurity-related examples

	Rivalrous	**Non-rivalrous**
Excludable	Private goods *(cars, houses, purchased network firewall)*	Club goods *(museum, cable television network, anomaly detection methods at NTNU)*
Non-excludable	Common Goods *(fish in ocean, national forest, Norwegian Cyber Range)*	Public goods *(national defense, country's financial stability, cyber incidents and crises management in the European Union)*

According to the degree of excludability and rivalry, there are four types of goods. Table 2.1 shows the typology of economic goods and two general examples of each type and one example within the context of cybersecurity. According to this typology, many security systems such as intrusion prevention systems and network firewalls in a firm are private goods. A private good is thus any item that can only be used or consumed by one party at a time. The majority of private goods must be purchased for a cost. Purchasing the item secures the right to consume it and compensates the producer for the costs involved in making it. It also gives you the right to prevent the use of the good by another. However, there are other aspects of cybersecurity, such as threat intelligence and vulnerability information sharing, collective response to cyber-attacks, integrity of elections, systems robustness, and critical infrastructure protection, that have the characteristics of public goods (130, 131)[5]. It is important to note that the public effects of a good can be local, national, regional, worldwide and cross-generational. For example, global public goods are goods of which benefits or costs are of nearly universal reach or potentially affect anyone anywhere (133). The EU's cyber incidents response and crises management is also

[5] As discussed by Colander (132), in reality there is no such thing as a pure public good. Moreover, what is and is not considered a public good depends on technology. For example, radio signals were previously classified as public goods because it was technologically impossible to exclude listeners, but when encoded satellite broadcasting was developed, exclusion became relatively easy.

considered as a regional public good which is provided with some form of public assistance (e.g. directives or other mandates).

In both academic and nonacademic discussions, people often confuse the common good with a public good or a set of public goods. But it is important to keep the two types distinct. Common goods are rivalrous. For example fish in seas. Seas are common resources; no one owns them, and whenever people catch fish, they reduce the number of fish that others can catch. The results will likely be overfishing which is known as the tragedy of commons. Norwegian Cyber Range is also a common good according to political discourse. In this discourse "common good" refers to those facilities—whether material, cultural or institutional—that the members of a community provide to all members in order to fulfill a relational obligation they all have to care for certain interests that they have in common (134). Although the benefits of NCR can be enjoyed by all members of society, it is not a public good as it owns limited resources (it is rivalrous) and it may not be a net benefit for each member of the community. The facilities that make up the common good serve a special class of interests that all citizens have in common, i.e., testing, training and practice within cybersecurity.

We emphasize that considering all aspects of cybersecurity as public goods may not be justified by both scientific and societal actors. For example, an organization (e.g., NTNU) employs highly advanced methods and products to detect anomalies in its network. Now the connection to this network for authenticated and authorized people has been recast into a club good. In some cases, provision of a good as a public good might be inefficient. For example, Moore argues that cybersecurity research data is a club good, and often provisioned as a public good (135). When this happens, research data becomes undervalued and under-provisioned, unless an entity is willing to underwrite the cost to society's benefit. In the absence of a benefactor, one could restrict access to those who are willing to pay for it. But this is problematic, since most researchers work in academic or other non-profit settings.

Accurate production and provision of public goods compared to the level that would be best for society is the main challenge of policy makers (136). Consumption of a public good by an end-user does not necessarily have to be free of charge, however, it is essential that its costs do not become a discriminating factor, and consequently, determining access and use of it (137). Some public goods are best created by direct government provisioning, while other may be best created by the all beneficiaries as a participatory public good. Participatory public goods are created best by changing individuals and organizations' incentives through different policies and regulations. For example, there are many reasons (e.g., risk of loss of reputation and trust, liability, negative effects on financial markets, and signals of weakness to adversaries (138)) why an organization may be reluctant to share information threats and vulnerabilities in its systems. Treating such information as a public good tends to overcome these issues.

Due to the established description of public goods, referring to two specific characteristics of non-excludability and non-rivalrous, public goods, along with information asymmetry, incomplete markets and so on, have been regarded as trouble-makers that cause market failures and provoke severe shortfalls of collective actions (139, 140). Several theorists argue that in order to prevent inefficiency and market failures, public goods need to be substituted by private goods (141, 142). In this project, we also recognize these problems. However, we portray public goods in a different lights. Public goods are beneficial as they allow for all members of society to have access to certain essential goods and services they otherwise might not have been able to access if they were not public goods. Due to their specific properties, public goods produce a range of positive side effects on society. Such goods support social inclusion, they generate the public, and they develop and strengthen a shared sense of responsibilities. Following a recent assessment of public goods in political philosophy, public goods are particularly suitable for sustaining a well-ordered society (143).

The public goods theory - as we sketch out in this section and as the contributions to RP3, RP4, and RP5 attest - offers a rich set of tools for assessing goals, identifying incentive structures, analyzing cooperation problems and specifying institutional solutions surrounding certain functions of cybersecurity, such as cyber incidents response and crises management, information sharing, and critical infrastructure protection, that are of high significance to security and sustainability of our societies. In our view, this theoretical approach can spur additional research into the field of cybersecurity economics and lead to a accumulation of insights into local, national, and international cooperation dynamics in provision of cybersecurity.

2.4.2 A Review on the Previous Arguments

The necessity for public–private collaboration, multifaceted strategies, and recognition of the significant role that industry plays in securing the information networks have been the fundamental notions of approaches to cybersecurity in the past decade (144, 145). However, with the raise of dependencies on critical infrastructures and increasing concerns about the consequences of possible cyber-physical incidents, many governments and super-national organizations like European Union (EU) are concerned with the possible failure of the private sector in delivering acceptable level of security in the society without governmental intervention (146, 147). This shift of the concept has lead to the proposals which suggest that cybersecurity needs to be treated as a public good.

Taddeo argues that considering cybersecurity as a public good will be a step in the right direction to support policy and governance approaches that will foster robust, open, pluralistic, and stable information societies (131). She elaborates managing cybersecurity as a public good brings the advantages of systemic approaches to security, shared responsibilities among different stakeholders; and facilitation of collaboration. Asllani et al. also explores the role of establishing an appropriate legal, social, and ethical framework to enhance cybersecurity (148). Asllani et al. compare the cybersecurity with safety and conclude that financing of cybersecurity by taxes justifies the significant role of governments in enhancing cybersecurity. Comparison of cybersecurity with other public goods is not limited to public safety and other researchers also compared it with public health. Sedenberg and Mulligan evaluated different cybersecurity information sharing proposals leaning on the analogous public good-oriented field of public health, and proposed some recommendations to orient cybersecurity policies towards adopting the doctrine of public cybersecurity (149).

The studies by McCarthy (150), Assaf (151), and Shore et al. (152) also discuss that cybersecurity appears to have the character of a public good. These studies question rational choice approaches and classic solutions that suggest public goods should be provided by the governments to avoid market failures. However, the incapability of the governments in providing the public good of cybersecurity on their own is also supported by (153). Hence, they propose solutions based on public-private partnerships to overcome the problems of treating cybersecurity as a public good. The effectiveness of these solutions has been the focus of analyses such as (154, 155, 156). The concern of these analyses is determining institutional forms, policy processes, and levels of government intervention through which partnerships can most effectively provide cybersecurity. Drawing from this interdisciplinary literature, Shackelford used the concept of polycentric governance to describe how cybersecurity as a public good should be regulated (157).

Reviewing the literature shows that there are different arguments favoring treating cybersecurity as a public good. There are also several studies that have incorporated this perspective in their game-theoretical analyses that capture essential characteristics of decision-making to protect assets withing an environment. Bauer and Eeten argue that cybersecurity has strong public good characteristics, although it is mostly provided by private stakeholders at a cost (86). Varian's exposition supports this argument. Varian observed that the success of reliability (as a critical component of security) decision-making depends on joint protection by all the agents in a network (158). Moreover, he posits that the computation of the protection level will often take the form of a public good contribution function with non-excludable and non-rival benefits or consequences. As a result, individuals may be able to free-ride on others' efforts or suffer from inadequate protection efforts by those members that have a decisive impact on the overall protection level in the environment.

Grossklags et al. continue Varian's work by adding another action available to the individuals. They can decide to self-insure themselves from harm. Consequently, the security games developed by Grossklags et al. consider share qualities of private (on the insurance side) and public (on the protection side) goods (159). Johnson et al. extend these security games by modeling network security investments that account for the choice between the hybrid goods of collective protection and individual mitigation and externally provided market insurance. Their study shows that several equilibria with full market insurance exist and, consequently, market insurance has a place in security games (160).

Unlike (159) and (160), we assume only public components have a constant marginal impact across the range of investment opportunities. Therefore, in RP4, individual agents decide strategically on how their security investment reduces the probability mass in the loss distribution function of all agents. Furthermore, their works look at the homogeneous population of fully rational agents with perfect information. Therefore, our work adds to the research literature by 1) considering the heterogeneous population of agents[6], where every agent has a different utility function, 2) exploring the

[6] As mentioned in RP3, the area of cybersecurity in organizations involves heterogeneous interacting, and in some cases, competitive and even adversarial,actors that are characterized by distinct

impact of decentralized punishment under a polycentric governance structure, and 3) featuring bounded rationality under uncertainty concepts.

Research paper RP4 attempts to quantitatively analyze whether the context of cybersecurity complies with this theory, and employing this theory maintains the robustness and resilience of such a dynamic and stochastic environment in presence of various externalities. The study develops a model that addresses the interdependence among the agents and captures the impact of social preferences and punishment on their average contribution to enhancing their cybersecurity posture. Cybersecurity posture is used to describe the cybersecurity capabilities of a country, organization, or business and collective efforts to protect its assets. It refers to the overall defense mechanisms in place to tackle malicious cyber activities. This metric relates to any kind of security measure, including policies, staff training, and intrusion prevention systems. In the model constructed in RP4, we assess the cybersecurity posture of the organizations by the number of failed attacks against them and their resources after each period.

As Section 2.3 put forward that cybersecurity economics research can adopt positions that incorporate different paradigms within research approach and research design, we applied two paradigms of constructivism and critical realism to determine how various human constructs, social structures, and institutional arrangements contributed to observable and unobservable events and actions in the ecosystem where cybersecurity is treated as a public good. As we discussed in Section 2.4.3, through consctructivist and critical realist we incorporated social preferences and polycentric governance structure in the constructed model in RP4. Sections 2.4.3 and 2.4.4 will briefly describe these two concepts, respectively.

2.4.3 Social Preferences

Neo-classical economics is built on the assumption that all people are entirely self-interested and do not care about the well-being of others (161). However, the self-interested hypothesis has come into question by other schools of thought such as behavioral economics (162) and evolutionary economics (163, 164). This hypothesis may be true for some, but it is certainly not true for all. A purely self-interested person refuses to contribute anything to the provision of public good and free rides on the contribu-

local cultures, structure, machines, and methods. Due to interdependencies among these actors, complex environments, and presence of adversaries, outcomes rely on strategic decision-making of all agents by taking past actions, potential future actions, and outcomes of other actors into account.

tion of others (165). Other-regarding individuals, on the other side, exhibit prosocial behavior when they do not always make choices that maximize their own pecuniary payoffs (166). They often act pro-socially, contribute to public goods, and engage in pro-environmental behavior, even if this imposes costs on them. The possibility that some individuals exhibit ‘social preferences’ (i.e., fairness concerns, reciprocity, and even pure altruism) has gained a more general acceptance among economists. The study represented in RP3 shows that these preferences also have a moderating effect on the decisions within the context of cybersecurity.

In RP3, we employed structural equation modeling (SEM) to model the relationships among multiple observable and latent variables[7]. There are two approaches to estimating SEM parameters: covariance-based or variance-based (167). Both approaches are similar, however, the covariance-based approach is more suited for confirmatory theory testing and the variance-based approach rather for theory development (168). We use the variance-based approach, here and in the following just referred to as Partial Least Squares (PLS), because it is widely used for predictive analysis and is an appropriate technique for theory development as done in this study. This method is furthermore applicable even under conditions of a very small sample size. Chin and Newsted indicated that PLS can be performed with a sample size as low as 50 (169). Figure 2.2 shows our conceptual research model in RP3. The latent variables in this model are represented by more than one observable variable. Each observable variable is corresponded to a question in our questionnaire. For example, Altruistic Punishment is corresponded to the question below:

How likely is your organization to take retaliatory action against your third parties that cause a data breach or misuse of other organizations’ sensitive and confidential information? (even if there may be costs for you).

Depending on the research objectives, conducting PLS may vary. In RP3, our main objective is to investigate whether social preferences have a moderating effect on willingness to cooperate. We differentiate between two often-confused functions of variables: Moderation and Mediation (171). A moderator is a variable that affects the strength and direction of the relation between the independent and dependent variables. A mediator, however, explains the process through which two variables are related[8]. Along with

[7] Opposed to observable variables, latent variables are not directly observed but are rather inferred through a mathematical model from other variables that are observed.

[8] In practice, the relationships between the independent variable, mediator, and dependent vari-

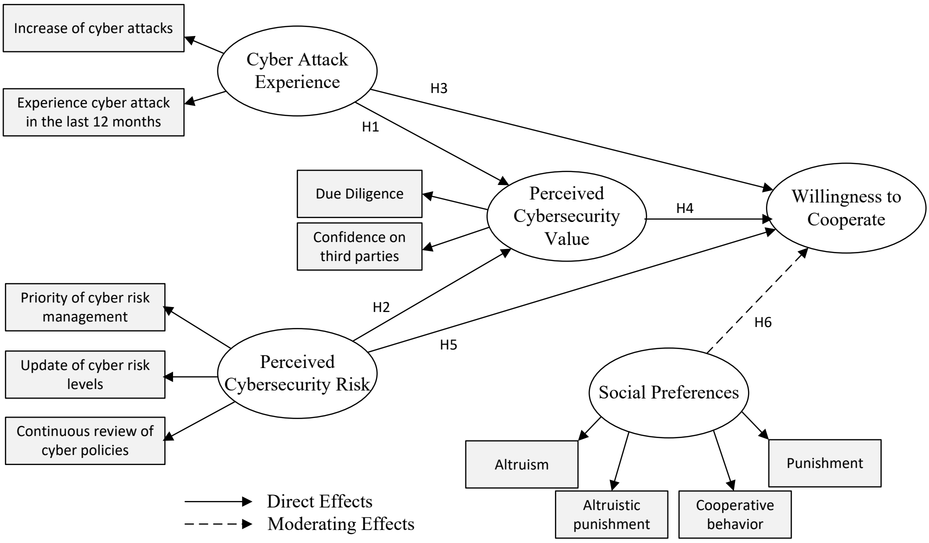

Increase of cyber attacks
Experience cyber attack in the last 12 months
Cyber Attack Experience
H3
H1
Due Diligence
Confidence on third parties
Perceived Cybersecurity Value
H4
Willingness to Cooperate
Priority of cyber risk management
Update of cyber risk levels
Continuous review of cyber policies
H2
H5
H6
Perceived Cybersecurity Risk
Social Preferences
Altruism
Altruistic punishment
Cooperative behavior
Punishment
Direct Effects
Moderating Effects

Figure 2.2: The research model in RP3. The latent variables (ovals) are represented by several observable variables (rectangles). The path coefficients (estimated structural parameters) are not calculated as it was beyond our research objectives. The path coefficient represents the response of the dependent variable to a unit change in an explanatory variable when other variables in the model are held constant (170). You can find the hypotheses (H) in RP3.

the main objective, RP3 also investigated the mediating effect of perceived value of cybersecurity.

A survey instrument was developed in order to test the research model. Initially, the measurement items were reviewed by two cybersecurity professional experts and two researchers within the field of cybersecurity who were asked to comment on the appropriateness of the research constructs. Based on the assessment from the experts and researchers, redundant and ambiguous items were either changed or eliminated. New items were finally accepted and included in the questionnaire. Hence, the content validity of the survey instrument was considered as appropriate. The questionnaires along with a covering letter mentioning objectives of the study and definition of of several terms were sent to various persons of government and private organizations dealing with cybersecurity. The specific sampling strategy was stratified random sampling. The main reasons for using a specific sampling strategy were to increase the precision in research and to reduce the sample variation and error (173). The results of this research supported the mediating effect of cybersecurity perceived value and moderating effect of social preference on willingness to cooperate. According to the these results, although decision-maker's attitude is towards cooperation in the context of cybersecurity, cybersecurity concerns cause they delay or ignore cooperation with other organizations. This implication is aligned with the findings of Olsson et al. which show despite being willing to share information with each other regarding vulnerabilities, however, the firms are less inclined to proactively sharing vulnerability information (174). Finally, we measured the social preferences of the respondents by operationalization of Social Value Orientation framework proposed by Murphy et al. (175). Figure 2.3 shows the distribution of social preferences in our sample (shifted toward cooperative behavior).

The results of RP3 shows that the actors' preferences and perceptions matter. Hence, understanding how preferences change and how social norms and institutions could be designed to facilitate and incentivize actors to provide cybersecurity as a public good is a key aspect that this thesis emphasizes. The concepts of social norms and institutions are important to the explanation of cooperation and prosocial behavior. Ostrom defined

able are not tested for causality, just a correlational relationship. The idea is that although the fit of a latent variable model to the data may not prove the existence of causally operating latent variables, the model does formulate this as a hypothesis; consequently, the fit of such models can be adduced as evidence supporting this hypothesis (172).

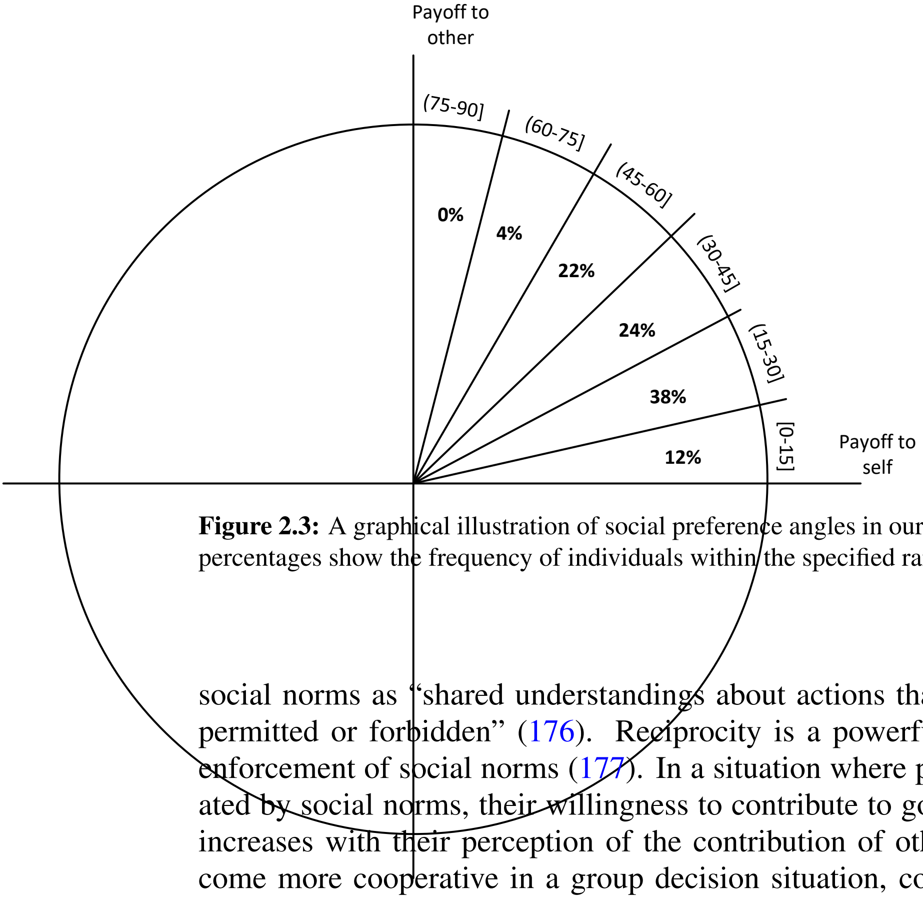


Figure 2.3: A graphical illustration of social preference angles in our sample in RP3. The percentages show the frequency of individuals within the specified range.

social norms as “shared understandings about actions that are obligatory, permitted or forbidden” (176). Reciprocity is a powerful device for the enforcement of social norms (177). In a situation where people are motivated by social norms, their willingness to contribute to good social causes increases with their perception of the contribution of others. People become more cooperative in a group decision situation, compared to when acting as individual decision-makers (178). Moreover, this research project stresses that cybersecurity economics solutions need to be embedded in social norms and institutions because norms emerge not from a collective need but from the decentralized interaction of actors according to their own interests (179). To govern these interactions, institutional structures are formed to make social priorities, resolve conflicts and facilitate coordination. Polycentricity is a concept that describes a complex form of governance with multiple centers of decision-making, each of which operates with some degree of autonomy. Governance arrangements exhibiting polycentric characteristics may be capable of striking a balance between centralized and decentralized governance (180). The agent-based model in RP4 is an implementation of a polycentric governance system in which autonomous agents take others into account through processes of cooperation and competition. The next section describes the polycentric governance structure in more detail.

2.4.4 Polycentricity

Polycentric governance systems refer to structural arrangements of governments that have multiple and overlapping, semi-autonomous centers of authority or decision-making, within a shared system of rules (181, 182, 183). Authority refers to the power to influence a governance system either directly or indirectly. Depending on the governance system, a center of authority refers to government or non-government entities that have some degree of authority to influence politics or policy. The overlapping centers of authority take each other into account through cooperation, conflict resolution or competition. This idea of overlap indicates that more than one decision-maker, whether at horizontal levels (i.e., authorities on the same hierarchical level within or across organizations) or at vertical levels (i.e., across different hierarchy levels), has authority over a shared governance issue which may affect the ability to solve common problems efficiently. Solutions may involve working through existing centers of authority or establishing new entities with the power to effectively address these problems in ways befitting their scope and complexity.

Several studies by Shackelford showed that cybersecurity can be regulated under a polycentric structure (157, 184). He argues that since cybersecurity comprises the processes, practices, and technologies built to protect networks, devices, programs, and data from attacks, actors engaged in its provision aspire to equitably share the benefits and costs of activities affecting each of them while also reducing potential risks that could befall any or all of them. Moreover, the results in RP4 showed that a polycentric governance structure can lead to persistent behavior that secures a resilient environment in which all the agents are interacting. Research paper RP5 therefore explores to what extend this structure is established in the European Union within the context of cyber incidents and crises management. The study employed Institutional Grammar 2.0 to code four cybersecurity policies that include EU-wide rules and regulations on cyber incidents and crises management. Our analysis revealed that EU has established a polycentric structure within this context. However, coordination mechanisms such as signaling of commitment or punishment of non-contributors and free-riders remained nascent in this context. These mechanisms are critical to for channeling the power dynamics, sustainability of the systematic governance structures, and better fitting the complexity of socio-technical problems.

Various advantages, such as enhancement of innovation, learning, adaptation, trustworthiness, levels of cooperation of participants, and the achievement of more effective, equitable, and sustainable outcomes at multiple scales, have been suggested for polycentric systems (182, 185). Surveying existing work, we have gathered the following list of potentially positive benefits from operating under a polycentric governance structure. Although the presence of collective action problems, including conflict among agents and free-riding, often sets high barriers to effectively creating a secure and sustainable environment, relying on these advantages and our findings in RP4, this research project suggests that polycentric governance structure has the potential to empower actors to achieve such sustainability and deal with collective action problems effectively.

- Recognizing the capabilities of dependent and independent stakeholders to govern themselves demonstrates the viability of bottom-up alternatives to the regulatory agencies (186).
- Ensuring balance between decision-making centers so as to prevent dominance of certain centers (187)
- Emergence of flexible and organized patterns of interaction and outcomes (188)
- Resilience of these patterns to shocks and changing circumstances (189)
- Effective production and provision of public goods which may not require systems-level coordination (190)
- Generation and sustainability of policy recommendations for better resource utilization are consistent with the local circumstances (186)
- Provision of a secure foundation for the sustainable realization of heterogeneous value systems found in multicultural societies (191)

2.5 Gamification as a method of knowledge re-integration

Achieving the objective of this research project and a societal transformation toward sustainable solutions within cybersecurity economics requires re-integration of generated knowledge in both scientific and societal discourses. Since researchers may perceive and study problems differently from involved stakeholders, who need applicable knowledge as a basis for decision-making, we rely on participatory approaches to re-integrate knowledge, close the gaps, and communicate the designed and created research outcomes to relevant actors. In this research project, we used gamification as a participatory approach 1) to identify practitioners' needs, disentangle their problems, and gather a comprehensive understanding of the problem context, and 2) to enable, engage, and empower them to contribute to actively implement the solutions proposed within the scientific practices.

According to (192), there are three levels of participation: enabling, engaging, and empowering. Although engagement has been extensively investigated in the literature of gamification (193, 194), research remains scarce with regards to the empowering and enabling (195). Enabling is about providing relevant information in a format that is both more accessible and more understandable to the participants. This level ensures that gamification tools enable informed engagement rather than engagement void of reliance on evidence or information. Empowering is concerned with supporting active participation and facilitating bottom-up ideas to influence the rules, agendas, and settings. Without enabling and empowering, top-down and bottom-up implementations would remain hard to emerge or facilitated.

Games are complex socio-technological artifacts that are hard to define (196). Playing games has been associated with several cognitive, emotional, motivational and social benefits (197). Cybersecurity games are increasingly employed to test, challenge, and develop both cybersecurity skills (198, 199) and decision-making skills (200). As a part of cybersecurity exercises and competitions, games can be used as a basis for experimentation in the security field (201). Brynielsson et al. discuss that games can be employed in the cyber domain to measure actual levels of cyber situation awareness (202). They, following the criteria proposed by Raser (203) for the validity of gaming as a research tool (psychological reality, structural validity, process validity, and predictive validity), proposed a methodology to set up cyber situation awareness measurement experiments within the context of simulated cyber defence exercises.

Referring back to our discussion on social preferences, studies by Ewoldsen et al. (204) and Gentile et al. (205) show that gamification enhances the acquisition of prosocial and interpersonal skills that often facilitate group and prosocial activities. Taking advantage of these benefits, this project focuses on policy games. The policy games bridge games and governance and looks into how simulation games can assist in policy planning and better organizational decision-making (206). The rationale is that policy games make engagement with said process fun for players as well as expand their horizons of policy-making by allowing them to think about different possibilities in the relatively safe and inconsequential space of play. RP6 proposes a socio-technical framework to design and develop games with the aim of motivating beneficial behaviors. An instantiation of this framework is developed and evaluated in RP7. In this research paper, we used concept maps drawn by players before and after playing the game. A concept map displays a person's representation of concepts or processes about a particular domain, showing the relationships, flows, and dynamics among them (207). We evaluated concept maps based on a method initially developed by Morine-Dershimer (208).

In Morine-Dershimer's method, the researcher asks the respondent to generate a list of concepts related to a major topic. The major topic is placed in the center, and then other concepts are placed around it, with unnamed links radiating out to them, and from them, to other concepts in turn (208). This method relies on two principles, (1) centrality – the proximity of concepts to the core of the map, which can be taken as an indicator of how important they are in the perception of the player and (2) specificity – the extent of detail with which a concept is worked out in subordinate branches. Based on elements identified on the concept maps, a set of categories was developed to describe responses. In this study, we categorized the responses into six main categories and 22 sub-categories. Subsequently, for each category on every map, scores for centrality and degree of specificity were calculated. Centrality scores were calculated based on the level at which the category first appeared on the concept map, relative to the map core. For example, if a concept was linked directly to the core, its centrality score was 1. If another concept first appeared in a reference connected to the first concept, its centrality score was 2, and so on. Specificity scores were calculated based on the relative frequency of items associated with one category – the number of items falling under a specific category was divided by the total number of items on the map. For instance, for a map with a total of 10 items, three of which were coded as belonging to the category "design", the degree of specificity for this category on this map was 0.3.

A comparison of shifts in the centrality and specificity of concepts from the pre- to the post-measurements allows tracing changes in the structuring of knowledge or a new prioritisation of certain aspects. Figure 2.4 illustrates

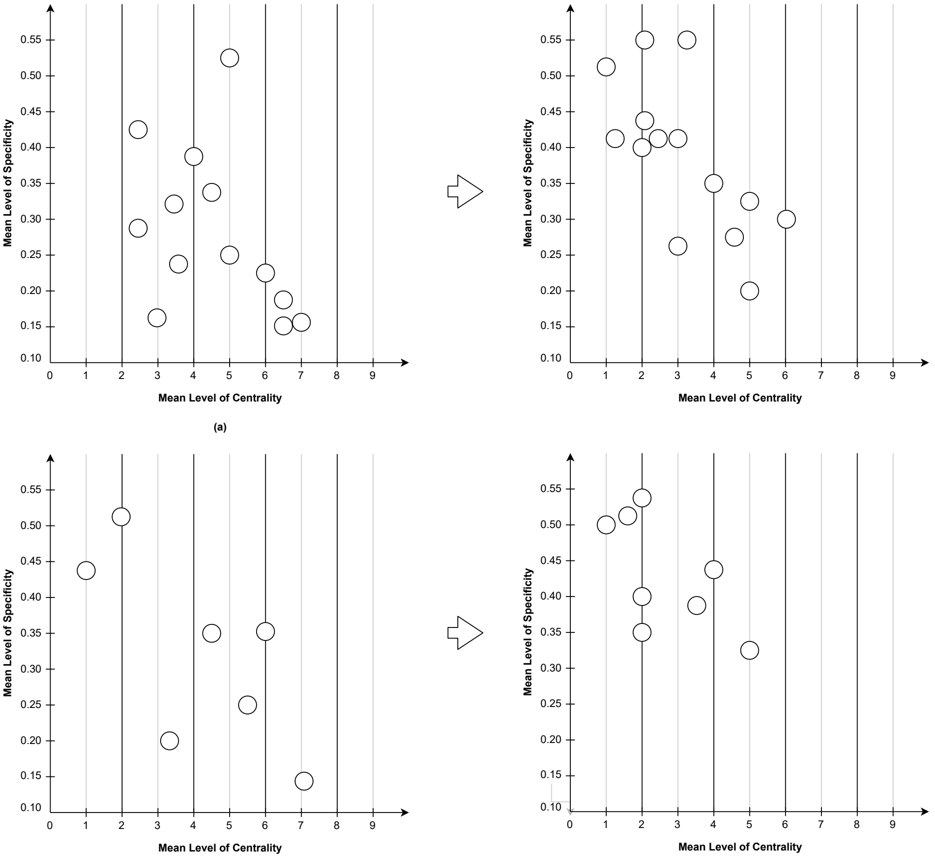


Figure 2.4: Patterns of centrality and specificity on players' pre- and post concept maps. (a) and (b) are pre-maps; (c) and (d) are post-maps.

players' pre and post concept maps emphases on the 22 sub-categories. You can find these sub-categories and our analysis of this evaluation in RP7. The results of evaluation shows that gamification aids with the active analysis, implementation and monitoring of decisions and development of key competencies to advance secure and sustainable behavior in digital ecosystems (e.g., system thinking, anticipatory competency, and problem-solving competency).

Chapter 3

Research Methodology

Section 1.4 described the research strategy of this project using the transdisciplinary research framework. This chapter presents our theoretical perspectives, research approach, research methodology, and tactics employed to answer the research questions of the thesis within the Phase B of the framework.

3.1 Theoretical rationale

To adopt a theoretical rationale is to adopt a way of looking at the world and making sense of it. Theoretical rationales are most often referred as research paradigms. Paradigms are universally recognized scientific achievements that, for a time, provide model problems and solutions for a community of practitioners. Each paradigm generates and develops theories, concepts, and means of experimentation, instrumentation, and equipment which are different from those of other paradigms (209). While research methods are systematic tools used to find, collect, analyze, and interpret information, paradigms determine how members of research communities view both the phenomena their particular community studies and the research methods that should be employed to study those phenomena. For example, dealing with only what may be measured or qualified, or subjectively ignoring social and political contexts of cybersecurity produces different, and sometimes incompatible, results which causes perplexity.

RP2 and Section 2.3 argue that adoption of multi-paradigmatic approaches empowers the researchers and practitioners to see the problems from different perspectives and their solutions are explored, assessed and developed using multiple paradigms. Due to our socio-technical perspective, this project initially adopted a functionalist paradigm. This paradigm is well-developed and prevalent in social sciences (210). It assumes that society is composed of multiple systems, yet each system is interdependent with one another (211). In this sense, a change in one system can affect others, and all systems of the society can contribute to the support, maintenance, and stability of the entire social system by conforming to shared values and norms (212). The functionalist paradigm also believes that humans are naturally competitive, individualistic, and rational; therefore, human behavior is motivated by self-interest (211). Based on its underlying assumptions, the functionalist paradigm is more concerned with "the status quo, social order, consensus, social integration, solidarity, and need satisfaction" (210).

The results of our literature review revealed that the issues that have been addressed in the literature of cybersecurity economics (e.g., budgeting, interdependent risks, sustainability, and governance) suggest that a further interpretive approach is necessary to derive underlying meaning from the observed socio-technical phenomena. Moreover, our theoretical foundations showed that the causality of some challenges in development and implementation of solutions proposed within cybersecurity economics research could not be explored further within the functionalist paradigm but could be investigated for the triggers contributing to them arising from structures, mechanisms, experience and perception. This led to the adoption of two other paradigms to provide complementary perspectives on themes discussed in RP2 (complexity, dynamism, interdisciplinarity, social rules and institutions, and ethics). These two paradigms are constructivism, and critical realism.

Constructivism considers knowledge as a social construct which results from exchanges and interactions between individuals and the settings within which they are formed and operating (213, 214). Constructivist paradigm relies on the analysis of societal discourse that is recorded through data captured in activities such as observations and interviews. Through this analysis, this paradigm seeks to identify world views, subjective meanings and perspectives within social contexts. It depends on the beliefs and opinions of those being studied leading the researcher to identify patterns and themes in the complexity of views rather (215). However, the constructivist paradigm provides a limited reflection of socially constructed reality (ongoing, dynamic processes in which individuals and groups participate in the creation and institutionalization of their perceived reality). However, the causality associated with socially constructed reality can be analyzed using another critical realist paradigm.

Although critical realism acknowledges social reality, it seeks its linkage to causal mechanisms and structures (216) and accepts a variety of research methods that can be incorporated in naturalistic settings (217). Fundamentally, the basis of critical realism examines the interaction of structures and mechanisms that produce conditions contributing to the generation of identifiable events. Sayer defines structures as "sets of internally related objects or practices". Therefore, structures may comprise a physical or social form (e.g., governance structures, management systems, and business strategies). Mechanisms, however, are viewed as either a causal power or tendency (e.g., collaborative activities) that are able to influence or affect and outcome or event.

By adoption of these two paradigms, we further explored the causality of mutually constructed meanings and associated observable or unobservable events that occur in our social settings. We did that by distinguishing between three reality domains of empirical (what is known and conceptualized by social agents and researchers), actual (what happens in the world irrespective of its conceptualisation and knowledge) and real (unobservable interactions between different causal powers and structures of social objects that produce (or not) events, processes and phenomena) as illustrated in Figure 3.2. This stratified reality is aligned with our initial paradigm and perspective as it recognises that encompassing complex systems, trajectories and transformations depend on all of the whole, the parts, the interactions among parts and whole, and the interactions of any system with other complex systems among which it is nested and with which it intersects (218). As illustrated in Figure 3.1, through these stratified levels, we connected interpretations of reality with the objective aspects of this project discussed in Section 2.4.

Collectively, by incorporating the epistemology and methodology associated with the three research paradigms of functionalism, constructivism, and critical realism, we extended our worldview in this project. As discussed by Patel (124), this multiparadigmatic approach improves the predictability of outcomes and deepens our understanding of the problems and the influencing factors.

Figure 3.1 illustrates our research model in this project.

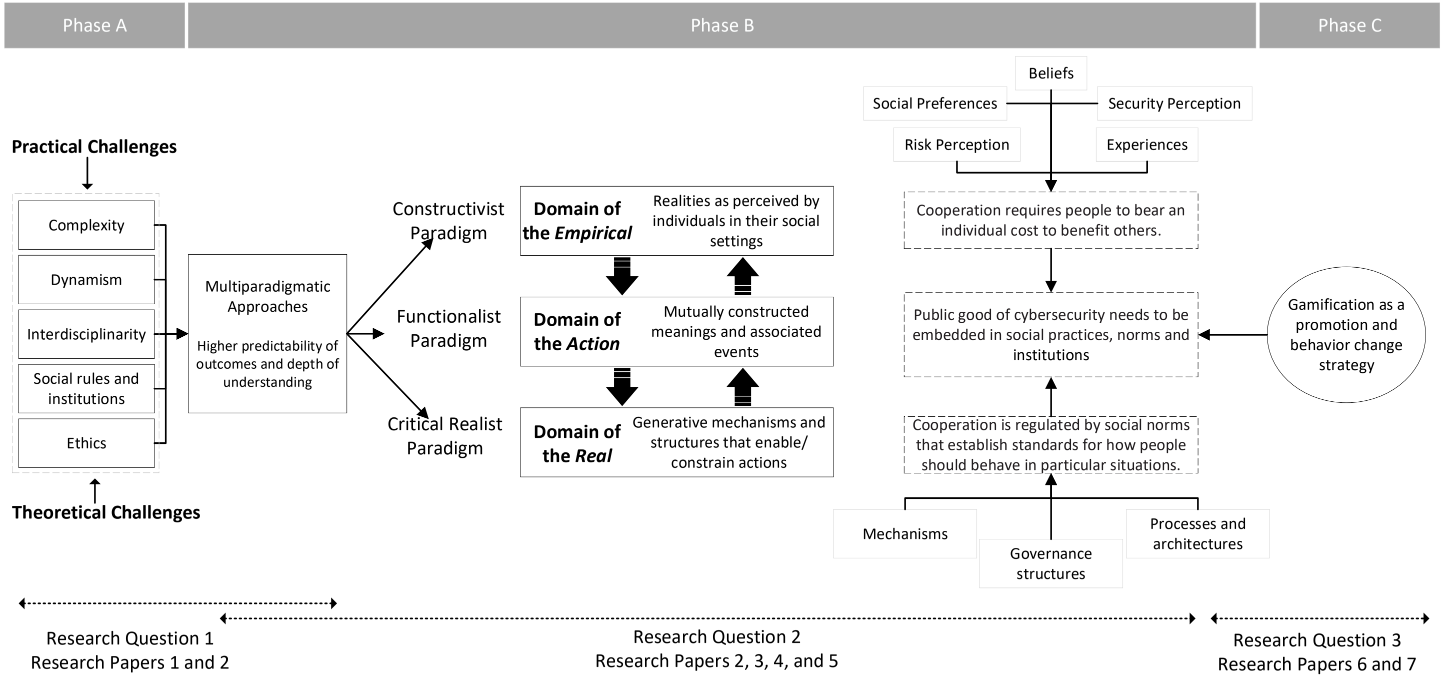

Phase A
Phase B
Phase C
Practical Challenges
Complexity
Dynamism
Interdisciplinarity
Social rules and institutions
Ethics
Theoretical Challenges
Multiparadigmatic Approaches
Higher predictability of outcomes and depth of understanding
Constructivist Paradigm
Functionalist Paradigm
Critical Realist Paradigm
Domain of the *Empirical*
Realities as perceived by individuals in their social settings
Domain of the *Action*
Mutually constructed meanings and associated events
Domain of the *Real*
Generative mechanisms and structures that enable/ constrain actions
Beliefs
Social Preferences
Security Perception
Risk Perception
Experiences
Cooperation requires people to bear an individual cost to benefit others.
Public good of cybersecurity needs to be embedded in social practices, norms and institutions
Cooperation is regulated by social norms that establish standards for how people should behave in particular situations.
Mechanisms
Governance structures
Processes and architectures
Gamification as a promotion and behavior change strategy
Research Question 1
Research Papers 1 and 2
Research Question 2
Research Papers 2, 3, 4, and 5
Research Question 3
Research Papers 6 and 7

Figure 3.1: Conceptual research model of this project and how it maps to the phases of transdisciplinary research strategy described in Section 1.4 (Phase A: Problem Framing, Phase B: Creation of solution-oriented knowledge through multi-paradigmatic research, and Phase C: Re-integration and application of created knowledge)

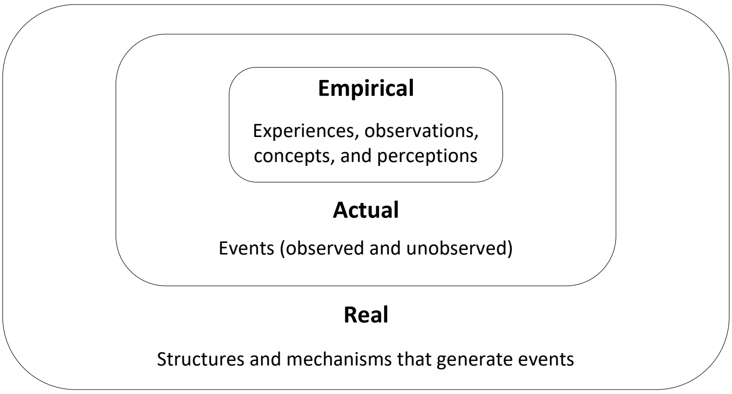

Empirical
Experiences, observations, concepts, and perceptions
Actual
Events (observed and unobserved)
Real
Structures and mechanisms that generate events

Figure 3.2: A view of stratified reality

3.2 Research Approaches

Considering the stratified view of reality, we need make sense of what we observe, if it is to mean anything to us, to enable us to understand the meaning of objects and events in their settings, to enable us to draw conclusions about the general from observations and perceptions of the individual. The research methods that enable us to achieve this goal revolve around different modes of inference. The concept of inference refers to different ways of arguing and drawing conclusions. Inference is a way of reasoning towards an answer to questions such as: What does this mean? What follows from this? What must exist for this to be possible? In this section we distinguish between four main forms of inferences: deduction, induction, abduction, and retroduction. Table 3.1 shows that each form represents a way of moving from one thing to something else. We consider the different form of inference as complementary in our research project. Deduction, for example, gives us universal guidelines for what is necessary for a logically valid argument. These guidelines can be used to test the validity of the conclusions drawn by means of retroduction.

While induction and deduction have been largely used in the literature of cybersecurity economics, and in general research practice, abductive and retroductive inferences have been applied less. Neither deductive nor inductive logic can inform discoveries such as How do we actually make the assumption that individual events may be part of a general context or structure? What makes us see structures in individual events? How does

Table 3.1: Four main forms of inferences used in this project

Inference Form	Description	Central Issue	Research Paper
Induction	Inference is drawn about larger populations or phenomena from individual observations.	What is common for a number of observed entities and is it true also for a larger population?	RP1 and RP3
Deduction	Knowledge of individual phenomena which is derived from universal laws.	What are the logical conclusions of the premises?	RP5
Abduction	To interpret and recontextualize individual phenomena within a conceptual framework or a set of ideas.	What meaning is given to something interpreted within a particular conceptual framework?	RP2 and RP6
Retroduction	A means of inference which involves imagining a model of a mechanism that, if it were real, would account for the phenomenon in question	What qualities must exist for something to be possible?	RP4 and RP7

a researcher discover that certain behavior is a manifestation of a norm structure? By means of abduction, individual phenomena are understood as embedded in, and an outcome of, social structures. In abductive inference, we 1) have some empirical observations, 2) which we relate to a rule, which 3) leads us to a new assumption about the observations.

RP4 and RP7 apply retroductive inferences. Retroduction is about advancing from one thing (empirical observations of events) and arriving at something different (a conceptualization of structures and transfactual conditions). For example, in RP4 we started by our observation of mediating effect of social preference and reciprocal behavior on willingness to cooperation under cyber risks and uncertainty. This observation led us to incorporate this variable into our model in which cybersecurity is treated as a public good. We therefore concluded that reciprocity sustains the prosocial behavior and promotes cooperative behavior under specific conditions and governance structure. In retroductive inference, counterfactual thinking is necessary. We ask questions like: How would this be if not . . . ? Could one imagine X without . . . ? Could one imagine X including this, without X then becoming something fundamentally different? In counterfactual thinking, we use our experiences and knowledge of social reality, as well as our ability to abstract and to think about what is not, but what might be.

Abductive and Retroductive inferences have a common limitation. Neither abduction nor retroduction is a logically valid mode of inference in the sense that deduction is. There are no fixed criteria from which it would be possible to assess in a definite way the validity of a abductive or retroductive inference. However, we applied these two forms since they broaden our knowledge and stimulate the research process. They are forms of inferences through which new ideas are introduced, and thus they are more important for scientific progress than, for example, deduction (219).

3.3 Research Methodology

The final step in developing a research plan is selecting methods and tactics to execute the plan. However, a specific procedure or technique, known as research methodology, is required to identify, select, and process these methods. A research methodology can be defined as ”a system of principles, practices, and procedures applied to a specific branch of knowledge” (220). The research in the field of cybersecurity economics draws on theories from natural sciences, computer sciences, social sciences, psychology,

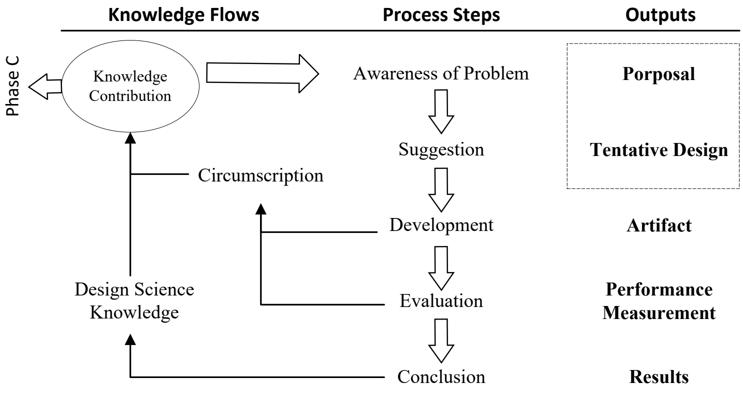


Figure 3.3: Vaishnavi and Kuechler's design science research process model (2)

and economics and finance to solve the problems at the intersection of information technology, information security, and organizations. Due to the interdisciplinary nature of this field, the Design Science Research Methodology (DSRM) presented in (221) incorporates principles, practices, and procedures required to carry out such research. DSRM is consistent with prior literature, provides a nominal process model for doing design science research, and it provides a mental model for presenting and evaluating research outcomes. These features are necessary for our research since 1) it crosses multiple paradigms and consistency and the presence of a process model in crucial, and 2) it aims to re-integrate and apply created knowledge into both societal and scientific practices.

DSRM involves the creation of knowledge and understanding of a problem, and its solution are acquired in the building and application of an artifact (222). The use and performance of designed artifacts is then analyzed to understand, explain, and solve the problem. Such an artifact can be a model, a method, human-computer interfaces, a standard, or a framework (223, 224). We will describe the design science research journey of this project in terms of Vaishnavi and Kuechler's general process model for design science research (2). This model describes an iterative process of problem awareness, solution suggestion, artifact development, evaluation, conclusion and knowledge flow circumscription. This model is depicted in Figure 3.3. The following describes each step extracted from (225).

Awareness of Problem. DSRM begins with the awareness and explication of the real-world problem. There can be multiple sources from which awareness may arise of an interesting practical and research problem. The problem should be interesting because it is proving intractable. Intractable problems are those for which the solutions at hand are unsatisfying. Intractable problems are interesting when we discover that these problems are essentially not of the nature previously assumed. In our research project, we assume that the essence of the problem has to do with overcoming the unwillingness of cybersecurity practitioners, ranging from operators to decision-makers, to effectively implement the solutions proposed within cybersecurity economics research. The problem becomes interesting when we assume the practitioners are behaving properly in the implementation of the solutions. It is a problem of helping them embed the solutions in their social norms and institutions and develop them to promote secure behavior in their systems. Intractable problems are often interesting research problems because researchers may have been basing their knowledge on the wrong range of theories or assumptions. Such a misalignment occurs because the practical problem has been misdiagnosed.

Suggestion. This phase of problem awareness is followed by the suggestion for a tentative design drawn from the existing knowledge base for the identified problem. As indicated by the dashed line around the proposal and tentative design in Figure 3.3, the Awareness and the Suggestion phases are closely connected. Both phases are likely to involve an abductive reasoning process. As we mentioned in the previous section, abduction is a reasoning process in which the designer observes the problem and then creates elements of the most likely solution (tentative design). This tentative design is the output of the Suggestion phase.

Development. The next step is an attempt for artifacts design which is derived from the suggested tentative solutions and defined requirements. The development and implementation may not necessarily involve novelty or originality beyond the current state-of-the-art. The novel contribution is usually present in the artifact's design rather than in its construction. Both the Development and the Conclusion phases involve deductive and retroductive reasoning in deducing the artifact's material characteristics from the tentative design and what qualities must exist for the artifact to be applicable and feasible.

Evaluation. In the Evaluation phase, the results of the artifact development are compared with the expectations that are either implicit or explicit in the Awareness and the Suggestion phases. When results embody essential deviations from expectations, we need tentative explanations to determine which further steps to follow next. These results and explanations often provide information that helps refine our understanding of the problem, the utility of the suggestion, and the feasibility of the originally imagined artifact.

Conclusion. In terms of reasoning, this phase involves reflection and abstraction. We give consideration to the meaning of the more important and general outcomes of the previous phases. It is not necessary that the outcomes are optimal, only that they satisfice. But in producing these outcomes, we learn about the nature of the problem, the character of the solution, and the effect of the artifact. In other words, we not only seek to solve the problem, but also to learn about the environment that produces the problem and envelopes the solution artifact.

As Figure 3.3 illustrates, **Circumscription** represents major feedback loops driving iteration in the research process. Circumscription informs us of the limits or boundaries of the knowledge discovered in each iteration. This information determines our awareness and suggestion, which in turn drive our conclusion to design and develop an artifact. In so doing, we create a new situation and we must again decide what to do. Accordingly, there are two types of arrows in the Figure 3.3 representation of this process. Broad white arrows represent knowledge use, and narrow black arrows represent the generation of knowledge. The white arrow headed out in the figure corresponds our transition to Phase C of our research design strategy described in Section 1.4. After description of each step, Table 3.2 shows the methods used at each step to answer the research questions defined in this project.

Table 3.2: The methods used in each step of DSRM to answer research questions

DSRM Step	**RQ1** Research Paper 1	**RQ2** Research Papers 2, 3, 4, and 5	**RQ3** Research Papers 6 and 7
Awareness	Literature Review	Literature Review	Literature Review
Suggestion	Literature Review	Empirical Studies	Synthesis of design principles based on empirical findings and adapting them with additional theories
Development	Synthesis of literature	-Mechanism Design -Parametric Design	Instantiation of design principles as a prototype
Evaluation	-	-Simulation (laboratory experiment) -Analytical	Qualitative evaluation of the artifact (focus groups)
Conclusion	-Frameworks	-Model -Construct	-Framework -Instantiation

Chapter 4

Conclusion

Over the past 20 years, a new stream of research, known as cybersecurity economics, seeks to adopt and apply selected methods from economics to better explain and mitigate cybersecurity failures. Most of the studies are founded on how people make decisions when they face trade-offs or respond to incentives, how individuals and organizations interact, and how the systems as a whole work. Although most of these studies have acknowledged the complexity of the problems they were aimed to solve, this thesis argues that using only one lens to look at those problems necessarily leads to blind spots. The increasing small and large-scale cyber incidents in the world continuously reveals these spots. Today, we realize that cybersecurity economics problems are characterized by different frames for defining the problem that depend on the worldviews of the different actors ranging from individuals to the whole society. Moreover, the quality of a solution cannot be assessed objectively, but depends on the actors' values, goals, and actions. These properties of such problems pose major challenges to both societal and scientific actors.

As supported in this thesis, one way to deal with these challenges is to employ multi-paradigmatic approached within a transdisciplinary research strategy by which both scientific and societal actors try to reach a consensus on how to define the problem, how a generally acceptable solution might look like and how it could be reached. This thesis suggested a set of guidelines to conduct multi-paradigmatic research. Then, it followed those guidelines to investigate the notion of cybersecurity as a public good to deal with collective action problems in implementation of cybersecurity economics solutions. We advanced this notion by two perspectives: 1) Cooperation requires people to bear an individual cost to benefit others, and 2) Cooperation is regulated by social norms that establish standards for how people should behave in particular situations. Hence, this thesis crossed paradigms of functionalism, constructivism, and critical realism to gain richer knowledge on the chosen subject: cybersecurity as a public good.

By crossing these paradigms and methods that which enabled us to serve the purpose of this research, we first examined the smallest levels of interaction, interaction within "the self". In RP3, we studied this topic initially by testing several hypotheses to show how the assumptions and parameters of behavioral models of social preferences relate to the willingness to cooperate within the context of cybersecurity. The moderating effect of social preferences on willingness to cooperate was supported by the collected data from societal stakeholders. This led us to incorporate social preferences into the utility function that predicts observed decisions. It also motivated us to study critical realism paradigm which perceives human nature as cooperative, collective, and social.

With these results, we constructed an agent-based model in which a group of heterogeneous agents participate in provision of several cybersecurity measures as public goods. Analyzing the influence of different parameters of this model showed that with possibility of punishment, the agents adopt an evolutionary strategy towards the provision of cybersecurity as a public good and create a robust environment. In other words, the simulation results for our baseline model suggested that the environment forms a dominant strategy which promotes the cooperation efficiently. Furthermore, our simulations have been able to exhibit altruistic punishment and inequity aversion preferences in the agents' decisions. In this connection, it is important to mention that the success of providing cybersecurity as a public good was predominantly enabled by the dynamic level of contributions based on the agents' experience of being a victim, punished, or number of existing free-riders. By analysis of the results in RP4, we realized active involvement of groups' members determines the success of achieving sustainable and effective development of a secure environment. The efficiency of these interactions depends largely on the institutional arrangements that involve, empower, and give a chance to the agents to use their cultures, knowledge and capabilities for sustainable cybersecurity.

With such insights, we suggested that polycentric governance structure should be used to promote active participation that empowers stakeholders to be critical in understanding their problems and enables them to reflect on their situations that help them to objectively decide on trade-offs. Therefore, we advanced our research to study how polycentricity is conceptualized and operationalized in cybersecurity policies and institutions. We employed Institutional Grammar 2.0 to investigate whether the EU's cybersecurity strategies and policies establish a polycentric governance structure. Moreover, we analyzed the EU cybersecurity policies to identify what sanctions are prescribed as part of the regime and to what extent the sanctioning is centralized or decentralized. Since the scope of this study has been narrowed down to cyber incident and crisis response across the EU, we also explored to what extent policies signal actors' commitment to ensure efficient cyber crisis management as a complex public good.

The results of this study uncovered the variation in polycentricity within specific cybersecurity regulations in the EU governance system and the variation in authorities of different actors across those regulations. However, our study found weak evidence of punishment and signals of commitment to common goals in the analyzed policies. Although the policies of punishment depend on cultural, political, and legal values, the neglect of proportionate punishment immensely influences the active participation of agents in the achievement of common goals. One of the reasons that policy-makers have failed to adequately address these two concepts in cybersecurity policies is that the policy-makers have been unable to perceive the complexity of human behavior and the systems in which we live. This led us to inquire constructivist paradigms once again to come up with approaches that enable policy-makers to identify the issues that are most relevant to their specific context and needs.

According to constructivism paradigm, people construct their own understanding and knowledge of the world through individual and social experiencing things and reflecting on those experiences. Hence, we designed, developed, and evaluated a policy game which empowers the players to practice their knowledge on how to promote secure and sustainable behavior in digital ecosystems using different security metrics. This game is an instantiation of our proposed socio-technical framework for developing serious games. The framework emphasizes on experiential learning and ability to reflect in practice. The evaluation results showed that the game was successful as a learning tool to understand complexity, consider uncertainty, enhance scenario analysis, base the decisions on deeper knowledge and insights, and change the way of thinking.

Ultimately, the research presented in this thesis has provided a view of how solutions proposed by cybersecurity economics research can be embedded in social norms and institutions that promote secure behavior in digital ecosystems. This is done through five main contributions of:

- Improved understanding of the problems and challenges in cybersecurity economics theory and practice
- A set of recommendations that aim to support a transdisciplinary, reflective, collaborative, and integrative research within the field of cybersecurity economics
- Examining the doctrine of cybersecurity as a public good through a multi-paradigmatic research
- A new framework and design process to design and develop serious games to raise security awareness, teach hands-on skills, and develop key competencies as well as to understand the needs and characteristics of the players through gamification experiences

While acknowledging the potential for effectively leveraging the guidelines suggested in this thesis, this research has also highlighted the complexity of fully realizing this potential. It requires researchers, practitioners, and policymakers to develop a more holistic understanding of cybersecurity. After this conclusion, the rest of this chapter outlines the limitations of this research in Section 4.1 and presents our suggestions for future work in Section 4.2.

4.1 Limitations

This research is not without its shortcomings. Problems have been identified with the theory and practice of this research. The issues of particular concern are as follows:

- Limited collaboration with the societal actors: Although the research strategy of this research project is transdisciplinary, our interaction with the societal actors were limited to the survey with C-level employees within research paper RP3. We plan to use the designed game as a negotiation platform to continue our communication with societal actors. This communication can affect on how societal actors in the field of cybersecurity perceive the notion of cybersecurity as a public good and how they understand this notion can contribute to dealing with collective action problems.

- For the quantitative part of this research, our questionnaire in RP3 is constrained by certain limitations. First, our survey relies on self-reported data. Despite being a common approach for collecting data in a number of disciplines, people are often biased when reporting on their own experience (meaning factual data may not coincide with respondents' perceptions). Second, we were unable to collect data from other countries. This limited our study to the Norwegian firms which may collectively have different preferences and attitudes.

- Despite our efforts to develop an inclusive model and generic constructs, our agent-based model RP4 cannot be considered a universal model, fully applicable to all settings. We are still in the very early stages, and the studies on the notion of cybersecurity as a public good are limited. While this model lays a solid foundation for future studies to extend its application, the future work can mitigate the concern of generalizability and provide interesting findings by adapting it.

- Our analysis of institutional design of EU cyber incidents and crises management as a complex public good provided some useful insights that can be employed in cybersecurity policies at the EU and Member States levels. However, the propositions in our research need to be supported by qualitative and quantitative evaluation and longitudinal field studies to be more structured and effective.

- The designed game in RP7 needs to be evaluated in further cycles of design science research and larger focus group including cybersecurity practitioners. Through these cycles, the design principles will be adapted and, accordingly, the prototype will be updated.

4.2 Future Research

This thesis represented an example of multi-paradigmatic research on cybersecurity economics by focusing on cybersecurity as a public good. Multi-paradigmatic studies represent a new and potentially enlightening path forward in cybersecurity economics. However, there are limits to methodological rigour in the complex world of multiple paradigms. Future work can propose a concise framework and a set of guidelines to extend this approach to other core issues such as budgeting, information asymmetry, and interdependent risks. Moreover, identification of factors that may impede researchers from engaging in multi-paradigmatic studies is important.

This research also opened up new avenues for more exploration within the problems and opportunities created by treating cybersecurity as a public good. New systematic approaches, underlying methodologies, and collaboration between societal and scientific actors are needed to study various aspects of treating cybersecurity as a public good. Our proposed multi-layered perspective can be a starting point to identify the needs for change at each layer and the conversion layers. Methodological tools can be employed to conduct multi-level and evolutionary network analysis on how patterns of institutional interconnections influence the dynamic state, the flow of information, and the intensity of cooperation at different layers of utility, supply, and production.

Consequently, future work can introduce a conceptual framework of 'sustainable transition pathways,' which is inherently derived from the contextualization of theoretical models developed in this thesis and the literature of cybersecurity economics. Through the case studies, this conceptual framework can provide additional theoretical inputs to better grasp the complexity of shifting from the current pathway initially chosen by the actors to pathways that various cybersecurity functions, products, and services are treated as public goods.

Moreover, future work can benefit from Institutional Grammar to study the the complex interplay between institutional arrangements and stakeholders' behavior, as well as researchers interested in the semantics of cybersecurity institutions and policies. This tool can also be utilized to propose new institutional arrangements that facilitate the apply the societally relevant outcomes of research within cybersecurity economics.

As it has been highlighted through this research project, collective action problems require different strategies to be addressed. When actors implement these strategies, it often results in specific and partially observable patterns of behavior. Therefore, future work can contribute to the literature of cybersecurity economics by development of a decentralized decision support framework for heterogeneous agents enabling complex interactions in dynamic environments with uncertainties. This system should incorporate notions such as risk aversion, social preferences, and perception accuracy in agents decision-making processes, and analyze their effects on their performance in the presence of unforeseen events. Moreover, following research questions, ranging from fundamental to analytical, can also be investigated along the way:

- How do the scientific and societal actors in the field of cybersecurity define public goods?[1]
- To what extent does the non-excludability and non-rivalry of cybersecurity as a public good play a role in their perspective?
- What are the specificities of the national and international institutions that shape understandings of the public dimension of cybersecurity?
- What mechanisms can be employed to handle barriers and path dependencies in socio-technical transitions towards cybersecurity as a public good?
- Which institutional arrangements are more prone to path-dependent outcomes, and which are open to continued modification and change?

In addition to these suggestions for future work within the context of cybersecurity as a public good, the literature of cybersecurity economics can take advantage of gamification as a participatory approach to both understand the societal problems and challenges and to integrate the generated knowledge in scientific discourse into the societal practices. However, the research on using gamification within the cybersecurity economics research is still nascent. Our suggested framework and design process can be starting points to explore this area more.

[1] An answer to this question is critically important for the choice of criteria and characteristics that determine the way different goods will be classified (the second item in the list). A review on the literature of public goods shows that there is a wide dispersion of view about what constitutes a public goods and what does not among economists. Although in this thesis we Such disagreement suggests that objective criteria do not exist. For example, Barzel (226), Demsetz (227), and Kindleberger (228) have argued that non-rivalness is the crucial characteristic of a public good and non-excludability is not. A number of other economists say that non-excludability, not non-rivalness, is the indicator of public goods (229, 230, 231). Some other economists agree with the Samuelson (232) and say that both non-exclusiveness and non-rivalness are necessary characteristics of public goods (233, 234). This thesis concur with the latter opinion and does not challenge other opinion since it is out of the scope of this thesis. However, the author is curious to know the scientific and societal actors in the field of cybersecurity devise what criteria to define (or determine) public goods.

Bibliography

[1] M. Kianpour, S. Kowalski, E. Zoto, C. Frantz, and H. Øverby, "Designing serious games for cyber ranges: A socio-technical approach," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 85–93.

[2] V. Vaishnavi and W. Kuechler, *Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd Edition*. CRC Press, 2015.

[3] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin, "A retrospective impact analysis of the wannacry cyberattack on the nhs," *NPJ digital medicine*, vol. 2, no. 1, pp. 1–7, 2019.

[4] S.-C. Hsiao and D.-Y. Kao, "The static analysis of wannacry ransomware," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2018, pp. 153–158.

[5] A. Greenberg, "The untold story of notpetya, the most devastating cyberattack in history," August 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] A. Holmes, "533 million facebook users' phone numbers and personal data have been leaked online," Apr 2021. [Online]. Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=feedburner&amp;utm_medium=feed&amp;utm_campaign=Feed%3A%2Btypepad%2Falleyinsider%2Fsilicon_

alley_insider%2B%28Silicon%2BAlley%2BInsider%29&amp;r=US&amp;IR=T

[7] H. Knowles, “533 million facebook users’ phone numbers, personal information exposed online, report says,” Apr 2021. [Online]. Available: https://www.washingtonpost.com/business/2021/04/03/facebook-data-leak-insider/

[8] B. F. Alex Marquardt and Z. Cohen, “Microsoft identifies more than 40 organizations targeted in massive cyber breach,” December 2020. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[9] N. Perlroth, “Russians are believed to have used microsoft resellers in cyberattacks,” July 2021. [Online]. Available: https://www.nytimes.com/2020/12/24/us/russia-microsoft-resellers-cyberattacks.html

[10] M. Sentonas, “Crowdstrike launches free tool to identify and help mitigate risks in azure active directory,” December 2020. [Online]. Available: https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-di

[11] T. Wayt, “Why is the log4j cybersecurity flaw the ‘most serious’ in decades?” December 2021. [Online]. Available: https://nypost.com/2021/12/20/why-is-the-log4j-cybersecurity-flaw-the-most-serious-in-decades/

[12] I. Corporation, “Cost of a data breach report 2022,” Ponemon Institute and IBM Security, Tech. Rep., 2022.

[13] S. Kraemer, P. Carayon, and J. Clem, “Human and organizational factors in computer and information security: Pathways to vulnerabilities,” *Computers & security*, vol. 28, no. 7, pp. 509–520, 2009.

[14] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, “The human factor of information security: Unintentional damage perspective,” *Procedia-Social and Behavioral Sciences*, vol. 147, pp. 424–428, 2014.

[15] M. Van Eeten, “Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity,” *Digital Policy, Regulation and Governance*, 2017.

[16] E. M. Ahmed, "Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth," *Journal of the Knowledge Economy*, pp. 1–19, 2020.

[17] J. Lewallen, "Emerging technologies and problem definition uncertainty: The case of cybersecurity," *Regulation & Governance*, vol. 15, no. 4, pp. 1035–1052, 2021.

[18] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship and Sustainability Issues*, 2019.

[19] S. Creese, J. Saunders, L. Axon, and W. Dixon, "Future series: Cybersecurity, emerging technology and systemic risk," in *World Economic Forum*, 2020.

[20] P. Kivimaa, M. C. Brisbois, D. Jayaram, E. Hakala, and M. Siddi, "A socio-technical lens on security in sustainability transitions: Future expectations for positive and negative security," *Futures*, p. 102971, 2022.

[21] A. M. Hernández, *Taming the Big Green Elephant: Setting in Motion the Transformation Towards Sustainability.* Springer Nature, 2021.

[22] C. Webel and J. Galtung, *Handbook of peace and conflict studies.* Routledge London, 2007, vol. 7.

[23] N. Kshetri, "Simple economics of cybercrime and the vicious circle," in *The global cybercrime industry.* Springer, 2010, pp. 35–55.

[24] D. K. Mulligan and F. B. Schneider, "Doctrine for cybersecurity," *Daedalus*, vol. 140, no. 4, pp. 70–92, 2011.

[25] F. W. Geels, "Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study," *Research policy*, vol. 31, no. 8-9, pp. 1257–1274, 2002.

[26] I. Fazey, N. Schäpke, G. Caniglia, J. Patterson, J. Hultman, B. Van Mierlo, F. Säwe, A. Wiek, J. Wittmayer, P. Aldunce *et al.*, "Ten essentials for action-oriented and second order energy transitions, transformations and climate change research," *Energy Research & Social Science*, vol. 40, pp. 54–70, 2018.

[27] K. E. Howell, *An introduction to the philosophy of methodology*. Sage, 2012.

[28] L. Van Kerkhoff, "Developing integrative research for sustainability science through a complexity principles-based approach," *Sustainability Science*, vol. 9, no. 2, pp. 143–155, 2014.

[29] R. W. Scholz and G. Steiner, "Transdisciplinarity at the crossroads," *Sustainability Science*, vol. 10, no. 4, pp. 521–526, 2015.

[30] B. Nölting and C. Mann, "Governance strategy for sustainable land management and water reuse: Challenges for transdisciplinary research," *Sustainable Development*, vol. 26, no. 6, pp. 691–700, 2018.

[31] C. Pohl, "What is progress in transdisciplinary research?" *Futures*, vol. 43, no. 6, pp. 618–626, 2011.

[32] S. Hoffmann, C. Pohl, and J. G. Hering, "Methods and procedures of transdisciplinary knowledge integration: empirical insights from four thematic synthesis processes," *Ecology and Society*, vol. 22, no. 1, 2017.

[33] C. Pohl and G. H. Hadorn, *Principles for designing transdisciplinary research*. oekom Munich, 2007.

[34] T. Bruhn, J. Herberg, G. Molinengo, D. Oppold, D. Stasiak, and P. Nanz, "Grounded action design. a model of scientific support for processes to address complex challenges," *IASS Discussion Paper*, 2019.

[35] D. J. Lang, A. Wiek, M. Bergmann, M. Stauffacher, P. Martens, P. Moll, M. Swilling, and C. J. Thomas, "Transdisciplinary research in sustainability science: practice, principles, and challenges," *Sustainability science*, vol. 7, no. 1, pp. 25–43, 2012.

[36] C. Mitchell, D. Cordell, and D. Fam, "Beginning at the end: The outcome spaces framework to guide purposive transdisciplinary research," *Futures*, vol. 65, pp. 86–96, 2015.

[37] G. H. Hadorn, H. Hoffmann-Riem, S. Biber-Klemm, W. Grossenbacher-Mansuy, D. Joye, C. Pohl, U. Wiesmann, and E. Zemp, *Handbook of transdisciplinary research*. Springer, 2008, vol. 10.

[38] G. Wuelser, C. Pohl, and G. Hirsch Hadorn, "Structuring complexity for tailoring research contributions to sustainable development: a framework," *Sustainability science*, vol. 7, no. 1, pp. 81–93, 2012.

[39] J. Blatter and M. Haverland, *Designing case studies: Explanatory approaches in small-N research.* Palgrave Macmillan, 2012.

[40] S. Talwar, A. Wiek, and J. Robinson, "User engagement in sustainability research," *Science and Public Policy*, vol. 38, no. 5, pp. 379–390, 2011.

[41] L. Van Kerkhoff and L. Lebel, "Linking knowledge and action for sustainable development," *Annu. Rev. Environ. Resour.*, vol. 31, pp. 445–477, 2006.

[42] J. M. Keynes, *The General Theory of Employment, Interest, and Money*. Palgrave Macmillan, 2018.

[43] M. Friedman, "The methodology of positive economics," *Essays in Positive Economics*, 1953.

[44] Y.-K. Ng, "Are unrealistic assumptions/simplifications acceptable? some methodological issues in economics," *Pacific Economic Review*, vol. 21, no. 2, pp. 180–201, 2016.

[45] C. Herley and P. C. Van Oorschot, "Sok: Science, security and the elusive goal of security as a scientific pursuit," in *2017 IEEE symposium on security and privacy (SP)*. IEEE, 2017, pp. 99–120.

[46] D. Lovallo, T. Koller, R. Uhlaner, and D. Kahneman, "Your company is too risk-averse," Feb 2020. [Online]. Available: https://hbr.org/2020/03/your-company-is-too-risk-averse

[47] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 235–243.

[48] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," *Journal of Economic Surveys*, vol. 36, no. 1, pp. 157–187, 2022.

[49] R. Anderson and T. Moore, “Information security economics–and beyond,” in *Annual International Cryptology Conference*. Springer, 2007, pp. 68–91.

[50] A. Lindbeck, S. Nyberg, and J. W. Weibull, “Social norms and economic incentives in the welfare state,” *The Quarterly Journal of Economics*, vol. 114, no. 1, pp. 1–35, 1999.

[51] T. Parsons and E. A. Shils, “The social system,” in *Toward a general theory of action*. Routledge, 2017, pp. 190–233.

[52] A. Festre, “Incentives and social norms: A motivation-based economic analysis of social norms,” *Journal of Economic Surveys*, vol. 24, no. 3, pp. 511–538, 2010.

[53] K. P. Scheibe and J. Blackhurst, “Systemic risk and the ripple effect in the supply chain,” in *Handbook of Ripple Effects in the Supply Chain*. Springer, 2019, pp. 85–100.

[54] R. Anderson, *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

[55] L. J. Camp and S. Lewis, *Economics of information security*. Springer Science & Business Media, 2006, vol. 12.

[56] R. Anderson, “Why information security is hard-an economic perspective,” in *Proceedings of the 17th Annual Computer Security Applications Conference*, ser. ACSAC ’01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 358–. [Online]. Available: http://dl.acm.org/citation.cfm?id=872016.872155

[57] H. E. Leland and D. H. Pyle, “Informational asymmetries, financial structure, and financial intermediation,” *The journal of Finance*, vol. 32, no. 2, pp. 371–387, 1977.

[58] S. J. Grossman and O. D. Hart, “Implicit contracts, moral hazard, and unemployment,” *The American Economic Review*, vol. 71, no. 2, pp. 301–307, 1981.

[59] S. C. Myers and N. S. Majluf, “Corporate financing and investment decisions when firms have information that investors do not have,” *Journal of financial economics*, vol. 13, no. 2, pp. 187–221, 1984.

[60] K. Fousiani, “Power asymmetry, negotiations and conflict management in organizations,” in *Organizational Conflict-New Insights*. IntechOpen, 2020.

[61] M. A. Martínez-Carrasco, “Behavioral spillovers in organizations: A selective review,” *Experiments in Organizational Economics*, vol. 19, pp. 251–280, 2016.

[62] R. Bohme and T. Moore, “The iterated weakest link,” *IEEE Security & Privacy*, vol. 8, no. 1, pp. 53–55, 2010.

[63] R. Pal and P. Hui, “On differentiating cyber-insurance contracts a topological perspective,” in *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*. IEEE, 2013, pp. 836–839.

[64] S. Durlauf and L. E. Blume, *The new Palgrave dictionary of economics*. Springer, 2016.

[65] T. Dehlen, T. Zellweger, N. Kammerlander, and F. Halter, “The role of information asymmetry in the choice of entrepreneurial exit routes,” *Journal of Business Venturing*, vol. 29, no. 2, pp. 193–209, 2014.

[66] K. Boersma and J. Wolbers, “Foundations of responsive crisis management: Institutional design and information,” in *Oxford Research Encyclopedia of Politics*. Oxford University Press, 2021.

[67] M. Stigendal and A. Novy, “Founding transdisciplinary knowledge production in critical realism: implications and benefits,” *Journal of Critical Realism*, vol. 17, no. 3, pp. 203–220, 2018.

[68] E. L. Trist, *The evolution of socio-technical systems*. Ontario Quality of Working Life Centre Toronto, 1981, vol. 2.

[69] P. Carayon, P. Hancock, N. Leveson, I. Noy, L. Sznelwar, and G. Van Hootegem, “Advancing a sociotechnical systems approach to workplace safety–developing the conceptual framework,” *Ergonomics*, vol. 58, no. 4, pp. 548–564, 2015.

[70] E. Mumford, “The story of socio-technical design: Reflections on its successes, failures and potential,” *Information systems journal*, vol. 16, no. 4, pp. 317–342, 2006.

[71] L. J. Hettinger, A. Kirlik, Y. M. Goh, and P. Buckle, “Modelling and simulation of complex sociotechnical systems: envisioning and analysing work environments,” *Ergonomics*, vol. 58, no. 4, pp. 600–614, 2015.

[72] L. Von Bertalanffy, “An outline of general system theory.” *British Journal for the Philosophy of science*, 1950.

[73] E. Mumford, *Redesigning human systems*. IGI Global, 2003.

[74] B. Faude and T. Gehring, “Regime complexes as governance systems,” in *Research handbook on the politics of international law*. Edward Elgar Publishing, 2017, pp. 176–204.

[75] T. Gehring and B. Faude, “The dynamics of regime complexes: Microfoundations and systemic effects,” *Global governance*, pp. 119–130, 2013.

[76] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002. [Online]. Available: http://doi.acm.org/10.1145/581271.581274

[77] B. Rodrigues, M. Franco, G. Parangi, and B. Stiller, “Seconomy: a framework for the economic assessment of cybersecurity,” in *International Conference on the Economics of Grids, Clouds, Systems, and Services*. Springer, 2019, pp. 154–166.

[78] H. Kunreuther and G. Heal, “Interdependent security,” *Journal of risk and uncertainty*, vol. 26, no. 2, pp. 231–249, 2003.

[79] H. Ogut, N. Menon, and S. Raghunathan, “Cyber insurance and it security investment: Impact of interdependent risk,” *4th Annual Workshop on the Economics of Information Security*, 2005.

[80] R. Böhme, G. Schwartz *et al.*, “Modeling cyber-insurance: towards a unifying framework.” in *WEIS*, 2010.

[81] G. A. Schwartz and S. S. Sastry, “Cyber-insurance framework for large scale interdependent networks,” in *Proceedings of the 3rd international conference on High confidence networked systems*, 2014, pp. 145–154.

[82] X. Zhao, L. Xue, and A. B. Whinston, “Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling,” *ICIS 2009 proceedings*, p. 49, 2009.

[83] W.-H. Shim, “An analysis of information security management strategies in the presence of interdependent security risk,” *Asia pacific journal of information systems*, vol. 22, no. 1, pp. 79–101, 2012.

[84] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, “Sharing information on computer systems security: An economic analysis,” *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[85] S. Laube and R. Böhme, “The economics of mandatory security breach reporting to authorities,” *Journal of Cybersecurity*, vol. 2, no. 1, pp. 29–41, 2016.

[86] J. M. Bauer and M. J. Van Eeten, “Cybersecurity: Stakeholder incentives, externalities, and policy options,” *Telecommunications Policy*, vol. 33, no. 10-11, pp. 706–719, 2009.

[87] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, “Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers,” *IEEE Security & Privacy*, vol. 14, no. 3, pp. 52–60, 2016.

[88] R. Anderson, C. Barton, R. Bölme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, and M. Vasek, “Measuring the changing cost of cybercrime,” *The 18th Annual Workshop on the Economics of Information Security*, 2019.

[89] A. Laszka, M. Felegyhazi, and L. Buttyan, “A survey of interdependent information security games,” *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, pp. 1–38, 2014.

[90] M. H. Jhaveri, O. Cetin, C. Gañán, T. Moore, and M. V. Eeten, “Abuse reporting and the fight against cybercrime,” *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–27, 2017.

[91] S. Laube and R. Böhme, “Strategic aspects of cyber risk information sharing,” *ACM Computing Surveys (CSUR)*, vol. 50, no. 5, pp. 1–36, 2017.

[92] S. DellaVigna, "Psychology and economics: Evidence from the field," *Journal of Economic literature*, vol. 47, no. 2, pp. 315–72, 2009.

[93] D. E. Broadbent, *Perception and communication.* Elsevier, 2013.

[94] A. Stirling, "Risk, uncertainty and precaution: some instrumental implications from the social sciences," *Negotiating environmental change: New perspectives from social science*, pp. 33–74, 2003.

[95] F. H. Knight, *Risk, uncertainty and profit.* Houghton Mifflin, 1921, vol. 31.

[96] M. D. Resnik, *Choices: An introduction to decision theory.* U of Minnesota Press, 1987.

[97] A. Stirling, "Risk at a turning point?" *Journal of Risk Research*, vol. 1, no. 2, pp. 97–109, 1998.

[98] I. Aldasoro, L. Gambacorta, P. Giudici, and T. Leach, "The drivers of cyber risk," *Journal of Financial Stability*, vol. 60, p. 100989, 2022.

[99] J. Wolff and W. Lehr, "Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data," *Available at SSRN 2943867*, 2017.

[100] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[101] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko, "Botcoin: Monetizing stolen cycles." in *NDSS*, vol. 2014. Citeseer, 2014, pp. 1–16.

[102] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: An empirical analysis of spam marketing conversion," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 3–14.

[103] C. Herley and D. Florêncio, “Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy,” in *Economics of information security and privacy*. Springer, 2010, pp. 33–53.

[104] E. Van De Sandt, “Deviant security: the technical computer security practices of cyber criminals,” Ph.D. dissertation, University of Bristol, 2019.

[105] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, “Sok: P2pwned-modeling and evaluating the resilience of peer-to-peer botnets,” in *2013 IEEE symposium on security and privacy*. IEEE, 2013, pp. 97–111.

[106] H. Berghel, “Hiding data, forensics, and anti-forensics,” *Communications of the ACM*, vol. 50, no. 4, pp. 15–20, 2007.

[107] K. Huang, M. Siegel, and S. Madnick, “Systematically understanding the cyber attack business: A survey,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[108] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *computers & security*, vol. 38, pp. 97–102, 2013.

[109] L. A. Gordon, M. P. Loeb, W. Lucyshyn, L. Zhou *et al.*, “Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the gordon-loeb model,” *Journal of Information Security*, vol. 6, no. 01, p. 24, 2014.

[110] A. Nagurney and L. S. Nagurney, “A game theory model of cybersecurity investments with information asymmetry,” *NETNOMICS: Economic Research and Electronic Networking*, vol. 16, no. 1-2, pp. 127–148, 2015.

[111] C. Brookson, S. Cadzow, R. Eckmaier, J. Eschweiler, B. Gerber, A. Guarino, K. Rannenberg, J. Shamah, and S. Górniak, “Definition of cybersecurity-gaps and overlaps in standardisation,” *Heraklion, ENISA*, 2015.

[112] P. Hammond and B. Gummer, “National cyber security strategy 2016 to 2021,” *HM Government*, 2016.

[113] I. Corradini, *Building a cybersecurity culture in organizations*. Springer, 2020, vol. 284.

[114] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*. Oxford University Press, 2014.

[115] J. M. Spring, T. Moore, and D. Pym, “Practicing a science of security: a philosophy of science perspective,” in *Proceedings of the 2017 New Security Paradigms Workshop*, 2017, pp. 1–18.

[116] O. Pieczul, S. N. Foley, and V. M. Rooney, “I’m ok, you’re ok, the system’s ok: Normative security for systems,” in *Proceedings of the 2014 New Security Paradigms Workshop*, 2014, pp. 95–104.

[117] A. Kuehn and M. Mueller, “Shifts in the cybersecurity paradigm: zero-day exploits, discourse, and emerging institutions,” in *Proceedings of the 2014 New Security Paradigms Workshop*, 2014, pp. 63–68.

[118] H. Vescent and B. Blakley, “Shifting paradigms: Using strategic foresight to plan for security evolution,” in *Proceedings of the New Security Paradigms Workshop*, 2018, pp. 28–40.

[119] C. Perez, “Technological revolutions and techno-economic paradigms,” *Cambridge journal of economics*, vol. 34, no. 1, pp. 185–202, 2010.

[120] T. S. Kuhn *et al.*, *Criticism and the growth of knowledge: Volume 4: Proceedings of the International Colloquium in the Philosophy of Science, London, 1965*. Cambridge University Press, 1970, vol. 4.

[121] G. Falco, M. Eling, D. Jablanski, V. Miller, L. A. Gordon, S. S. Wang, J. Schmit, R. Thomas, M. Elvedi, T. Maillart *et al.*, “A research agenda for cyber risk and cyber insurance,” in *Workshop on the Economics of Information Security (WEIS)*, 2019.

[122] J. Hassard, “Multiple paradigms and organizational analysis: A case study,” *Organization Studies*, vol. 12, no. 2, pp. 275–299, 1991.

[123] M. W. Lewis and M. L. Kelemen, “Multiparadigm inquiry: Exploring organizational pluralism and paradox,” *Human Relations*, vol. 55, no. 2, pp. 251–275, 2002.

[124] T. Patel, “Promoting multi-paradigmatic cultural research in international business literature: An integrative complexity-based argument,” *Journal of Organizational Change Management*, 2016.

[125] T. Moore, “The economics of cybersecurity: Principles and policy options,” *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103–117, 2010.

[126] B. Jerman-Blažič *et al.*, “An economic modelling approach to information security risk management,” *International Journal of Information Management*, vol. 28, no. 5, pp. 413–422, 2008.

[127] M. Milgate, “Goods and commodities,” *The New Palgrave: A Dictionary of Economics*, vol. 2, pp. 546–548, 1987.

[128] P. Rosenzweig, “Cybersecurity, the public/private’partnership,’and public goods,” *Hoover National Security and Law Task Force*, 2011.

[129] D. L. Weimer and A. R. Vining, *Policy analysis: Concepts and practice*. Routledge, 2017.

[130] E. Krahmann, “Security: Collective good or commodity?” *European journal of international relations*, vol. 14, no. 3, pp. 379–404, 2008.

[131] M. Taddeo, “Is cybersecurity a public good?” pp. 349–354, 2019.

[132] D. C. Colander, *Microeconomics*. USA: McGraw-Hill Education, 2020.

[133] I. Kaul, I. Grunberg, and M. Stern, “Global public goods,” *New York-Oxford*, 1999.

[134] W. Hussain, “The Common Good,” in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. Metaphysics Research Lab, Stanford University, 2018.

[135] T. Moore, E. Kenneally, M. Collett, and P. Thapa, “Valuing cybersecurity research datasets,” in *Tyler Moore, Erin Kenneally, Michael Collett, and Prakash Thapa. Valuing cybersecurity research datasets. In 18th Workshop on the Economics of Information Security (WEIS)*, 2019.

[136] J. Anomaly, “Public goods and government action,” *Politics, Philosophy & Economics*, vol. 14, no. 2, pp. 109–128, 2015.

[137] M. Taddeo and F. Bosco, “We must treat cybersecurity as a public good. here’s why,” Aug 2019. [Online]. Available: https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/

[138] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[139] A. Kallhoff, "Why societies need public goods," *Critical Review of International Social and Political Philosophy*, vol. 17, no. 6, pp. 635–651, 2014.

[140] I. M. D. Little, *Ethics, economics, and politics: Principles of public policy*. Oxford University Press on Demand, 2002.

[141] C. T. Clotfelter, "Public services, private substitutes, and the demand for protection against crime," *The American Economic Review*, vol. 67, no. 5, pp. 867–877, 1977.

[142] T. E. Borcherding and R. T. Deacon, "The demand for the services of non-federal governments," *The American economic review*, vol. 62, no. 5, pp. 891–901, 1972.

[143] T. Zimmermann, "A political philosophy of public goods," in *European Republicanism*. Springer, 2019, pp. 157–196.

[144] T. Tropina, "Public–private collaboration: Cybercrime, cybersecurity and national security," in *Self-and co-regulation in Cybercrime, cybersecurity and national security*. Springer, 2015, pp. 1–41.

[145] M. Kianpour, "Knowledge and skills needed to craft successful cybersecurity strategies," in *Norsk IKT-konferanse for forskning og utdanning*, no. 3, 2020.

[146] J. H. Choi and K. Han, "Implications of false alarms in dynamic games on cyber-security," *Available at SSRN 3660197*, 2020.

[147] R. Pittiglio, F. Reganati, F. Ricci, and C. Tedeschi, "Cybersecurity, personal data protection and crime prevention from an italian perspective," in *The Palgrave Handbook of Corporate Sustainability in the Digital Era*. Springer, 2020, pp. 131–156.

[148] A. Asllani, C. S. White, and L. Ettkin, "Viewing cybersecurity as a public good: The role of governments, businesses, and individuals," *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, no. 1, p. 7, 2013.

[149] E. M. Sedenberg and D. K. Mulligan, “Public health as a model for cybersecurity information sharing,” *Berkeley Technology Law Journal*, vol. 30, no. 3, pp. 1687–1740, 2015.

[150] D. R. McCarthy, “Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order,” *Politics and Governance*, vol. 6, no. 2, pp. 5–12, 2018.

[151] D. Assaf, “Models of critical information infrastructure protection,” *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 6–14, 2008.

[152] M. Shore, Y. Du, and S. Zeadally, “A public-private partnership model for national cybersecurity,” *Policy & Internet*, vol. 3, no. 2, pp. 1–23, 2011.

[153] M. Dunn-Cavelty and M. Suter, “Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 179–187, 2009.

[154] M. Carr, “Public–private partnerships in national cyber-security strategies,” *International Affairs*, vol. 92, no. 1, pp. 43–62, 2016.

[155] A. D. Givens and N. E. Busch, “Realizing the promise of public-private partnerships in us critical infrastructure protection,” *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 39–50, 2013.

[156] R. J. Harknett and J. A. Stever, “The new policy world of cybersecurity,” *Public Administration Review*, vol. 71, no. 3, pp. 455–460, 2011.

[157] S. J. Shackelford, “Toward cyberpeace: Managing cyberattacks through polycentric governance,” *Am. UL Rev.*, vol. 62, p. 1273, 2012.

[158] H. Varian, “System reliability and free riding,” in *Economics of information security*. Springer, 2004, pp. 1–15.

[159] J. Grossklags, N. Christin, and J. Chuang, “Secure or insure? a game-theoretic analysis of information security games,” in *Proceedings of the 17th international conference on World Wide Web*, 2008, pp. 209–218.

[160] B. Johnson, R. Böhme, and J. Grossklags, “Security games with market insurance,” in *International Conference on Decision and Game Theory for Security*. Springer, 2011, pp. 117–130.

[161] D. T. Miller and R. K. Ratner, “The power of the myth of self-interest,” in *Current societal concerns about justice*. Springer, 1996, pp. 25–48.

[162] S. Mullainathan and R. H. Thaler, “Behavioral economics,” 2000.

[163] D. T. Kenrick, V. Griskevicius, J. M. Sundie, N. P. Li, Y. J. Li, and S. L. Neuberg, “Deep rationality: The evolutionary economics of decision making,” *Social cognition*, vol. 27, no. 5, pp. 764–785, 2009.

[164] M. P. Schlaile, M. Mueller, M. Schramm, and A. Pyka, “Evolutionary economics, responsible innovation and demand: Making a case for the role of consumers,” *Philosophy of Management*, vol. 17, no. 1, pp. 7–39, 2018.

[165] P. Asch and G. A. Gigliotti, “The free-rider paradox: Theory, evidence, and teaching,” *The Journal of Economic Education*, vol. 22, no. 1, pp. 33–38, 1991.

[166] F. Artinger, F. Exadaktylos, H. Koppel, and L. Sääksvuori, “In others’ shoes: do individual differences in empathy and theory of mind shape social preferences?” *PloS one*, vol. 9, no. 4, p. e92844, 2014.

[167] M. Haenlein and A. M. Kaplan, “A beginner’s guide to partial least squares analysis,” *Understanding statistics*, vol. 3, no. 4, pp. 283–297, 2004.

[168] J. Henseler, C. M. Ringle, and R. R. Sinkovics, “The use of partial least squares path modeling in international marketing,” in *New challenges to international marketing*. Emerald Group Publishing Limited, 2009.

[169] W. W. Chin and P. R. Newsted, “Structural equation modeling analysis with small samples using partial least squares,” *Statistical strategies for small sample research*, vol. 1, no. 1, pp. 307–341, 1999.

[170] K. A. Bollen, “A new incremental fit index for general structural equation models,” *Sociological methods & research*, vol. 17, no. 3, pp. 303–316, 1989.

[171] R. M. Baron and D. A. Kenny, “The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations.” *Journal of personality and social psychology*, vol. 51, no. 6, p. 1173, 1986.

[172] D. Borsboom, G. J. Mellenbergh, and J. Van Heerden, “The theoretical status of latent variables.” *Psychological review*, vol. 110, no. 2, p. 203, 2003.

[173] M. Shahrokh Esfahani and E. R. Dougherty, “Effect of separate sampling on classification accuracy,” *Bioinformatics*, vol. 30, no. 2, pp. 242–250, 2014.

[174] T. Olsson, M. Hell, M. Höst, U. Franke, and M. Borg, “Sharing of vulnerability information among companies–a survey of swedish companies,” in *2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. IEEE, 2019, pp. 284–291.

[175] R. O. Murphy, K. A. Ackermann, and M. Handgraaf, “Measuring social value orientation,” *Judgment and Decision making*, vol. 6, no. 8, pp. 771–781, 2011.

[176] E. Ostrom, “Collective action and the evolution of social norms,” *Journal of economic perspectives*, vol. 14, no. 3, pp. 137–158, 2000.

[177] E. Fehr, U. Fischbacher, and S. Gächter, “Strong reciprocity, human cooperation, and the enforcement of social norms,” *Human nature*, vol. 13, no. 1, pp. 1–25, 2002.

[178] T. Hopthrow and L. G. Hulbert, “The effect of group decision making on cooperation in social dilemmas,” *Group Processes & Intergroup Relations*, vol. 8, no. 1, pp. 89–100, 2005.

[179] J. A. Kitts, “Collective action, rival incentives, and the emergence of antisocial norms,” *American Sociological Review*, vol. 71, no. 2, pp. 235–259, 2006.

[180] K. Carlisle and R. L. Gruby, “Polycentric systems of governance: A theoretical model for the commons,” *Policy Studies Journal*, vol. 47, no. 4, pp. 927–952, 2019.

[181] V. Ostrom, C. M. Tiebout, and R. Warren, “The organization of government in metropolitan areas: a theoretical inquiry,” *The American Political Science Review*, vol. 55, no. 4, pp. 831–842, 1961.

[182] E. Ostrom, “Polycentric systems for coping with collective action and global environmental change,” *Global environmental change*, vol. 20, no. 4, pp. 550–557, 2010.

[183] H. L. Boschken, “Aligning a multi-government network with situational context: Metropolitan governance as an organizational systems problem,” *The American Review of Public Administration*, vol. 47, no. 2, pp. 189–208, 2017.

[184] S. J. Shackelford, *Cyber War and Peace: Toward Cyber Peace*. Cambridge University Press, 2020.

[185] T. Toonen, “Resilience in public administration: the work of elinor and vincent ostrom from a public administration perspective,” *Public Administration Review*, vol. 70, no. 2, pp. 193–202, 2010.

[186] E. Ostrom, *Governing the commons: The evolution of institutions for collective action*. Cambridge university press, 1990.

[187] J. Van Zeben and A. Bobić, *Polycentricity in the European Union*. Cambridge University Press, 2019.

[188] M. Polanyi, *The logic of liberty: Reflections and rejoinders*. Routledge, 1951.

[189] D. A. DeCaro, B. C. Chaffin, E. Schlager, A. S. Garmestani, and J. Ruhl, “Legal and institutional foundations of adaptive environmental governance,” *Ecology and society: A journal of integrative science for resilience and sustainability*, vol. 22, no. 1, p. 1, 2017.

[190] C. Pahl-Wostl, “A conceptual framework for analysing adaptive capacity and multi-level learning processes in resource governance regimes,” *Global environmental change*, vol. 19, no. 3, pp. 354–365, 2009.

[191] P. D. Aligica, P. J. Boettke, and V. Tarko, *Public governance and the classical-liberal perspective: Political economy foundations*. Oxford University Press, 2019.

[192] A. Macintosh, “Characterizing e-participation in policy-making,” in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the.* IEEE, 2004, pp. 10–pp.

[193] J. Koivisto and J. Hamari, “The rise of motivational information systems: A review of gamification research,” *International Journal of Information Management*, vol. 45, pp. 191–210, 2019.

[194] J. Hamari, J. Koivisto, and H. Sarsa, “Does gamification work?–a literature review of empirical studies on gamification,” in *2014 47th Hawaii international conference on system sciences.* Ieee, 2014, pp. 3025–3034.

[195] L. Hassan and J. Hamari, “Gameful civic engagement: A review of the literature on gamification of e-participation,” *Government Information Quarterly*, vol. 37, no. 3, p. 101461, 2020.

[196] J. Stenros, “The game definition game: A review,” *Games and culture*, vol. 12, no. 6, pp. 499–520, 2017.

[197] I. Granic, A. Lobel, and R. C. Engels, “The benefits of playing video games.” *American psychologist*, vol. 69, no. 1, p. 66, 2014.

[198] V. Švábenskỳ, J. Vykopal, M. Cermak, and M. Laštovička, “Enhancing cybersecurity skills by creating serious games,” in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 2018, pp. 194–199.

[199] J.-N. Tioh, M. Mina, and D. W. Jacobson, “Cyber security training a survey of serious games in cyber security,” in *2017 IEEE Frontiers in Education Conference (FIE).* IEEE, 2017, pp. 1–5.

[200] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, and F. Smeraldi, “Cybersecurity games and investments: A decision support approach,” in *International Conference on Decision and Game Theory for Security.* Springer, 2014, pp. 266–286.

[201] T. Sommestad and J. Hallberg, “Cyber security exercises and competitions as a platform for cyber security experiments,” in *Nordic conference on secure IT systems.* Springer, 2012, pp. 47–60.

[202] J. Brynielsson, U. Franke, and S. Varga, “Cyber situational awareness testing,” in *Combatting cybercrime and cyberterrorism.* Springer, 2016, pp. 209–233.

[203] J. R. Raser, *Simulation and society: An exploration of scientific gaming.* ERIC, 1969.

[204] D. R. Ewoldsen, C. A. Eno, B. M. Okdie, J. A. Velez, R. E. Guadagno, and J. DeCoster, "Effect of playing violent video games cooperatively or competitively on subsequent cooperative behavior," *Cyberpsychology, Behavior, and Social Networking*, vol. 15, no. 5, pp. 277–280, 2012.

[205] D. A. Gentile, C. A. Anderson, S. Yukawa, N. Ihori, M. Saleem, L. K. Ming, A. Shibuya, A. K. Liau, A. Khoo, B. J. Bushman *et al.*, "The effects of prosocial video games on prosocial behaviors: International evidence from correlational, longitudinal, and experimental studies," *Personality and Social Psychology Bulletin*, vol. 35, no. 6, pp. 752–763, 2009.

[206] J. L. Geurts, R. D. Duke, and P. A. Vermeulen, "Policy gaming for strategy and change," *Long Range Planning*, vol. 40, no. 6, pp. 535–558, 2007.

[207] H.-G. Ridder, *Book Review: Qualitative data analysis. A methods sourcebook.* Sage publications Sage UK: London, England, 2014, vol. 28, no. 4.

[208] G. Morine-Dershimer, "Tracing conceptual change in preservice teachers," *Teaching and Teacher Education*, vol. 9, no. 1, pp. 15–26, 1993.

[209] T. S. Kuhn, *The structure of scientific revolutions.* Chicago University of Chicago Press, 1970, vol. 111.

[210] G. Burrell and G. Morgan, *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life.* Routledge, 2017.

[211] R. P. Mullaly and B. Mullaly, *Structural social work: Ideology, theory, and practice.* Oxford University Press, 1997.

[212] S. Deetz, "Describing differences in approaches to organization science: Rethinking burrell and morgan and their legacy," *Organization science*, vol. 7, no. 2, pp. 191–207, 1996.

[213] W. J. Orlikowski and J. J. Baroudi, "Studying information technology in organizations: Research approaches and assumptions," *Information systems research*, vol. 2, no. 1, pp. 1–28, 1991.

[214] P. Leavy, *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. Guilford Publications, 2017.

[215] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.

[216] L. D. Peters, A. D. Pressey, M. Vanharanta, and W. J. Johnston, "Constructivism and critical realism as alternative approaches to the study of business networks: Convergences and divergences in theory and in research practice," *Industrial Marketing Management*, vol. 42, no. 3, pp. 336–346, 2013.

[217] J. Mingers, A. Mutch, and L. Willcocks, "Critical realism in information systems research," *MIS quarterly*, vol. 37, no. 3, pp. 795–802, 2013.

[218] D. Byrne and C. C. Ragin, *The Sage handbook of case-based methods*. Sage Publications, 2009.

[219] J. Habermas, *Knowledge and human interests*. John Wiley & Sons, 2015.

[220] J. Eekels and N. F. Roozenburg, "A methodological comparison of the structures of scientific research and engineering design: their similarities and differences," *Design studies*, vol. 12, no. 4, pp. 197–203, 1991.

[221] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[222] O. Samuel-Ojo, D. Shimabukuro, S. Chatterjee, M. Muthui, T. Babineau, P. Prasertsilp, S. Ewais, and M. Young, "Meta-analysis of design science research within the is community: trends, patterns, and outcomes," in *International Conference on Design Science Research in Information Systems*. Springer, 2010, pp. 124–138.

[223] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision support systems*, vol. 15, no. 4, pp. 251–266, 1995.

[224] S. Purao, "Design research in the technology of information systems: Truth or dare," *GSU Department of CIS Working Paper*, pp. 45–77, 2002.

[225] J. Vom Brocke, A. Hevner, and A. Maedche, *Design Science Research. Cases.* Springer, 2020.

[226] Y. Barzel, "The market for a semipublic good: the case of the american economic review," *The American Economic Review*, vol. 61, no. 4, pp. 665–674, 1971.

[227] H. Demsetz, "The private production of public goods," *The Journal of Law and Economics*, vol. 13, no. 2, pp. 293–306, 1970.

[228] C. P. Kindleberger, "International public goods without international government," *The american economic review*, vol. 76, no. 1, pp. 1–13, 1986.

[229] M. Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with a New Preface and Appendix.* Harvard University Press, 2009, vol. 124.

[230] M. V. Pauly, "Mixed public and private financing of education: Efficiency and feasibility," *The American Economic Review*, vol. 57, no. 1, pp. 120–130, 1967.

[231] T. Yamagishi and K. Sato, "Motivational bases of the public goods problem." *Journal of Personality and Social Psychology*, vol. 50, no. 1, p. 67, 1986.

[232] P. A. Samuelson, "The pure theory of public expenditure," *The review of economics and statistics*, pp. 387–389, 1954.

[233] B. M. Fleisher, E. J. Ray, and T. J. Kniesner, *Principles of Economics.* Wm. C. Brown, 1987.

[234] E. Mansfield, "Economics: Principles, problems, decisions," *New York: WW Norton*, vol. 466, pp. 61–62, 1977.

Part II

Research Papers

Chapter 5

Research Paper 1: Systematically Understanding Cybersecurity Economics: A Survey

Mazaher Kianpour, Stewart Kowalski, and Harald Øverby - *Sustainability, 2021*

sustainability

Article

Systematically Understanding Cybersecurity Economics: A Survey

Mazaher Kianpour *, Stewart J. Kowalski and Harald Øverby

Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU Norwegian University of Science and Technology, 2815 Gjøvik, Norway; stewart.kowalski@ntnu.no (S.J.K.); haraldov@ntnu.no (H.Ø.)

* Correspondence: mazaher.kianpour@ntnu.no

Abstract: Insights in the field of cybersecurity economics empower decision makers to make informed decisions that improve their evaluation and management of situations that may lead to catastrophic consequences and threaten the sustainability of digital ecosystems. By drawing on these insights, cybersecurity practitioners have been able to respond to many complex problems that have emerged within the context of cybersecurity over the last two decades. The academic field of cybersecurity economics is highly interdisciplinary since it combines core findings and tools from disciplines such as sociology, psychology, law, political science, and computer science. This study aims to develop an extensive and consistent survey based on a literature review and publicly available reports. This review contributes by aggregating the available knowledge from 28 studies, out of a collection of 628 scholarly articles, to answer five specific research questions. The focus is how identified topics have been conceptualized and studied variously. This review shows that most of the cybersecurity economics models are transitioning from unrealistic, unverifiable, or highly simplified fundamental premises toward dynamic, stochastic, and generalizable models.

Keywords: cybersecurity economics; economics of information security; complex systems; socio-technical systems; meta-narrative literature review; sustainable digital ecosystems

check for updates

Citation: Kianpour, M.; Kowalski, S.J.; Øverby, H. Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability* **2021**, *13*, 13677. https://doi.org/10.3390/su132413677

Academic Editor: Bruce Morley

Received: 26 October 2021
Accepted: 4 December 2021
Published: 10 December 2021

1. Introduction

At the time of conducting this research, the world is being shaken by an unprecedented upheaval as the coronavirus pandemic has affected billions of people worldwide. This large-scale event has not only affected us in the physical dimension but also cyberspace. Elections, Olympic games, and wars quickly make their way into the cyber world, and adversaries can take advantage of these global incidents to attack people, organizations, and governments. These events have given the decision makers in the cybersecurity domain a pause for reflection. Moreover, the scholars focused on cybersecurity economics are trying to build a consensus on the need to have secure, sustainable hyper-connected digital societies through greater awareness, strong multi-stakeholder partnerships, and deep structural changes in key areas of institutional activities.

The importance of cybersecurity in digital ecosystems has resulted in a large stream of research that focuses on technical defenses and solutions, such as encryption, intrusion prevention systems, and access controls. In addition to the technical defenses, the sustainability of digital ecosystems is at least as much dependent on the aspects that can be explained more clearly and convincingly using the language of economics. However, research focusing on the economic aspects of cybersecurity is at an infant stage, despite four decades of research activity that was started in 1982 by Courtney [1]. He stated that a security control should not be implemented if it costs more than tolerating the problem. He also added that the selection of security controls requires a systematic approach with full recognition of interdependencies and cost–benefit relationships. The economic implications of decisions made in the context of cybersecurity are influenced by the presence of reinforcing features, such as complexity, deep uncertainty, and non-ergodicity.

The economic models with a neoclassical theoretical basis were among the most often used tools in the early stages of cybersecurity economics research. This school of thought imposes a set of assumptions on economics models, including rationality, representative agents, constant returns to scale, and cleared markets in the long-term [2]. However, as the maturity of the field increases, cybersecurity economics literature revealed models which are characterized by dynamic (i.e., accounting time), stochastic (i.e., representing random behavior of agents), and generalizable (i.e., describing the entire ecosystem) features. These models attempt to avoid the oversimplifying assumptions such as homogeneous agents, rationality, and optimizing behavior. Hence, they introduce additional variables to consider bounded rationality, uncertainty, or imperfect information. While a detailed discussion of this school and other schools is beyond this article's scope, we will discuss briefly how they have been applied for cybersecurity economics in Section 3.

This study provides a meta-narrative literature review of existing cybersecurity economics models applicable for cybersecurity investments, information sharing, sustainability, and cyber insurance. Our overall assessment of the literature is critical. The literature has succeeded in providing broad and intriguing coverage of the application of economic analysis to cybersecurity. It presents significant results consistent with complex systems and suggests the presence of the sorts of heterogeneity and interdependencies across agents. It also contributes to developing key competencies (e.g., system thinking, adversarial thinking, and anticipatory competencies) to advance security and sustainability in digital ecosystems. Yet, "The Global Risks Report 2021", published by the World Economic Forum, has categorized cybersecurity failures as clear and present dangers [3]. This category reveals concerns about lives and livelihoods. Moreover, a report by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, shows that in 2020, it was initially forecast that the investment in cybersecurity by the organizations would surpass USD 145 billion [4]. However, despite increasing cybersecurity spending, the annual cost of cybercrime, globally in 2020, is estimated at USD 1 trillion [4], and data breaches continue to proliferate [5]. Now, the question that arises here is whether these models have been effective in developing secure and sustainable digital ecosystems.

These numbers cast doubt over these models' effectiveness, particularly when they compare it with other areas of business investment and performance improvement. For example, the proposed models for cybersecurity investment, as one of the core issues in cybersecurity economics, mainly have limitations such as inaccurate estimates and applying complexity in real-world situations. Limited scenarios and inconsideration of constraints, type of organizations, and adversaries' strategies are common problems of the models that claim accuracy and simplicity. Therefore, our criticism is not that scholars fail to employ models according to the assumptions of particular rationality or perfect markets. Rather, they do not use models adequately and appropriately with respect to the purposefulness of individual behavior and systems' complexity. The limitations of the literature are not surprising given the novelty of cybersecurity economics as an interdisciplinary field. We believe that this field will experience an exploratory and dialectical empirical development. This process is critical for developing economically viable cybersecurity strategies and policies.

In the form of a literature review, this study critically reflects on the literature to build a deep understanding of cybersecurity economics and identify seven core issues that have been subject to analysis under this field. The first contribution of this study is the provision of different schools of economics employed in cybersecurity. The second contribution is presenting (1) the topics and challenges that have been investigated under the perspective of cybersecurity economics, (2) the characteristics of an efficient cybersecurity economic model, and (3) how this field has contributed to providing solutions to known and unknown problems within the cybersecurity domain. Finally, the third contribution is to demonstrate how particular research in economic aspects of cybersecurity has unfolded over time and shaped the kind of questions being asked and the methods used to answer them.

The remainder of this paper is organized as follows. In Section 2, we provide a brief background on the cybersecurity economics. Section 3 presents the theoretical underpinnings of cybersecurity economics models and the schools of thought employed to develop these models. The core issues of cybersecurity economics models are discussed in Section 4. The research methodology of this review is demonstrated in Section 5. The research questions are answered in Section 6. Section 7 concludes by summarizing the key findings of this article and provides insights for future research.

2. Background

The subject of this study is cybersecurity economics. Accordingly, a fundamental issue it must address is what makes cybersecurity economics a single subject of investigation. Indeed, cybersecurity and economics each constitute distinct types of investigation, as reflected in the fact that they have long been studied as two separate disciplines by two large independent groups of researchers, respectively, information and computer scientists and economists. Therefore, there might be barriers to understanding how together they constitute a single field of study. It can be argued that cybersecurity economics should be understood as an interdisciplinary field of study that falls between and combines cybersecurity and economics. However, this perspective faces the problem that there is more than one conception of how different disciplines are related.

Cat [6] presented a taxonomy of possible conceptions: interdisciplinary, multidisciplinary, cross-disciplinary, and transdisciplinary. The strategy adopted in this review is closest to the transdisciplinarity (i.e., a synthetic creation that encompasses work from different disciplines), which treats cybersecurity and economics as two different relatively independent systems of thinking that interact in a complex socio-technical system. A complex socio-technical system paradigm takes the interaction of different systems as the starting point and explains their relative interdependence regarding how they interact in social and technical settings. This paradigm enables us to capture the transformative effects that cybersecurity and economics might each have on one another. To develop a more clear understanding of these effects, this section continues to elaborate on how cybersecurity started to draw from economics.

The terms cybersecurity and information security are often used interchangeably. Solms and Niekerk argue that, despite the substantial overlap between cybersecurity and information security, the two concepts are not equal [7]. They posit that cybersecurity goes beyond traditional information security boundaries to include protecting information resources and other assets, including the human and cyber-physical systems. According to this viewpoint, which is also supported by the international standard ISO/IEC 27032:2012(E), in information security, a reference to the human factor usually relates to humans' role(s) in the security process. In cybersecurity, however, this factor has an additional dimension, namely the humans as potential targets of cyber attacks or even the humans that unknowingly participate in a cyber attack due to lack of awareness.

While ENISA concludes that there does not need to be a definition for cybersecurity [8], we provide a definition to avoid vagueness regarding what cybersecurity entails. Cybersecurity is basically the name of standard practices that involve the people, processes, and technologies in an organization, in a group, or stand-alone environments in which the computers and cyber-physical systems with valuable data are connected to cyberspace. Cybersecurity deals with the different procedures that create a secure environment by protecting the assets. According to ISO/IEC 27002, an asset is anything that has value to an organization [9]. Assets can be categorized into different subtypes based on their convertibility (current and non-current assets), physical existence (tangible or intangible assets), and usage (operating or non-operating assets) [10]. Some assets are relation specific. These assets are the results of one or both parties having made investments to support a particular relationship [11]. For example, people who work for a specific organization and learn skills that are valuable only for that specific organization are considered relation-specific assets. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

Valuation of these assets and the risks of loss or damage have been controversial topics in cyber risk management and cybersecurity economics. The valuation methods vary based on cost [12], market [13], and utility [14] of the assets. With the rapid development of information technology, digital assets have been recognized as critical parts of organizations. However, cybersecurity is not limited to digital assets. In the last decade, the increasing number of cyber attacks against physical assets and critical infrastructures (e.g., Stuxnet, Industroyer, Triton, etc.) has indicated that cybersecurity can be labeled as a serious cyber and physical challenge for organizations and governments.

An accurate valuation of assets is central to efficient investment in protecting them, capital budgeting, and strategic planning. This is why this process is changed if poor decisions have been and/or are being made. Much of the published research on cybersecurity economics has been focused on the economic valuation of the assets and finding the optimal security investment level in organizations to protect those assets [15–21]. However, cybersecurity economics not only is concerned with whether an organization is spending enough to secure their assets and whether the security budget is spent on the right security measures and controls [22,23], but is also concerned with how a digital ecosystem and its operating agents function and behave. Cybersecurity economics covers the regulatory changes and competitive pressures (e.g., how cybersecurity can be aligned with broader business processes [24]). It studies how resource allocation by governments and businesses satisfies the requirements of creating a resilient cyber environment for themselves and other agents [25]. Furthermore, cybersecurity economics focuses on the efficiency surrounding the decisions made as a result of incentives and policies that are designed to maximize the profit and trust within the environment [26].

Currently, there is no consensus on a definition of the term cybersecurity economics. Multiple studies have created their definitions, most of which are broad. Probably the most accepted definition for cybersecurity economics is an area concerned with providing maximum protection of assets at the minimum cost [27,28]. However, Rathod and Hämäläinen adopted a wider perspective to the economics of cybersecurity based on strategic, long-term thinking incorporating economics from the outset [26]. They stated that cybersecurity economics and analysis provide benchmarks for the economic assessment of national and international cybersecurity audits and standards. It also provides policy recommendations to align policies and regulations to ensure trust within a digital environment. Additionally, Ahmed argues that cybersecurity economics addresses the issues of protection of Information and Communications Technology (ICT) applications designed to facilitate the economic activities that normally face cybercrimes that cost the companies and countries a significant amount of money and disturb the economic and financial activities around the globe, as has been indicated in ICT-based sustainable development [25].

Despite the many different definitions of cybersecurity economics, all of these studies point out that cybersecurity economic situations are characterized by direct and indirect interdependencies among the agents involved. Each agent's behavior affects the available options of other agents and even the results that they can achieve. Given a particular situation and different options, which option do agents choose and why? Does the outcome satisfy them? Does it unintentionally leave other agents worse off while it has been an optimal decision for some of them? To answer these questions, we would imply that it is crucial to be aware that cybersecurity economics covers a broader range of situations than exchanging products and services for money. Rather, this field of study includes organizations having to decide how to value their assets and scarce resources and adapt economic theories to practice in complex, uncertain environments.

Cybersecurity economics studies include forces motivating stakeholders to invest in cybersecurity provision; market structures and regulatory structures; and environmental, institutional, and distributional consequences of the social decision situation. The studies also investigate the cybercrime economics and motivation, tools, and interest of actors in today's underground marketplaces. All in all, this paper defines cybersecurity economics as a field of research that offers a socio-technical perspective on economic aspects of cybersecurity, such as budgeting, information asymmetry, governance, and types of goods, to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems. A socio-technical perspective is essential for understanding and managing the state of cybersecurity today, as well as how to enhance it moving forward.

3. Theoretical Underpinnings of Cybersecurity Economics Models

Colander defines economics as the study of how human beings coordinate their wants and desires, given the decision-making mechanisms, social customs, and political realities of the society [29]. In this definition, the term coordination can mean many things. In our study of cybersecurity economics, we refer to coordination as the efforts to solve problems such as:

- What is the adequate level of cybersecurity and how much should we spend to provide this level.
- How and for whom to provide cybersecurity.
- Who needs to pay for interdependent and cascaded risks.

The answers to these questions, under the assumptions that agents have unlimited resources and complete information, operate in closed systems, and make rational choices, might be clear and straightforward. However, these assumptions are subject to criticism since they rely on unrealistic, unverifiable, or highly simplified fundamental premises. Furthermore, scarcity, incertitude, and ever-changing digital ecosystems make these questions complicated. Hence, understanding the interrelationships among them is central to dealing with the problems mentioned above. Scarcity means that the available resources to satisfy individuals' desires are too few. For example, organizations are faced with a shortage of skilled cybersecurity staff. By 2022, the global cybersecurity workforce shortage is projected to reach upwards of 1.8 million unfilled positions [30].

Moreover, laboratory studies in psychology indicate that attention is also a limited resource [31,32]. In given situations, individuals selectively concentrate on some information while ignoring other perceivable information. These situations embody two main elements: our desires and the resources to fulfill those desires. In the context of cybersecurity, these desires are constantly changing, developing, and partially determined by both society and technological advances. Moreover, the resources and means we employ to fulfill desires can affect those desires. Hence, the degree of scarcity is continually changing and subject to incertitude. Sterling introduced the concept of incertitude to distinguish between uncertainty and risk [33]. According to Figure 1, there are four ways of conceptualizing incertitude. *Risk* refers to situations in which there is moderate knowledge about calculating probabilities for different outcomes. *Ambiguity* differs from risk in the poorly defined characterization of outcomes. Further, *uncertainty* refers to a situation in which outcomes are known, but there is a poor basis for assigning probabilities to these outcomes. Finally, *ignorance* is a situation that combines poor knowledge about both outcomes and likelihood (i.e., a case of surprises).

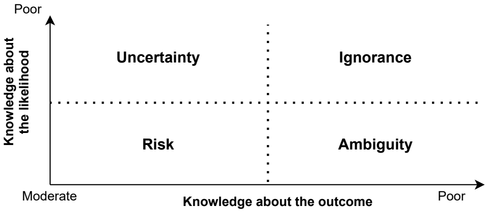


Figure 1. Types of incertitude. Adapted from [33].

When faced with scarcity, we need to make decisions. Decisions are made by comparing the costs and benefits of choices. Rational decision makers invest in cybersecurity if that investment yields a positive return or the marginal cost is less than that of the risk it eliminates. The proposed cybersecurity investment model by Gordon and Loeb [27], and introductory sequence of models based on it [34–36], premised a rational approach to managing risks and making decisions. Nevertheless, is this idealized conception also applicable in real-world situations? Real-world problems require reasoning about distributions over many different internal (e.g., decision-making mechanism, cognitive processes, emotional arousal, etc.) and external factors (e.g., business information, operating environment, available resources, etc.). During the last two decades, various economic models have been constructed to make inferences within cybersecurity by considering these factors. These models are based on generalizations and insights, called theories, about the workings of the cybersecurity market as well as on contextual knowledge about the institutional structure of the interacting stakeholders [37]. This knowledge is acquired from various resources such as individuals, groups, institutions, and systems. Figure 2 depicts that, according to the source of knowledge, economic theories are divided into two branches: microeconomics and macroeconomics.

Microeconomics is the study of individual choice and how economic forces influence that choice [29]. However, to analyze the entire economy built up from microeconomics analysis, everything becomes rather complicated. Therefore, to simplify matters by taking a different approach, macroeconomics studies the economy as a whole. In highly interconnected digital ecosystems, these two branches are very much interrelated. What happens in these environments as a whole is based on individual decisions, but individual decisions are made within an environment and can be understood only within their macro context. Research by Gartner shows that 60% of organizations are now working with more than 1000 third parties [38]. The increasing reliance on partners, sub-contractors, and suppliers contributes to the growing complexity of digital ecosystems and requires an understanding of both micro- and macroeconomics analyses.

Figure 2 shows the particular schools of economic thoughts employed in the cybersecurity economics literature. As the figure shows, some of the schools acquire their knowledge from different resources. Moreover, the problems that matter when looking at the situations from a particular school's perspective are depicted in this figure. It is beyond the scope of this paper to provide a full explanation of these schools. Yet, it is important we reflect on them to understand their characteristics.

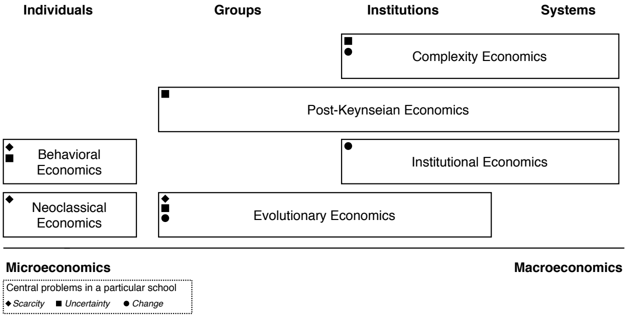

Individuals
Groups
Institutions
Systems
■ ● Complexity Economics
■ Post-Keynseian Economics
◆ ■ Behavioral Economics
● Institutional Economics
◆ Neoclassical Economics
◆ ■ ● Evolutionary Economics
Microeconomics
Macroeconomics
Central problems in a particular school
◆ Scarcity ■ Uncertainty ● Change

Figure 2. The required knowledge in cybersecurity economics model acquired from different resources such as individuals, groups, institutions, and systems. Source: compiled by the authors.

Neoclassical economics forms today's economic mainstream. Organization and allocation of scarce resources is the central economic problem from the neoclassical perspective. It implies that efficiency (i.e., the optimal usage of the available resources to maximize individual utility) is the most relevant evaluation criterion. Econometrics serves as an analytical tool. Mathematical models are used in the analysis of the economic system. It has been argued that rationality, selfishness, and equilibrium are fundamental to neoclassical economics [39]. These paradigmatic cores have been applied in cybersecurity economics by employing two different approaches: decision-theoretic and game-theoretic.

The decision-theoretic approach utilizes traditional risk assessment models to analyze organizations' spending on cybersecurity. Cavusoglu knows these methods are incomplete because of the security problem's strategic nature [40]. Several empirical studies support that attackers do not randomly select their targets and their attack strategies [41–43]. Hence, researchers proposed game-theoretic approaches that treat cybersecurity investment as a game between organizations and attackers [34,40]—or interdependent organizations [44,45]. Aligned with neoclassical economics, the ideal goal of these models is utility maximization. However, this is not the only goal in cybersecurity. In practice, cybersecurity decision makers need to seek how they can mitigate cyber risks, balance business needs and cybersecurity requirements, maintain compliance, and ensure cultural fit [46]. Moreover, the benefits and costs cannot be reliably calculated for cybersecurity since the value of cybersecurity investment comes from the avoidance of potential incidents and the loss reduction from an investment [47,48].

Considering that utility maximization is not the only goal in cybersecurity, neoclassical economics systematically neglects the complexity of our problems and our bounded set of fundamental capabilities, such as rationality, farsightedness, and influence. These limitations are addressed in other economics schools such as behavioral economics, evolutionary economics, and complexity economics. Behavioral economics takes up some of the neoclassical economics critiques by focusing on which decisions are made and what motivations lead to particular actions (in general, observable behavior of humans). In behavioral economics, the findings from psychology, social sciences, neuroscience, and cognitive sciences are transferred to the economic discipline to improve the reliability and precision of explaining human decisions and behaviors [49]. The research on behavioral economics suggests that individuals deviate from the standard model in three respects: *nonstandard preferences* (time preferences, risk preferences, and social preferences), *nonstandard beliefs* (overconfidence, the law of small numbers, and projection bias), and *nonstandard decision making* (framing, limited attention, menu effects, persuasion and social pressure, and emotions) [31].

For example, consider the utility function as a standard model. Individual i at time $t = 0$ maximizes expected utility subject to a probability distribution $p(s)$ of the states of the world $s \in S$:

$$\max_{x_i^t \in X_i} \sum_{t=0}^{\infty} \delta^t \sum_{s_t \in S_t} p(s_t) U(x_i^t | s_t). \tag{1}$$

The utility function $U(x|s)$ is defined over the payoff x_i^t of player i and future utility is discounted with a (time-consistent) discount factor δ. DellaVigna discusses how this function can be deviated from its main hypotheses [31]. The research on nonstandard preferences, beliefs, and decision making constitutes the bulk of the empirical research in psychology and economics. However, some of these topics are relatively new to the field of cybersecurity, and thus there is much that future work can explore. For instance, the results of a study by Kianpour et al. suggest that social preferences have moderating effect on the decision making under cyber risks and uncertainty [37]. With respect to the social preferences, the utility function is $U(x_i, x_{-i}|s)$, meaning that it also depends on the payoff of others x_{-i}. Risk preferences, on the other hand, have been studied more by the researchers under the topics of loss aversion [50,51], insurance [52–54], willingness to pay [55–57], and endowment effect [58,59].

As DellaVigna explains, the standard model in (1) assumes that individuals are normally correct about the distribution of the states $p(s_t)$. However, experiments suggest that they have systematically incorrect beliefs in three ways: overconfidence, the law of small numbers, and projection bias. In the context of cybersecurity, the recent reports show that when it comes to cybersecurity practices, there is general overconfidence among security professionals and C-levels [60]. NIST defines overconfidence as the tendency for stakeholders to be overly optimistic about either the potential benefits of an opportunity or the ability to handle a threat. Dong et al. discussed how overconfidence is negatively associated with information security investment and information security performance in organizations [61].

Nevertheless, incorporating this variable with more complex situations, such as budget constraints and risk interdependencies, could reveal more insights into the role of overconfidence in cybersecurity provision. As with many of the issues raised in this, there is limited literature on projection bias and the law of small numbers and projection bias. However, these issues concern the part of the decision-making process that probabilities need to be considered. Therefore, studying the impact of these beliefs can help us understand why decision makers underestimate cyber risks or underinvest in cybersecurity solutions.

Given the standard utility $U(x|s)$ and belief $p(s)$, individuals may make nonstandard decisions. This can be caused by different framing of a situation, the underweighting (or overweighting) of information because of limited attention, suboptimal heuristics used for choices out of menu sets, social pressure, and emotions. The framing effect is one of the many different cognitive biases that we can be susceptible to. Framing strategies (i.e., strategies for communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged [62]) have been studied extensively in the context of cyber risk [63–65] and cyber warfare [66,67]. A situation that is framed differently may elicit different responses [68]. Bruijn and Janssen described how evidence-based framing can be used to build cybersecurity awareness. They argue that, in cybersecurity policymaking, utopian or dystopian views might be counterproductive and result in complicating the problems [69]. The findings of another study show how news media framing can generate privacy tradeoffs in exchange for stronger cybersecurity prevention or economic gains [70]. When high societal risks are perceived through news media framing, individuals engage in privacy tradeoffs, encouraging them to comply with intrusive privacy initiatives. Unlike the framing effect, the impact of emotions also has been addressed in cybersecurity decision making. Blunden et al. investigated two threat-induced emotions after a cyber attack: fear and anxiety [71]. Their results show that fearful participants embrace avoidance as their safety behavior, while anxious participants appeal to surveillance and vigilance.

Moreover, Renaud and Dupuis have presented cybersecurity studies that use fear appeals [72]. They outline the literature's limitations and how cybersecurity researchers can study fear appeal models in field experiments rather than laboratory experiments. Many other biases are identified in cognitive psychology. However, unlike framing effects and emotions, other patterns of deviations from standard decision making within the context of cybersecurity are not well-addressed. With the extension of cybersecurity to susceptible areas such as military and critical infrastructures, investigating the impacts of other cognitive biases on people's decisions must be weighed alongside other topics to avoid inference and reasoning problems.

As we mentioned earlier, neoclassical economics ignores the complexity of the problems. Evolutionary economics and complexity economics, on the other hand, use computational and mathematical analysis to explore the complex structures and investigate how and why the systems change. These schools look at the evolutionary systems, not the systems continuously in or tending toward equilibrium. This emphasis on the changing nature of the systems appears to be the crucial feature within the context of cybersecurity. Cybersecurity is no longer a barrier to change [73]. Instead, it is considered as a business enabler or an influencer [74]. Consequently, topics including structural and technological changes, innovation processes, and capabilities development could be used in this domain to explain both change and stability. It should be noted that neoclassical economics can also incorporate dynamic elements such as path dependencies [75]. However, evolutionary economics deals with uncertainty and change in addition to the optimal usage of scarce resources to satisfy individual needs. Therefore, both knowledge and individuals are considered crucial phenomena. Methodologically, evolutionary economics assumes that agents' interaction leads to the formation of new entities and causes of a phenomenon known as emergence. These entities' characteristics cannot be reduced to the individual level, and the performance of the system is determined by the practical level of available knowledge shared among the individuals.

Shiozawa has identified a non-exclusive and non-comprehensive list of seven economic entities being subject to evolutionary changes: economic behavior, commodities, technology, institutions, organizations, systems, and knowledge [76]. While a decision of an individual can change economic behavior, institutions require broad social support to change. For example, the internet is a new system that has quickly become an institution. The present form of this system evolves autonomously, and no one can completely control it, albeit its basic concepts are the results of human design. This category shows that evolutionary economics is compatible with other schools of thought such as behavioral economics, institutional economics, and complexity economics. However, they are different in their perspective, fundamental assumptions, independence of context, etc.

These schools, known as Heterodox economics, have been applied within the context of cybersecurity using different methods such as evolutionary game theory, behavioral game theory, simulation, agent-based modeling, and system dynamics modeling. Different works have relied on the certain concepts of these schools to provide detailed descriptions and arguments grounded in economics about different aspects of cybersecurity and cyberspace. For example, drawing from institutional economics, Kuerbis and Badiei presented a conceptual model to describe the cybersecurity governance landscape based on three governance structures that are commonly noted in institutional economics: markets, hierarchies, and networks [77]. Lindsay has also combined concepts from international relations theory and new institutional economics to understand cyberspace as a complex global institution with contracts embodied in both software code and human practice [78]. He argues that constitutive inefficiencies (market and regulatory failure) and incomplete contracts (generative features and unintended flaws) create the vulnerabilities that hackers exploit and increase the likelihood and magnitude of cyber conflicts.

4. Cybersecurity Economics Models: Core Issues

In 2001, Anderson [79] asserted that providing security of information assets is more than focusing on technological risks. He added that the management of information security is a much deeper problem that has to be explained more clearly and convincingly using the language of economics. Since then, various attempts were made to provide intelligence for cybersecurity decision makers and assess the cyberspace environment using economic models. Most of these models use "Security Level" as an aggregated economic variable to determine the efficiency of the models [80]. However, Böhme and Nowey outlined the economic metrics of security, including annual loss expectancy (ALE), the expected net benefit of investment in information security (ENBIS), the expected benefit of investment in information security (EBIS), and return on security investment (ROSI). Some of the models also defined new metrics to cover more details in their proposed models. For example, References [27,81] defined the security breach probability function, which maps the monetary value of the investment in security and the probability of incurring a pre-defined loss. These metrics enable us to compare the proposed solutions to budgeting problems (e.g., investment, externalities, and insurance). However, budgeting is not the only core issue of cybersecurity economics. In this section, we highlight issues such as economic efficiency, interdependent risks, information asymmetry, and governance.

The analysis of investment models and suggestions of new models have attracted quite a lot of interest in the economics of cybersecurity. The security investment models are used to determine the optimal level of security investments to reduce security risks in the organization effectively. This line of research was preceded by Gordon and Loeb, in which an organization's optimal amount to invest in cybersecurity activities was studied [27]. They presented the importance of understanding risks involved in the investment in cybersecurity in order to assess the expected benefit of the investment. The Gordon and Loeb model examines how the firm's optimal level of cybersecurity expenditures varies with the probability that a cyber attack will be successful in the absence of any cybersecurity expenditures and the expected loss to the organization if the attack is successful. A number of researchers have conducted research in order to analyze and extend this model [81–84]. There are also a number of studies that suggested new models to determine the optimal spending on cybersecurity activities or adoption of new secure technologies (e.g., fog computing [85]). Table 1 shows our categorization of some of these models, which have drawn attention by academic and practitioner literature.

Table 1. Cybersecurity investment models.

Approaches	Description	Works
Microeconomics	Game Theory	[16,19,86,87]
	Behavioral Economics	[88,89]
	Combinatorial Approach	[90]
Financial Analysis	Return on Security Investment (ROSI)	[44,91–93]
	Net Present Value (NPV)	[94,95]
	Internal Rate Return (IRR)	[96]
	Combinatorial Approach	[97]
Management Approaches	Decision Theory	[17,98]
	Risk Management	[36,99,100]
	Organization Theories	[101]
	Combinatorial Approach	[102]
Combinatorial Approaches	Management and Microeconomics	[18,27,35,103]
	Management and Financial Analysis	[97]

As this table shows, researchers have employed different approaches to build cybersecurity investment models. One of the most popular methods is game theory. Game theory is a tool to analyze the structure that lies beneath the social interaction, its possibilities and opportunities, the development paths of interactions, and less likely and more likely outcomes [104]. The financial analysis utilizes organization's information from the most recently available years of accounts. This approach is becoming more popular as the impact of cyber incidents on equity market volatility across publicly traded corporations is increasing [105]. For example, a study by Szubartowicz and Schryen indicates that after fundamental security incidents in a given industry, the stock price will react more positively to an organization's announcement of actual cybersecurity investments in comparison to announcements of the intention to invest [106]. Overall, they also found that the lowest abnormal return can be expected when the intention to invest is announced before a fundamental cybersecurity incident and the highest return when actually investing after a fundamental cybersecurity incident in the respective industry.

Management approaches in constructing cybersecurity models have drawn increasing attention because cybersecurity now has a high priority among managers, policymakers, regulators, and enforcement officials across various sectors. Tisdale knows cybersecurity is a knowledge management problem due to the amount of data, perishability of data, technology turnover, and the multitude of stakeholders and information involved [107]. Therefore, methods such as business intelligence [108] and big data analytics [109] can assist managers to find new solutions to emerging problems in this field. This table also shows several models that employed combinatorial approaches, both inter- and intra-category. These approaches allow the models to be flexible and adaptable as they cover more details, such as interdependent security and human expectations. For example, Reference [102] leverages the economics models of [27,35] and applies the expected utility theory and the presented approach in [41] to understand how cybersecurity investments change breach probabilities and potential loss.

In addition to the investment in cybersecurity, externalities and cyber insurance have been rapidly developing topics in cybersecurity economics. Anderson and Moor [110] have borrowed this term from economics to describe the side effects of security operations and transactions. Externalities can be positive (e.g., scientific research and development) or negative (e.g., cybercrimes or security weaknesses). A different set of externalities can be found when we analyze stakeholders' decisions and operations made within the context of cybersecurity. Varian proposed a model to examine whether the defense depends on the sum of the individuals' efforts, or the minimum effort by the free-riders, or the maximum effort by some of the defenders [111]. This is an important challenge if cybersecurity is treated as a public good and poses a problem known as the tragedy of the commons [79]. This category shows that cybersecurity economics includes aspects of leadership, and societal and corporate culture, and encompasses larger economic and sociopolitical elements such as national and international security.

Although measuring the effectiveness of the investment in cybersecurity plays a vital role in decision making, the economics of cybersecurity has other considerable aspects that we need to investigate as well. Hausken [112] emphasizes the importance for the organizations to understand how they can make the most efficient outcome of their cybersecurity strategy planning. This requires a wider perspective towards this issue. Economics of cybersecurity studies factors that actors perceive as relevant for cybersecurity decisions and affect actions by individuals, groups, organizations, and governments, in both the cybersecurity market's social and technical components. These factors are externalities [113,114], information asymmetry [86,99], and alignment of incentives [114,115]. Furthermore, Dacus and Yannakogeorgos [116] proposed an incentive framework to motivate cybersecurity stakeholders to devote more effort to secure their environment. They point out that information asymmetry can cause a moral hazard. Moral hazard arises when cybersecurity service providers' priorities do not match the client's (U.S. Federal Government, in this case) priorities and their incentives are not aligned.

The economic impact of regulations and policies to increase organizations' investments in cybersecurity activities is also discussed in [117–119]. Massacci et al. [120] investigated the optimal way to regulate cybersecurity for critical infrastructure operators. They presented a cybersecurity economics model to show that operators will eventually stop investing in cybersecurity, depending on the incentives, and care only about compliance. They compared the effectiveness of rule-based with risk-based regulations on the incentive for the security investment by employing a game-theoretic model. They concluded that rules could apply to less security-mature actors and actors above a certain maturity threshold would be subject to a risk-based regulatory framework. In addition to investment and policies, we identified seven areas pertaining to cybersecurity economics which have been subject to analysis and explored under this field. These areas are discussed in more detail under Research Question 2 in Section 6.

5. Research Methodology

To pursue this paper's objectives, conceptual, empirical, and analytical articles published in cybersecurity economics research were analyzed. Given that cybersecurity economics research is a highly interdisciplinary research field, a meta-narrative review approach is used [121]. Meta-narrative review is one of the new approaches to qualitative and mixed-method systematic review. This form of review is especially designed for reviewing topics that have been conceptualized and studied variously by different groups of researchers. It can be used to overview a complex topic area, highlighting the relative strength and limitations of the respective research approaches. This does not mean that we need to know everything about every discipline we are using.

We begin to understand how different paradigmatic assumptions shape different disciplines and perspectives we are drawing on. This adaptation enables us to conduct an inquiry-driven literature review rather than discipline driven. It means that the scope is defined by the need of the subject matter, not determined and guided by the parameter of the discipline [122]. Unlike other literature review methods, such as realist reviews, meta-narrative reviews are primarily concerned with how issues were researched rather than synthesizing the findings and so can be considered a form of multi-level configuring mapping rather than synthesis of research findings [123].

The review starts by developing five research questions that the study sets out to answer. Table 2 shows the identified research questions. A set of search terms are selected from these research questions. We then use the different combinations of these search terms to find relevant studies in academic databases. The focus is not to cover every article published on the topic, but rather to provide a review of different studies which enable us to answer the questions in Table 2. Therefore, we applied inclusion, exclusion, and quality assessment criteria on the identified studies and shortlist the most relevant studies. These studies are referred to as selected studies. They are a combination of early articles (when the concept of cybersecurity economics first appeared), the most cited articles, and more recent articles.

Table 2. Research questions.

RQ1	What are the characteristics of an efficient cybersecurity economic model?
RQ2	What challenges have been addressed by proposing the existing economic models?
RQ3	What are the main issues faced by the current cybersecurity economic models?
RQ4	What data is needed to reliably assess the performance of a cybersecurity economic model?
RQ5	How has cybersecurity economics contributed to providing solutions for known and unknown problems within the cybersecurity domain?

As discussed in Section 2, there are controversial arguments in the literature regarding the definitions of "cybersecurity" and "information security". Consequently, we decided to use both keywords as the primary search terms. For the secondary terms, we used keywords such as model, theories, and analysis. Finally, we constructed the search string using "AND" and "OR" Boolean operators to link the search terms. Table 3 shows the list of primary and secondary search terms and the search string. We used the search string to look for relevant studies in five databases, presented in Table 4. Although we did not specify a time range for the search, the oldest finding based on this search string is the Gordon and Loeb model [27] published in 2002 (ACM Library). According to Scopus, this article has been cited by 660 documents, which is the highest number of citations in the list of our findings. Moreover, based on Google Scholar, this article has the highest number of citations (1563 up to date of search) in the field of cybersecurity economics. After the Gordon and Loeb model, "Why information security is hard-an economic perspective" by Ross Anderson [79] has acquired the highest number of citations (Scopus: 357, Google Scholar: 1096) in the field of cybersecurity economics.

Table 4 shows the number of findings using our search string in academic databases. We found that many of the studies were indexed by more than one database. Therefore, to avoid duplicates, we screened the results manually and removed the 73 identical results.

Study Selection

We selected the studies in two phases. In the first phase, we excluded according to the criteria presented in Table 5. Our study is not a Multivocal Literature Review (MLR). MLR is a form of a systematic literature review which includes the grey literature (e.g., blog posts, videos, and white papers) in addition to the published (formal) literature (e.g., journal and conference papers) [124]. After exclusion of the results, 385 studies were selected. Then, we applied the inclusion criteria (see Table 6) to identify the most relevant studies to our research questions. A total of 62 studies passed our inclusion criteria. In the second phase, we applied the quality assessment listed in Table 7 to the studies identified in the first phase. After this assessment, 28 studies were selected.

Table 3. Search terms.

Criteria	Description
Primary Search Terms	cybersecurity economics, information security economics, economics of cybersecurity, economics of information security, cybersecurity investment, cybersecurity spending
Secondary Search Terms	model, theories, framework, analysis
Search String	("cybersecurity economics" OR "information security economics" OR "economics of cybersecurity" OR "economics of information security" OR "cybersecurity investment" OR "cybersecurity spending") AND ("model" OR "theories" OR "framework" OR "analysis")

Table 4. Search results (date: 27 August 2021).

Database	Number of Results
IEEE Xplore	26
SpringerLink	489
ScienceDirect	124
ACM Library	62
Total	701
Total (without duplicates)	628

Table 5. Exclusion criteria (EC).

ID	Description
EC1	Short papers, extended abstracts, and studies that do not provide significant new ideas or insights.
EC2	Gray literature (e.g., blog posts, videos, and white papers).
EC3	Non-English studies.
EC4	The study mainly or exclusively investigates non-economic approaches of cybersecurity (e.g., purely risk management or loss prevention expenses).

Table 6. Inclusion criteria (IC).

ID	Description
IC1	The study describes the theoretical function of the employed economic theories and proposed models.
IC2	The study describes the significance of proposed model and provides insights about the application of the model in prediction and management of novel cybersecurity challenges.
IC3	Research objectives are clearly defined in the study.
IC4	The study proposes a new model or provides details of employing existing economics models in cybersecurity domain.
IC5	The study focuses on cybersecurity domain (i.e., not only information security, cyber-physical systems security, etc.).

Table 7. Quality assessment criteria (QAC).

ID	Description
QAC1	Are the research objectives clearly defined in the study?
QAC2	Does the study propose an artifact, or provide an analysis or extension of an existing artifact?
QAC3	Is the artifact clearly defined and validated in the study?
QAC4	Is the artifact compared to existing artifacts?
QAC5	Does the study provide insights and implications about the role and importance of the proposed artifact?
QAC6	Does the study consider the novel and emerging problems within the context of cybersecurity?

6. Data Synthesis

In this section, we investigate the selected studies listed in Table 8 to answer the research questions in Table 2.

Table 8. The list of the selected studies.

ID	Title	Year
[S01]	Institutional influences on information systems security innovations [125]	2012
[S02]	Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints [18]	2013
[S03]	A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis [126]	2014
[S04]	The impact of information sharing on cybersecurity underinvestment: A real options perspective [127]	2015
[S05]	Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment [128]	2019
[S06]	Cybersecurity investments in a two-echelon supply chain with third-party risk propagation [20]	2020
[S07]	Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers [120]	2016
[S08]	Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth [25]	2020
[S09]	Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements [129]	2013
[S10]	Coordination in network security games: A monotone comparative statics approach [83]	2012
[S11]	A game theory model of cybersecurity investments with information asymmetry [86]	2015
[S12]	Competitive cyber-insurance and internet security [130]	2010
[S14]	Increasing cybersecurity investments in private sector firms [131]	2015
[S15]	Should your firm invest in cyber risk insurance? [132]	2015
[S16]	Returns to information security investment: Endogenizing the expected loss [133]	2014
[S17]	Security investment and information sharing under an alternative security breach probability function [134]	2014
[S18]	The economic cost of publicly announced information security breaches: empirical evidence from the stock market [135]	2003
[S19]	Secure or Insure? A Game-Theoretic Analysis of Information Security Games [136]	2008
[S13]	Allocation of resources to cybersecurity: The effect of misalignment of interest between managers and investors [137]	2015
[S20]	Measuring the cost of cybercrime [138]	2013
[S21]	Investment decision on information system security: A scenario approach [98]	2009
[S22]	The economics of cybersecurity: Principles and policy options [113]	2010
[S23]	Security decision support challenges in data collection and use [139]	2010
[S24]	Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment [140]	2013
[S25]	The economics of information security investment [27]	2002
[S26]	Sharing information on computer systems security: An economic analysis [141]	2003
[S27]	Robustness of optimal investment decisions in mixed insurance/investment cyber risk management [100]	2020
[S28]	Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem [142]	2021

RQ1. What are the characteristics of an efficient cybersecurity economic model?

Economic models are theoretical constructs and conceptual frameworks that aid in the understanding, illustrating, and/or prediction of human behavior and complex processes. These models are methodologically used to investigate, theorize, and establish argumentative frameworks that represent the real world. The literature of cybersecurity economics shows that this area is being treated as an interdisciplinary field. Accordingly, the models proposed in this field draw concepts and techniques from a number of different disciplines, including organizational studies, complexity science, psychology, computer science, and sociology. Although each of the disciplines describes an efficient model in its own distinct way, nevertheless, when examined together, the scholars express efficient cybersecurity economic models as having five main properties. These properties go beyond the classical assumptions of rationality, optimization, and dynamic consistency. We believe that such assumptions are better considered as hypotheses that should be tested or conjectures that should be proved, and not fundamental characteristics of efficient economic models.

- Simplicity: The principle of simplicity has been largely accepted in science and it has been applied in different fields including economics. In the scientific methods, simple or parsimonious models prevent the researchers from manipulating the model so that it overfits the available facts by relying on relatively few special assumptions. Overfitting is a modeling error that occurs when a model works well in a given situation but fails to make accurate and reliable out-of-sample predictions. For example, [S01] incorporates a large set of qualitative biases. This model is non-parsimonious since the selective combination of those biases enables the researcher to adjust the model so that it can explain almost any pattern of observations. Likewise, complex budget constraints in [S02], makes the model relatively non-parsimonious. It can be argued that more flexible models enable the researchers to combine many elements and factors in the real world. However, this produces a false impression that the model has real explanatory power whereas it just makes it easy to explain in-sample data.
- Generalizability: If the results of a model are broadly applicable to a wide range of settings, the model is said to have good generalizability. The generalizability of a model's results depends on the researcher's ability to separate the "relevant" from the "irrelevant" facts of the study, and then carry forward a judgment about the relevant facts [143]. This would be easy if we always knew what might eventually turn out to be relevant. For example, uncertainty and complexity of the problems in [S02] and [S03] have caused to propose models with poor generalizability. As we mentioned earlier, agents make intertemporal choices within the context of cybersecurity economics. Therefore, a generalizable model of intertemporal choice (e.g., [S10]) could be used to study decisions with consequences that occur in the near-term and long-term future. Studies such as [S19], [S20], and [S21] attempted to propose generalizable models to unveil important patterns in systems' behavior.
- Empirical verifiability, applicability, and reproducibility: The empirically verifiable models are consistent with the available data and do not generate predictions that can be falsified by the data. If the researcher figures out that his model is empirically verifiable only if a certain effect is not present, then he must specify the domain of applicability of his model. The models are not intended to have universal applicability. They can be specialized to cases in which the arguments are evaluated. For example, models with homogeneous agents (e.g., [S12]) do not provide an ideal test for real-word settings that agents are characterized by their own culture, structure, machines, and methods. However, as argued in [S23] and [S24], the researchers have restricted their model to situations in which this effect is absent by stating the domain assumptions.
- Predictive precision: High predictive precision is desirable to facilitate model evaluation. This characteristic refers to how close the model's predictions are to the observed values. For example, [S07] allows a prospective test of theoretical understanding to generate testable predictions in changes that could occur in regulatory systems, depending on the combination of operators' incentives. Models with predictive precision are useful tools for decision makers who are trying to forecast future events or the consequences of new policies [144].

- Tractability: The degree to which a model admits convenient analysis and demands time, or other computational resources, with increasing its input size, is captured by tractability of a model. For example, [S11] is easy to implement and is manageable for more complex problems. However, [S14] and [S09] have not been able to provide a feasible solution. Consequently, they ignored the interaction among the agents in their proposed models to avoid an intractable problem.

RQ2. What challenges have been addressed by proposing the existing economic models?

Based on the selected studies, we identified issues and challenges that have been addressed and discussed by the literature of cybersecurity economics. We have classified these challenges into five categories. We acknowledge that this list is not exhaustive. However, it covers the most important problems that have been tackled or are yet to be studied in depth (e.g., rent-seeking behavior and lock-in). We discussed several of these challenges, such as investment and policies, as the main core issues of cybersecurity economics, in Section 4. Here, we outline the rest of issues that have received wide attention as well.

- **Budgeting** is an integral part of running any business efficiently and effectively. A budget is an estimation of revenue and expenses over a specified future period of time, and it can be made for a person, a group of people, a business, or a government. The budget development process plays a vital role in setting goals, measuring outcomes, and planning for contingencies.
  - *Investment* is a part of an overall budget development and expenditure management processes. Finding optimal investment strategies to balance cybersecurity risks and spending in security measures and controls has been a topic of major importance in cybersecurity economics.
  - *Externalities* or spillover effects occur when the benefits or costs of providing cybersecurity are not fully reflected in the budget development process. Overcoming externalities, both from public and private sectors, is important to avoid future budget deficiencies. Regulation is considered the most common solution to offset the effects of externalities [114].
  - Insurance is a contract in which an agent receives financial protection against losses from an insurance company. Insurance policies are used to hedge against the cybersecurity risks and cover the business' liabilities in the event of a cyber attack. By increasing the severity of financial consequences of cyber attacks, more businesses are turning to cybersecurity insurances. The literature of cybersecurity insurance has been focusing on determining how much cyber insurance businesses need to help insurers to understand the demand [145]. Moreover, uncertainty of outcomes, reinsurance (i.e., insurers lay off the risk to another capital source), and scale are problems that would suggest an increase in prices, hardening risk transfer, and influx of capital [S27].
- **Economic efficiency**, depending on the context, has various definitions in economics. For the sake of this review, we define economic efficiency as a situation in which no agent can make more profit without making at least one agent loss thereof.
  - *Misallocation of resources* indicates a state in which all resources are not allocated to serve each agent in the best way possible. The models that address this challenge are built based on the scarcity hypothesis. This hypothesis is the original source of methods such as the zero-sum games, comparative advantages, marginal returns, and time discount.
  - *The type of goods* that cybersecurity would treat would significantly influence the overall structures and success of cybersecurity economic models. According to Samuelson, there are four types of economics goods: private, common, club, and public goods [146]. The controversial arguments on how cybersecurity should be treated based on Samuelson's typology started in the last two decades [147].

    Any of these types raise issues that might result in reduced economic efficiency through misallocation of resources, inefficient cybersecurity provision, and potential national and international insecurity. For example, attempts at managing free-riding problem ([S19]) and rent-seeking behavior is at the center of models that consider cybersecurity as a public good [148].

- **Interdependent risks** are common in today's hyper-connected world. The risks faced by any one agent depend not only on its choices but also on those of all others with which it is directly or indirectly interacting.
    - *Network effects* are phenomena whereby increased numbers of people or participants improve the value of a good or service. Positive and negative network effects have been extensively studied within the context of software security economics [149].
    - *Lock-in effects* refer to situations in which users are dependent on a single vendor or supplier for a specific service or product and cannot move to another vendor without substantial costs. Recently, companies (e.g., Apple and Microsoft) increase their lock-in through security mechanisms. This phenomenon can be investigated in terms of control, governance, and dominance of organizations or groups such as Trusted Computing Group within the security value chain.
    - *Supply chains risks* associated with digital transformation of supply chains globally are increasingly becoming part of the enterprise risk listing and supply chain management. Modeling the target system, identifying threats, and analyzing countermeasures are three main issues that require systematic studies and socio-technical analyses to mitigate this type of risk [150].
- **Information asymmetry** deals with the situation where one party possesses more information than the other party. A lack of equal information results in adverse selection and moral hazards. All of these economic weaknesses have the potential to lead to market failure. Moral hazard is a situation where there is a tendency to take undue risks because the costs are not borne by the party taking the risk. Our tendency toward technological ubiquity, the unclear relationships between technology manufacturer and user, the inherent complexity of technology, and the network effects inherent to connected technologies are some of the factors that help this failure [151].
- **Governance** effectively coordinates the security activities of organizations and enables the flow of security information and decisions around them. Governance defines the rules and procedures for decision making. Governance is important because it specifies the structure and distribution of rights and responsibilities among the different agents in the system.
    - *Coordination* among different agencies and stakeholders involved in performing cybersecurity functions and practices, such as response to threats or incidents and cyber crisis management, has been studied in terms of incentives, costs, and business alignment. However, there are still problems with regard to economic complexity of the coordination procedures and dependable enforcement of effective measures.
    - *Cybersecurity Policies, Regulations, and Rules (PRR)* are the areas that have involved public and private sectors in many forms of self- and co-regulations since the emergence of the internet. In this regard, the dominated notion is that cybersecurity policymaking and regulations require multifaceted strategies and recognition of the significant role that economic analysis plays to determine the actual need or effectiveness of these regulations [152].
- **Cybercrimes** are global and have strong externalities. Many academic studies and industrial documents examine the costs and losses caused by cybercrime. Some works estimate the overall costs, others evaluate the costs of individual countries, while industrial documents even measure losses of certain organizations regardless of or considering their size and technological development. For example, [S20] is one of the

first studies of measuring the costs of cybercrime. The authors continued this work seven years later to report major changes that significantly influenced the results of the original study [153].

- **Sustainability** of cybersecurity providers and services is increased by better formulation of business strategies and policies. For example, [S28] discusses how, to achieve sustainability of the digital ecosystems, finding a balance between the values obtained by the stakeholders is essential. If any of the stakeholders do not gain sufficient value, the entire ecosystem will collapse. Hence, promoting secure and sustainable properties is becoming a requirement in both development processes of cybersecurity products and services [154].

Table 9 shows the main challenges that are addressed by the selected studies. The diversity of these challenges shows that cybersecurity economics is not limited to the financial and budgeting issues, but it also covers politics, coordination, and other organizational topics.

Table 9. The main challenges addressed by the selected studies.

ID	Challenges
[S01]	Economic Efficiency and Governance
[S02]	Investment
[S03]	Supply Chain
[S04]	Investment and Information Sharing
[S05]	Investment
[S06]	Supply Chain and Investment
[S07]	Policies, Regulations, and Rules (PRR)
[S08]	Externalities
[S09]	Insurance
[S10]	Coordination and Network Effect
[S11]	Information Asymmetry
[S12]	Moral Hazard
[S13]	Misallocation of Resources
[S14]	Types of Goods and PRR
[S15]	Insurance
[S16]	Investment
[S17]	Investment and Information Sharing
[S18]	Economic Efficiencies
[S19]	Types of Goods
[S20]	Cybercrime
[S21]	Investment
[S22]	Policies, Regulations, and Rules (PRR)
[S23]	Governance
[S24]	Policies, Regulations, and Rules (PRR)
[S25]	Investment
[S26]	Information Sharing
[S27]	Insurance
[S28]	Sustainability

RQ3. What are the main issues faced by the current cybersecurity economic models?

Recently developed cybersecurity strategies and policies have recognized that cybersecurity is a continuously evolving phenomenon in a complex socio-technical system in which multistakeholder governance processes and multilateral approaches are required to enhance cybersecurity posture in organizations and nations. Despite this understanding, the field of cybersecurity economics continues to face challenges that limits the applicability, effectiveness, and functionality of proposed models and analysis. Here, we highlight five major challenges that have been pointed out in the literature of cybersecurity economics. The first challenge that has been extensively recognized in the literature is complexity. If organizations, societies, and markets are viewed as complex and out-of-equilibrium systems, understanding non-linear, adaptive, and evolutionary patterns which emerge from system dynamics and agents' behavior in network structures is important for researchers. To tackle this challenge, the researchers need to reconsider the dominant equilibrium thinking in their models and shift from focusing on proposing models to optimize and predict system equilibrium to manage the complexity of cybersecurity better. This has also been recognized in other areas such as financial market regulations [155], energy [156], and healthcare policies [157].

The second challenge is that most economic models rest on a number of assumptions that are not entirely realistic. For example, it is often assumed that the decision makers are assumed to be rational and to have perfect information. There is growing literature in economics that shows humans do not have the processing capacity to be perfectly rational, even if they had perfect and complete information. Therefore, any analysis of the results and application of the proposed models must consider the inaccuracies that compromises the model based on these assumption. In addition to the unrealistic assumptions, the model overlooks issues that are important to the question being studied, such as externalities and interdependencies. These concepts intertwine with bounded rationality, cognitive dispositions, and social preferences [37].

The third challenge is the difficulty in measurement and quantification of the psychometric variables, such as the perceived value of cybersecurity, perceived cyber risks, and willingness to pay/collaborate. When the researchers neglect these variables, their model cannot provide full explanations or correct predictions of the phenomenon under study. The lack of reliable instruments to determine the indicators of these latent constructs contribute to the difficulty in measuring them. Another important challenge is the tension between rigor and relevance across cybersecurity economics models. The models that are purely theoretical or expressed mathematically are prone to poor relevance and applicability. The main question here is if a tradeoff must exist between rigor and relevance. If yes, what is the right balance between rigor and relevance in the study? To answer these questions, the researchers need to understand the system, identify the significant constructs, and use scientific methods that promote the systematic uptake of research findings and other evidence-based practices into routine practice.

Finally, the fifth challenge is the arising problem of parameter identification in construction of models using econometrics. Econometrics is the application of statistical and mathematical methods using observational and empirical data to develop new theories or test hypotheses. In all of the preceding sections, we discussed that the behavior, structure and characteristics of the environment, and the agents that operate within it do have an influence on the cybersecurity posture of the system as a whole. However, the situation is complicated when it comes to empirically testing such propositions. As Manski has pointed out, the propensity of agent behavior can vary with the behavior of group (i.e., contagious effects) or with exogenous characteristics of the group (i.e., contextual effects). It also can be similar to the group as they face a similar institutional environment (i.e., correlated effects).

To give an example, suppose that we observe an increase in the cybersecurity spending of three aluminum companies (Norsk Hydro in Norway, Kaiser Aluminum in America, and Hindalco in India) in 2020. A natural inference would be that they raised their investment due to the perceived cyber risk after the cyber attack against Norsk Hydro in 2019. However, on careful investigation, we find Kaiser Aluminum raised its investment due to the adoption of new information technology systems [158] and Hindalco due to the huge investment in capacity building after unveiling major capacity expansion plans in UltraTech (another subsidiary of the Aditya Birla Group). The question then is how these two possibilities can be distinguished. If you want to determine the importance of network effect in this example, what is most lacking is dependable empirical evidence and observational data.

RQ4. What data is needed to reliably assess the performance of a cybersecurity economic model?

Adequate data are critical in verification, validation, and assessment of the proposed economic models. The models often assist the researchers in considering what kind of data is useful to provide a foundation for investigations and explorations. As we discussed in the RQ2, cybersecurity economic models are developed with respect to a particular phenomenon or class of phenomena (e.g., budgeting, regulations, economic efficiency, etc.). To explain the phenomenon and test the models' key implications, the researchers use different types of data. The selection of type might be justifiable with regard to the research questions, scientific method, and availability. In this review, we identify five data types that were used in the studies:

- Observational data are captured through observation of agent's and system's behavior and their interactions in the real world. It is collected using methods such as observation by human or artificial sensors and open-end surveys. Since observational data are captured in real-time, the reproducibility of data would be difficult or, in some cases, impossible. [S03] has used observational data to assess the performance of the proposed model.
- Empirical data are also collected by means of senses and observation of behavior and patterns. However, this process is through experiments. Within the experiments, the experimenter can either control the conditions or not. Whereas the collected data from controlled and uncontrolled experiments can be qualitatively similar, their quantitative differences could be significant. Empirical data are captured when the conditions are not controlled, and they will be recorded along with the results. This type of data is often reproducible. Studies [S01], [S05], [S08], and [S14] have used empirical data to validate and assess the performance of their proposed models.
- Simulation data are generated by imitating the operation of agents in a real-world process or systems over time using computer-aided modeling and simulations. This type of data is suitable for theoretical verification and testing any combination of parameters in the model. Studies [S02], [S06], and [S28] use simulation data for the purpose of their research.
- Derived data use existing data, often from different data sets, to generate new data through transformation by arithmetic/mathematical formula and aggregation. Compiled databases or data derived from the game theoretical analyses are good examples of this data type. Studies [S09], [S10], [S11], [S12], and [S13] have used derived data to assess the performance of their proposed models.
- Projected data are useful in the context of policy evaluations when data do not exist or are scarce. These data can also be used to validate the results obtained from simulation of models. [S04] and [S07] are the two studies that have used projected data to show the insights of their proposed models.

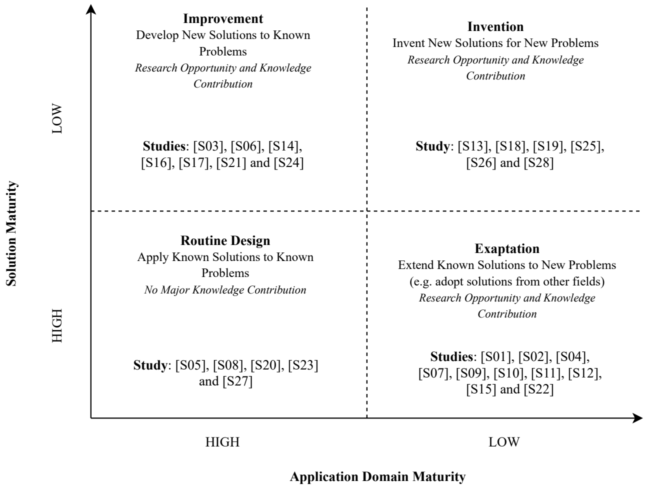
However, there are several challenges along the way. Data are expensive to collect, difficult to harmonize, and, sometimes, difficult to realize if they are relevant to a specific model [159]. Furthermore, considering the fact that digital technologies and business processes are fast changing, data tend to become outdated and must be refreshed and improved. This delineates a necessary revision of the way we collect, use, communicate, and share data. Various biases such as selection bias [e.g., S01], publication bias, reporting bias, confirmation bias [e.g., S08], and funding bias might also be introduced in these processes. Therefore, data plays an increasingly significant role in answering the crucial question of the determinants of success or failure of economics models. UK Data Archive suggests a guide [160] to managing and sharing research data that can be useful in fields such as cybersecurity economics.

RQ5. How has cybersecurity economics contributed to providing solutions for known and unknown problems within the cybersecurity domain?

Our literature review shows that cybersecurity economics has had both descriptive and prescriptive roles. In its descriptive role, cybersecurity economics not only explains how various economic forces affect the cybersecurity posture of an organization or state but also predicts the consequences of the decisions made by it. In its prescriptive role, however, cybersecurity economics prescribes the rules, regulations, and policies for the improvement of decision making by organizations or governments so that they can achieve their objectives efficiently. However, as Colander states [29], to know whether you can apply economic theories to real-world settings, you must know about economic institutions, and cybersecurity is not an exception. Organizations, governments, and cultural norms are all examples of institutions that have social, political, and regulatory dimensions which all can impact on the sustainability of cybersecurity in those institutions. Therefore, it is important to understand the institutions to gain insight on how economic theories function. It also helps both researchers and practitioners who employ the proposed models account for the differences between the ways that models work in reality and throughout their experiments.

Since the inception of the field in 2000, the general acceptance of cybersecurity economics as a competent approach to tackle the challenges that were highlighted in RQ2 is increasing. A wide range of socio-technical artifacts such as decision support systems, modeling and simulation tools, governance strategies, evaluation methods, and change interventions have been constructed in this field of research. Understanding and positioning the knowledge contribution of the research projects in this field is necessary to employ their findings in the day-to-day routines and the longer-term direction of the agents. As Marc and Smith stated, “real problems must be properly conceptualized and represented, and appropriate techniques for their solution must be constructed” [161]. Our review reveals that this has been achieved by combining practical knowledge and scientific rigor. On the whole, to answer this question, we used the Design Science Research Knowledge Contribution Framework to classify the theoretical and empirical contributions of the selected studies based on their research problems and proposed solutions.

As depicted in Figure 3, most of the proposed solutions in the selected studies result in improvement or exaptation of the artifacts. These types of research is also common in information system studies, where new problems emerge with the changes in digital ecosystem. The key challenges in these two quadrant is to clearly demonstrate the improvement and exaptation properly advance the existing knowledge.



Improvement
Develop New Solutions to Known Problems
Research Opportunity and Knowledge Contribution

Studies: [S03], [S06], [S14], [S16], [S17], [S21] and [S24]

Invention
Invent New Solutions for New Problems
Research Opportunity and Knowledge Contribution

Study: [S13], [S18], [S19], [S25], [S26] and [S28]

Routine Design
Apply Known Solutions to Known Problems
No Major Knowledge Contribution

Study: [S05], [S08], [S20], [S23] and [S27]

Exaptation
Extend Known Solutions to New Problems (e.g. adopt solutions from other fields)
Research Opportunity and Knowledge Contribution

Studies: [S01], [S02], [S04], [S07], [S09], [S10], [S11], [S12], [S15] and [S22]

Figure 3. Classification of selected studies based on DSR Knowledge Contribution Framework.

7. Conclusions

Interweaving dimensions of theory and practice, this paper reflected on some of the issues in the research on cybersecurity economics, emphasizing, in particular, the constructive and complexity aspects of the field. Moreover, the paper analyzes different cybersecurity economics models described in the scientific literature and identifies the relevant properties to cybersecurity economics. To this end, we conducted a transdisciplinary meta-narrative literature review in which we identified 628 articles on cybersecurity economics models. Out of these articles, we selected 28 studies based on an exhaustive selection process. The findings of the review and our observations suggest remarkable, persistent effects of factors that contribute to sustainable cybersecurity posture in reality. Drawing on the contributions of many studies, most of which are cited in this survey, this study provided an overview of the theoretical and empirical sides of the growing literature on cybersecurity economics.

The literature of cybersecurity economics has covered a broad range of topics from budgeting to policies and regulation. Both quantitative and qualitative tools have been used to provide important insights from various research fields and disciplines into this field. However, complexity science, interdisciplinary knowledge, ethical and moral aspects, and the importance of institutions and social rules could be included more explicitly. Furthermore, more than half of the reviewed studies have extended the known solutions to new problems (i.e., exaptation). This shows that the maturity of the cybersecurity economics field is growing and provides the researchers with more research opportunities. Furthermore, the empirical evidence shows that the practical implications of the research in this field can be successfully implemented for sustainable solutions if the researchers eliminate the most pressing anomalies and enhance the maturity of the application domain and developed solutions. Our paper, “Multi-paradigmatic Approaches in Cybersecurity Economics” [162], suggests five core themes to reflect on the further development on paradigm, methodologies, and hypotheses in which the research on cybersecurity economics has been based on. These themes are interrelated and shape a multi-paradigmatic structure of the field. They can also be known as the characteristics of a new approach in cybersecurity economics. We recommend that researchers strengthen their capabilities of integration of these characteristics and comparability across models. The latter is important to identify the strengths and weaknesses of different models and synergies in model advancement by exploiting the model structure of the different disciplines’ knowledge base.

We also argue that the goal of cybersecurity economics is, in addition to the suggested financial and budgeting tools, to explain and predict the behavior and patterns of the agents and systems, design institutions, and recommend sustainable policies and regulations. In the context of cybersecurity, the policymakers are, increasingly, in urgent need of new short- and long-term planning tools capturing the relevant features of the modern digital ecosystem, including complexity, uncertainty, bounded rationality, and out-of-equilibrium. We need further research on exploring new, meaningful, and clear ways to interpret, compare, and communicate the results and policy insights of the proposed models so that policymakers and decision makers fully understand the relevance of these findings.

Finally, our review does not investigate some important questions such as: Can different macro- and microeconomics models be connected to each other and, if so, what are the benefits of doing so? How could synergies in model building be better exploited? What are the best approaches to combine and compare the different models to gain a more comprehensive picture of the practical implications? How and to what extent are these implications determined by the model structure? These questions warrant further research and analysis on the topic. Another limitation of this study is excluding grey literature from the selected studies. While we acknowledge that business reports and analyses (e.g., publications by Deloitte, PWC, EY, and KPMG) contribute to the maturity of the cybersecurity economics research significantly, this study covered academic journals and conference papers. Hence, selecting all the relevant publications is not guaranteed.

Future studies can expand the study domain to include editorial papers, white papers, and industrial reports and insights.

Author Contributions: Conceptualization, M.K., S.J.K. and H.Ø.; methodology, M.K., S.J.K. and H.Ø.; validation, M.K., S.J.K. and H.Ø.; formal analysis, M.K; investigation, M.K. and S.J.K.; resources, M.K. and S.J.K.; data curation, M.K.; writing—original draft preparation, M.K.; writing—review and editing, M.K. and H.Ø.; visualization, M.K.; supervision, S.J.K. and H.Ø.; project administration, M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data supporting the results are found within the body of the paperand in referenced works.

Acknowledgments: The authors greatly appreciate the thoughtful comments and suggestions of the anonymous reviewers.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Courtney, R.H., Jr. A systematic approach to data security. *Comput. Secur.* **1982**, *1*, 99–112. [CrossRef]
2. Dixon, P.B.; Jorgenson, D. *Handbook of Computable General Equilibrium Modeling*; Elsevier: Newnes, UK, 2012; Volume 1.
3. McLennan, M. *The Global Risks Report*, 16th ed.; The World Economic Forum: Geneva, Switzerland, 2021.
4. Lewis, J.; Smith, Z.; Lostri, E. The Hidden Costs of Cybercrime (CSIS, 2020). 2021. Available online: https://www.csis.org/analysis/hidden-costs-cybercrime (accessed on 17 August 2021).
5. Verizon. *Data Breach Investigations Report 2020*; Technical Report; Verizon: New York, NY, USA, 2020. [CrossRef]
6. Cat, J. The Unity of Science. In *The Stanford Encyclopedia of Philosophy*; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2017.
7. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
8. Brookson, C.; Cadzow, S.; Eckmaier, R.; Eschweiler, J.; Gerber, B.; Guarino, A.; Rannenberg, K.; Shamah, J.; Gorniak, S. *Definition of Cybersecurity-Gaps and Overlaps in Standardisation*; ENISA: Heraklion, Greece, 2015.
9. ISO/IEC27002. *Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS ISO/IEC 27002: 2015)*; International Organization for Standardization: Geneva, Switzerland, 2015.
10. Coulon, Y. *Rational Investing with Ratios: Implementing Ratios with Enterprise Value and Behavioral Finance*; Springer Nature: Cham, Switzerland, 2019.
11. Straub, D.; Rai, A.; Klein, R. Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *J. Manag. Inf. Syst.* **2004**, *21*, 83–114. [CrossRef]
12. Moody, D.L.; Walsh, P. Measuring the Value of Information—An Asset Valuation Approach. In Proceedings of the Seventh European Conference on Information Systems (ECIS'99), Copenhagen Business School, Frederiksberg, Denmark, 23–25 June 1999; pp. 496–512.
13. Henderson, S.; Peirson, G.; Herbohn, K.; Howieson, B. *Issues in Financial Accounting*; Pearson Higher Education: Melbourne, Australia, 2015.
14. Godfrey, J.; Hodgson, A.; Tarca, A.; Hamilton, J.; Holmes, S. *Accounting Theory*; Wiley and Sons: Hoboken, NJ, USA, 2010.
15. Arora, A.; Hall, D.; Piato, C.; Ramsey, D.; Telang, R. Measuring the risk-based value of IT security solutions. *IT Prof.* **2004**, *6*, 35–42. [CrossRef]
16. Bistarelli, S.; Dall'Aglio, M.; Peretti, P. Strategic games on defense trees. In *International Workshop on Formal Aspects in Security and Trust*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–15.
17. Shirtz, D.; Elovici, Y. Optimizing investment decisions in selecting information security remedies. *Inf. Manag. Comput. Secur.* **2011**, *19*, 95–112. [CrossRef]
18. Huang, C.D.; Behara, R.S. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *Int. J. Prod. Econ.* **2013**, *141*, 255–268. [CrossRef]
19. Ezhei, M.; Ladani, B.T. Interdependency analysis in security investment against strategic attacks. In *Information Systems Frontiers*; Springer: New York, NY, USA, 2018; pp. 1–15.
20. Li, Y.; Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *Int. J. Prod. Res.* **2020**, *59*, 1216–1238. [CrossRef]
21. Schatz, D.; Bashroush, R. Economic valuation for information security investment: A systematic literature review. *Inf. Syst. Front.* **2017**, *19*, 1205–1228. [CrossRef]

22. Ekelund, S.; Iskoujina, Z. Cybersecurity economics–balancing operational security spending. *Inf. Technol. People* **2019**, *32*, 1318–1342. [CrossRef]
23. Anderson, R.; Schneier, B. Guest Editors' Introduction: Economics of Information Security. *IEEE Secur. Priv.* **2005**, *3*, 12–13. [CrossRef]
24. Neubauer, T.; Klemen, M.; Biffl, S. Secure business process management: A roadmap. In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 20–22 April 2006; p. 8.
25. Ahmed, E.M. Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth. *J. Knowl. Econ.* **2020**, *2020*, 1–19. [CrossRef]
26. Rathod, P.; Hämäläinen, T. A novel model for cybersecurity economics and analysis. In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 274–279.
27. Gordon, L.A.; Loeb, M.P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2002**, *5*, 438–457. [CrossRef]
28. Bojanc, R.; Jerman-Blažič, B. A quantitative model for information-security risk management. *Eng. Manag. J.* **2013**, *25*, 25–37. [CrossRef]
29. David, C.C. *Microeconomics*; McGraw-Hill Education: New York, NY, USA, 2020.
30. Crumpler, W.; Lewis, J.A. *Cybersecurity Workforce Gap*; Center for Strategic and International Studies (CSIS): Washington, DC, USA, 2019.
31. DellaVigna, S. Psychology and economics: Evidence from the field. *J. Econ. Lit.* **2009**, *47*, 315–372. [CrossRef]
32. Broadbent, D.E. *Perception and Communication*; Elsevier: Amsterdam, The Netherlands, 2013.
33. Stirling, A. Risk, uncertainty and precaution: Some instrumental implications from the social sciences. In *Negotiating Environmental Change: New Perspectives from the Social Sciences*; Edward Elgar: Cheltenham, UK, 2003; pp. 33–76.
34. Cavusoglu, H.; Mishra, B.; Raghunathan, S. A model for evaluating IT security investments. *Commun. ACM* **2004**, *47*, 87–92. [CrossRef]
35. Huang, C.D.; Hu, Q.; Behara, R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *Int. J. Prod. Econ.* **2008**, *114*, 793–804. [CrossRef]
36. Hoo, K.J.S. How Much Is Enough? A Risk Management Approach to Computer Security. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 2000.
37. Kianpour, M.; Øverby, H.; Kowalski, S.J.; Frantz, C. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In *International Conference on Human-Computer Interaction*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 149–163.
38. Bryan, J. *A Better Way to Manage Third-Party Risk*; Gartner: Stanford, CA, USA, 2019.
39. Colander, D.; Holt, R.; Rosser, B., Jr. The changing face of mainstream economics. *Rev. Political Econ.* **2004**, *16*, 485–499. [CrossRef]
40. Cavusoglu, H.; Raghunathan, S.; Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *J. Manag. Inf. Syst.* **2008**, *25*, 281–304. [CrossRef]
41. Cremonini, M.; Nizovtsev, D. Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. In Proceedings of the 4th Workshop on the Economics of Information Security, Boston, MA, USA, 2–3 June 2005.
42. Schechter, S.E.; Smith, M.D. How much security is enough to stop a thief? In Proceedings of the International Conference on Financial Cryptography, Guadeloupe, France, 27–30 January 2003; pp. 122–137.
43. Leeson, P.T.; Coyne, C.J. The economics of computer hacking. *JL Econ. Policy* **2005**, *1*, 511.
44. Huang, C.D.; Behara, R.S.; Goo, J. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decis. Support Syst.* **2014**, *61*, 1–11. [CrossRef]
45. Miura-Ko, R.A.; Yolken, B.; Mitchell, J.; Bambos, N. Security decision-making among interdependent organizations. In Proceedings of the 2008 21st IEEE Computer Security Foundations Symposium, Pittsburgh, PA, USA, 23–25 June 2008; pp. 66–80.
46. Kayworth, T.; Whitten, D. Effective information security requires a balance of social and technology factors. *MIS Q. Exec.* **2010**, *9*, 2012–2052.
47. Gordon, L.A.; Loeb, M.P. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*; McGraw-Hill: New York, NY, USA, 2006; Volume 1.
48. Huang, C.D.; Behara, R.S.; Hu, Q. Economics of information security investment. In Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 26–28 June 2006.
49. Kersting, F.; Obst, D. Behavioral Economics. Exploring Economics. Available online: https://www.exploring-economics.org/en/orientation/behavioral-economic (accessed on 12 June 2021).
50. Paul, J.A.; Wang, X.J. Socially optimal IT investment for cybersecurity. *Decis. Support Syst.* **2019**, *122*, 113069. [CrossRef]
51. Koepke, P. *Cybersecurity Information Sharing Incentives and Barriers*; Sloan School of Management at MIT University: Cambridge, MA, USA, 2017.
52. Xu, M.; Hua, L. Cybersecurity insurance: Modeling and pricing. *N. Am. Actuar. J.* **2019**, *23*, 220–249. [CrossRef]
53. Wang, S.S. Integrated framework for information security investment and cyber insurance. *Pac.-Basin Financ. J.* **2019**, *57*, 101173. [CrossRef]
54. Tosh, D.K.; Shetty, S.; Sengupta, S.; Kesan, J.P.; Kamhoua, C.A. Risk management using cyber-threat information sharing and cyber-insurance. In *International Conference on Game Theory for Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 154–164.

55. Rowe, B.; Pokryshevskiy, I.D.; Link, A.N.; Reeves, D.S. Economic analysis of an inadequate cyber security technical infrastructure. In *National Institute of Standards and Technology Planning Report*; NIST: Gaithersburg, MD, USA 2013.
56. Blythe, J.M.; Johnson, S.D.; Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Sci.* **2020**, *9*, 1. [CrossRef]
57. Grossklags, J.; Acquisti, A. *When 25 Cents is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information*; In Proceedings of the 6th Workshop on the Economics of Information Security (WEIS), Pittsburgh, PA, USA, 7–8 June 2007.
58. Renaud, K.; Otondo, R.; Warkentin, M. "This is the way 'I'create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Comput. Secur.* **2019**, *82*, 241–260. [CrossRef]
59. Fineberg, V. BECO: Behavioral Economics of Cyberspace Operations. *Games People Play. Behav. Secur.* **2014**, *2*, 20.
60. Keysight Surveys. *Security Operations Effectiveness*; Keysight Technologies: Santa Rosa, CA, USA, 2020.
61. Dong, K.; Lin, R.; Yin, X.; Xie, Z. How does overconfidence affect information security investment and information security performance? *Enterp. Inf. Syst.* **2019**, *15*, 1–18. [CrossRef]
62. de Bruijn, H. *The Art of Framing: How Politicians Convince Us That They Are Right*; Amsterdam University Press: Amsterdam, The Netherlands, 2017.
63. Sivan-Sevilla, I. Framing and governing cyber risks: Comparative analysis of US Federal policies [1996–2018]. *J. Risk Res.* **2019**, *24*, 692–720. [CrossRef]
64. Lawson, S. Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *J. Inf. Technol. Politics* **2013**, *10*, 86–103. [CrossRef]
65. Wheeler, E. Framing cyber security as a business risk. *Cyber Secur. Peer-Rev. J.* **2018**, *2*, 202–210.
66. Ween, A.; Dortmans, P.; Thakur, N.; Rowe, C. Framing cyber warfare: An analyst's perspective. *J. Def. Model. Simul.* **2019**, *16*, 335–345. [CrossRef]
67. Dortmans, P.J.; Thakur, N.; Ween, A. Conjectures for framing cyberwarfare. *Def. Secur. Anal.* **2015**, *31*, 172–184. [CrossRef]
68. Tversky, A.; Kahneman, D. The framing of decisions and the psychology of choice. *Science* **1981**, *211*, 453–458. [CrossRef]
69. de Bruijn, H.; Janssen, M. Building cybersecurity awareness: The need for evidence-based framing strategies. *Gov. Inf. Q.* **2017**, *34*, 1–7. [CrossRef]
70. Mak, J.K.L.; Cho, H. Framing Smart Nation: A moderated mediation analysis of frame-focus effects. *Inf. Commun. Soc.* **2019**, *35*, 1–21. [CrossRef]
71. Cheung-Blunden, V.; Cropper, K.; Panis, A.; Davis, K. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion* **2019**, *19*, 1353. [CrossRef]
72. Renaud, K.; Dupuis, M. Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop, Costa Rica, CA, USA, 23–26 September 2019; pp. 42–56.
73. Nelson, N.; Madnick, S. *Studying the Tension between Digital Innovation and Cybersecurity*; Sloan School of Management, MIT: Cambridge, MA, USA, 2017.
74. Bailetti, T.; Craigen, D. Examining the Relationship Between Cybersecurity and Scaling Value for New Companies. *Technol. Innov. Manag. Rev.* **2020**, *10*, 62–69. [CrossRef]
75. Garud, R.; Karnøe, P. Path creation as a process of mindful deviation. *Path Depend. Creat.* **2001**, *138*, 38.
76. Shiozawa, Y.; Morioka, M.; Taniguchi, K. Microfoundations of evolutionary economics. In *Microfoundations of Evolutionary Economics*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–52.
77. Kuerbis, B.; Badiei, F. Mapping the cybersecurity institutional landscape. *Digit. Policy Regul. Gov.* **2017**, *19*, 33. [CrossRef]
78. Lindsay, J.R. Restrained by design: The political economy of cybersecurity. *Digit. Policy Regul. Gov.* **2017**, *19*, 493–514. [CrossRef]
79. Anderson, R. Why Information Security is Hard-An Economic Perspective. In Proceedings of the 17th Annual Computer Security Applications Conference, ACSAC '01, New Orleans, LA, USA, 10–14 December 2001; IEEE Computer Society: Washington, DC, USA, 2001; p. 358.
80. Brecht, M.; Nowey, T. A closer look at information security costs. In *The Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 3–24.
81. Baryshnikov, Y. IT Security Investment and Gordon-Loeb's 1/e Rule. In Proceedings of the 11th Workshop on the Economics of Information Security (WEIS), Berlin, Germany, 25–26 June 2012.
82. Willemson, J. On the Gordon & Loeb Model for Information Security Investment. In Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 26–28 June 2006.
83. Lelarge, M. Coordination in network security games: A monotone comparative statics approach. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 2210–2219. [CrossRef]
84. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *J. Inf. Secur.* **2014**, *6*, 24. [CrossRef]
85. Patwary, A.A.N.; Naha, R.K.; Garg, S.; Battula, S.K.; Patwary, M.A.K.; Aghasian, E.; Amin, M.B.; Mahanti, A.; Gong, M. Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control. *Electronics* **2021**, *10*, 1171. [CrossRef]
86. Nagurney, A.; Nagurney, L.S. A game theory model of cybersecurity investments with information asymmetry. *Netnomics Econ. Res. Electron. Netw.* **2015**, *16*, 127–148. [CrossRef]

87. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cyber security investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
88. Hota, A.R.; Sundaram, S. Interdependent security games on networks under behavioral probability weighting. *IEEE Trans. Control. Netw. Syst.* **2016**, *5*, 262–273. [CrossRef]
89. Abdallah, M.; Naghizadeh, P.; Hota, A.R.; Cason, T.; Bagchi, S.; Sundaram, S. The impacts of behavioral probability weighting on security investments in interdependent systems. In Proceedings of the 2019 American Control Conference (ACC), Philadelphia, PA, USA, 10–12 July 2019; pp. 5260–5265.
90. Abdallah, M.; Naghizadeh, P.; Hota, A.R.; Cason, T.; Bagchi, S.; Sundaram, S. Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 1585–1596. [CrossRef]
91. Sonnenreich, W.; Albanese, J.; Stout, B. Return on security investment (ROSI)—A practical quantitative model. *J. Res. Pract. Inf. Technol.* **2006**, *38*, 45.
92. Pontes, E.; Guelfi, A.E.; Silva, A.A.; Kofuji, S.T. A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI). In *Risk Management in Environment, Production and Economy*; InTech: Rijeka, Croatia, 2011; pp. 149–170.
93. Smith, M.D.; Paté-Cornell, M.E. Cyber risk analysis for a smart grid: How smart is smart enough? a multiarmed bandit approach to cyber security investment. *IEEE Trans. Eng. Manag.* **2018**, *65*, 434–447. [CrossRef]
94. Čapko, Z.; Aksentijević, S.; Tijan, E. Economic and financial analysis of investments in information security. In Proceedings of the 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 26–30 May 2014; pp. 1550–1556.
95. Sheen, J. Fuzzy economic decision-models for information security investment. In Proceedings of the 9th International Conference on Instrumentation, Measurement, Circuits and Systems, IMCAS'10, Hangzhou, China, 11–13 April 2010; pp. 141–147.
96. Jerman-Blažič, B. Quantitative model for economic analyses of information security investment in an enterprise information system. *Organizacija* **2012**, *45*, 276–288.
97. Jerman-Blažič, B. Towards a standard approach for quantifying an ICT security investment. *Comput. Stand. Interfaces* **2008**, *30*, 216–222.
98. Huang, C.D.; Goo, J. Investment decision on information system security: A scenario approach. In Proceedings of the 15th Americas Conference on Information Systems, San Francisco, CA, USA, 6–9 August 2009; p. 571.
99. Jerman-Blažič, B. An economic modelling approach to information security risk management. *Int. J. Inf. Manag.* **2008**, *28*, 413–422.
100. Mazzoccoli, A.; Naldi, M. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Anal.* **2020**, *40*, 550–564. [CrossRef] [PubMed]
101. Hagen, J.M.; Albrechtsen, E.; Hovden, J. Implementation and effectiveness of organizational information security measures. *Inf. Manag. Comput. Secur.* **2008**, *16*, 377–397. [CrossRef]
102. Mayadunne, S.; Park, S. An economic model to evaluate information security investment of risk-taking small and medium enterprises. *Int. J. Prod. Econ.* **2016**, *182*, 519–530. [CrossRef]
103. Miaoui, Y.; Boudriga, N. Enterprise security investment through time when facing different types of vulnerabilities. *Inf. Syst. Front.* **2019**, *21*, 261–300. [CrossRef]
104. Elsner, W.; Heinrich, T.; Schwardt, H. *The Microeconomics of Complex Economies*; Academic Press: Cambridge, MA, USA, 2014.
105. Corbet, S.; Gurdgiev, C. What the hack: Systematic risk contagion from cyber events. *Int. Rev. Financ. Anal.* **2019**, *65*, 101386. [CrossRef]
106. Szubartowicz, E.; Schryen, G. Timing in information security: An event study on the impact of information security investment announcements. *J. Inf. Syst. Secur.* **2020**, *16*, 3–31.
107. Tisdale, S.M. Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues Inf. Syst.* **2015**, *16*, 191–198.
108. Krivo, A.; Mirvoda, S. The Experience of Cyberthreats Analysis Using Business Intelligence System. In Proceedings of the 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 14–15 May 2020; pp. 0619–0622.
109. Mahmood, T.; Afzal, U. Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, 11–12 December 2013; pp. 129–134.
110. Anderson, R.; Moore, T. Information Security: Where Computer Science, Economics and Psychology Meet. *Philos. Trans. Math. Phys. Eng. Sci.* **2009**, *367*, 2717–2727. [CrossRef] [PubMed]
111. Varian, H. System reliability and free riding. In *Economics of Information Security*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–15.
112. Hausken, K. Information sharing among firms and cyber attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. [CrossRef]
113. Moore, T. The economics of cybersecurity: Principles and policy options. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 103–117. [CrossRef]
114. Bauer, J.M.; Van Eeten, M.J. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommun. Policy* **2009**, *33*, 706–719. [CrossRef]
115. Lelarge, M.; Bolot, J. Economic incentives to increase security in the internet: The case for insurance. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1494–1502.

116. Dacus, C.; Yannakogeorgos, P.A. Designing Cybersecurity into Defense Systems: An Information Economics Approach. *IEEE Secur. Priv.* **2016**, *14*, 44–51. [CrossRef]
117. Brangetto, P.; Aubyn, M. Economic aspects of national cyber security strategies. *Proj. Rep. Annex.* **2015**, *1*, 9–16.
118. Newmeyer, K.P. Elements of national cybersecurity strategy for developing nations. *Natl. Cybersecur. Inst. J.* **2015**, *1*, 9–19.
119. Kelly, D. The economics of cybersecurity. In Proceedings of the International Conference on Cyber Warfare and Security, Dayton, OH, USA, 2–3 March 2017; p. 522.
120. Massacci, F.; Ruprai, R.; Collinson, M.; Williams, J. Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Secur. Priv.* **2016**, *14*, 52–60. [CrossRef]
121. Wong, G.; Greenhalgh, T.; Westhorp, G.; Buckingham, J.; Pawson, R. RAMESES publication standards: Meta-narrative reviews. *J. Adv. Nurs.* **2013**, *69*, 987–1004. [CrossRef]
122. Montuori, A. The complexity of transdisciplinary literature reviews. *Complicity Int. J. Complex. Educ.* **2013**, *10*, 45–55. [CrossRef]
123. Gough, D. Meta-narrative and realist reviews: Guidance, rules, publication standards and quality appraisal. *BMC Med.* **2013**, *11*, 1–4. [CrossRef]
124. Garousi, V.; Felderer, M.; Mäntylä, M.V. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf. Softw. Technol.* **2019**, *106*, 101–121. [CrossRef]
125. Hsu, C.; Lee, J.N.; Straub, D.W. Institutional influences on information systems security innovations. *Inf. Syst. Res.* **2012**, *23*, 918–939. [CrossRef]
126. Feng, N.; Wang, H.J.; Li, M. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Inf. Sci.* **2014**, *256*, 57–73. [CrossRef]
127. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *J. Account. Public Policy* **2015**, *34*, 509–519. [CrossRef]
128. Jalali, M.S.; Siegel, M.; Madnick, S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *J. Strateg. Inf. Syst.* **2019**, *28*, 66–82. [CrossRef]
129. Zhao, X.; Xue, L.; Whinston, A.B. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Manag. Inf. Syst.* **2013**, *30*, 123–152. [CrossRef]
130. Shetty, N.; Schwartz, G.; Felegyhazi, M.; Walrand, J. Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 229–247.
131. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Increasing cybersecurity investments in private sector firms. *J. Cybersecur.* **2015**, *1*, 3–17. [CrossRef]
132. Shackelford, S.J. Should your firm invest in cyber risk insurance? *Bus. Horiz.* **2012**, *55*, 349–356. [CrossRef]
133. Hausken, K. Returns to information security investment: Endogenizing the expected loss. *Inf. Syst. Front.* **2014**, *16*, 329–336. [CrossRef]
134. Gao, X.; Zhong, W.; Mei, S. Security investment and information sharing under an alternative security breach probability function. *Inf. Syst. Front.* **2015**, *17*, 423–438. [CrossRef]
135. Campbell, K.; Gordon, L.A.; Loeb, M.P.; Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *J. Comput. Secur.* **2003**, *11*, 431–448. [CrossRef]
136. Grossklags, J.; Christin, N.; Chuang, J. Secure or insure? A game-theoretic analysis of information security games. In Proceedings of the 17th International Conference on World Wide Web, Beijing, China, 21–25 April 2008; pp. 209–218.
137. Srinidhi, B.; Yan, J.; Tayi, G.K. Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decis. Support Syst.* **2015**, *75*, 49–62. [CrossRef]
138. Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Van Eeten, M.J.; Levi, M.; Moore, T.; Savage, S. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 265–300.
139. Cook, I.; Pfleeger, S. Security decision support challenges in data collection and use. *IEEE Secur. Priv.* **2010**, *8*, 28–35. [CrossRef]
140. Vishik, C.; Sheldon, F.; Ott, D. Economic incentives for cybersecurity: Using economics to design technologies ready for deployment. In *ISSE 2013 Securing Electronic Business Processes*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 133–147.
141. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. [CrossRef]
142. Rashid, Z.; Noor, U.; Altmann, J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Gener. Comput. Syst.* **2021**, *124*, 436–466. [CrossRef]
143. Rothman, K.J.; Greenland, S.; Lash, T.L. *Modern Epidemiology*; Lippincott Williams & Wilkins: Baltimore, MD, USA, 2008.
144. Caplin, A.; Schotter, A. *The Foundations of Positive and Normative Economics: A Handbook*; Oxford University Press: Oxford, UK, 2008.
145. Marotta, A.; Martinelli, F.; Nanni, S.; Orlando, A.; Yautsiukhin, A. Cyber-insurance survey. *Comput. Sci. Rev.* **2017**, *24*, 35–61. [CrossRef]
146. Samuelson, P.A. The pure theory of public expenditure. *Rev. Econ. Stat.* **1954**, *36*, 387–389. [CrossRef]
147. Mulligan, D.K.; Schneider, F.B. Doctrine for cybersecurity. *Daedalus* **2011**, *140*, 70–92. [CrossRef]
148. Asllani, A.; White, C.S.; Ettkin, L. Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *J. Leg. Ethical Regul. Issues* **2013**, *16*, 7.

149. Rietveld, J.; Schilling, M.A. Platform competition: A systematic and interdisciplinary review of the literature. *J. Manag.* **2021**, *47*, 0149206320969791. [CrossRef]
150. Al Sabbagh, B.; Kowalski, S. A socio-technical framework for threat modeling a software supply chain. *IEEE Secur. Priv.* **2015**, *13*, 30–39. [CrossRef]
151. Vagle, J.L. Cybersecurity and Moral Hazard. *Stanf. Tech. Law Rev.* **2020**, *23*, 71. [CrossRef]
152. Brito, J.; Watkins, T. Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy. *Harard Natl. Secur. J.* **2011**, *3*, 39.
153. Anderson, R.; Barton, C.; Bölme, R.; Clayton, R.; Ganán, C.; Grasso, T.; Levi, M.; Moore, T.; Vasek, M. Measuring the Changing Cost of Cybercrime. In Proceedings of the 18th Annual Workshop on the Economics of Information Security, Boston, MA, USA, 3–4 June 2019.
154. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application. *Ain Shams Eng. J.* **2021**, *12*, 2227–2240. [CrossRef]
155. Thurner, S.; Poledna, S. DebtRank-transparency: Controlling systemic risk in financial networks. *Sci. Rep.* **2013**, *3*, 1888. [CrossRef]
156. Ahmadi, E.; McLellan, B.; Tezuka, T. The economic synergies of modelling the renewable energy-water nexus towards sustainability. *Renew. Energy* **2020**, *162*, 1347–1366. [CrossRef]
157. Barabási, A.L.; Gulbahce, N.; Loscalzo, J. Network medicine: A network-based approach to human disease. *Nat. Rev. Genet.* **2011**, *12*, 56–68. [CrossRef]
158. Morgan, S. *2019 Official Annual Cybercrime Report*; Technical Report; Cybersecurity Ventures: Northport, NY, USA, 2020.
159. Moore, T.; Kenneally, E.; Collett, M.; Thapa, P. Valuing Cybersecurity Research Datasets. In Proceedings of the 18th Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019.
160. Corti, L.; Van den Eynden, V.; Bishop, L.; Woollard, M. *Managing and Sharing Research Data: A Guide to Good Practice*; Sage: Newcastle upon Tyne, UK, 2019.
161. March, S.T.; Smith, G.F. Design and natural science research on information technology. *Decis. Support Syst.* **1995**, *15*, 251–266. [CrossRef]
162. Kianpour, M.; Kowalski, S.J.; Øverby, H. Multi-Paradigmatic Approaches in Cybersecurity Economics. In Proceedings of the STPIS'21: Workshop on Socio-Technical Perspectives in Information Systems, Trento, Italy, 14–15 October 2021.

Chapter 6

Research Paper 2: Multi-Paradigmatic Approaches in Cybersecurity Economics

Mazaher Kianpour, Stewart James Kowalski, Harald Øverby - *Proceedings of the 7th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2021)*

Multi-Paradigmatic Approaches in Cybersecurity Economics

Mazaher Kianpour, Stewart James Kowalski and Harald Øverby

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway

Abstract

In cybersecurity economics, the selection of a particular methodology is a matter of interest and importance for the researchers. Methodologically sophisticated research forms an essential basis for understanding the challenges and opportunities for the richer descriptions of the behavior of cybersecurity practitioners (i.e., what they are doing and why they are doing it). This requires a broad and self-reflective approach to understand the use of a technique in socio-technical research within cybersecurity economics. Such understanding recognizes that research in this field involves more than just applying a method to create knowledge and diffuse it throughout society, organizations, and governments. This paper argues in favor of a multi-paradigmatic approach to cybersecurity economics research. Rather than adopting a single paradigm, this study suggests that results will be more prosperous and reliable if different methods from different existing paradigms are combined. Hence, it puts forward the desirability and feasibility of the multi-paradigmatic approach in cybersecurity economics research. It also outlines several practical guidelines that help design multi-paradigmatic research studies. These are illustrated with a critical evaluation of three examples of studies.

Keywords

cybersecurity economics, paradigm crisis, multi-paradigmatic approach, socio-technical research

1. Introduction

The study of cybersecurity economics is developing as a field of research in which it becomes essential to determine the kind and soundness of models to build in the future, to explore and observe how to implement them in practice, and to understand how these models affect the systems within which agents interact. This field is strongly motivated to explain substantive and considerable real-world phenomena in the cybersecurity area. For example, Gordon and Loeb's theoretical model [1] found that optimal cybersecurity investment does not always increase with the agent's increasing vulnerabilities. However, when more real-world observations were made, Willemson [2] and Hausken [3] provided demonstrations that this rule does not always hold and the basic model can not explain these anomalies. Hence, considering the complexity of these phenomena, this study considers cybersecurity as part of a complex socio-technical system that involves interactions among many stakeholders, social institutions, and physical systems. Moreover, drawing upon sociology, risk in complex systems is emergent and evolves as a product of collective actions [4, 5]. Here, we build on these discussions by arguing that the impacts of the decisions made by agents within the context of cybersecurity should also be understood as emergent and non-deterministic. Therefore, decision-makers need cybersecurity economic models to capture features, such as complexity, out-of-equilibrium dynamics, and social rules. Now, the relevant question is whether these studies have been successful in representing a stylized

STPIS'21: Workshop on Socio-Technical Perspectives in Information Systems, October 14-15, 2021, Trento, Italy

mazaher.kianpour@ntnu.no (M. Kianpour); stewart.kowalski@ntnu.no (S. J. Kowalski); haraldov@ntnu.no (H. Øverby)

view of reality that effectively offers an applicable, robust, and cohesive explanation of the fundamental problems of economics (i.e., scarcity, uncertainty, dominance and change) of cybersecurity in a complex socio-technical system like cyberspace.

To answer the question whether the proposed models in cybersecurity economics are sound enough to solve the known and unknown problems within cybersecurity, this paper adopts an inductive approach and uses observations to reach a conjecture. Verizon's breach report confirms that 86% of breaches in 2019, up from 71% in 2018, were financially motivated. According to threat research by RiskIQ[1] and threat researchers worldwide, every minute, US$11,400,000 will be lost to cybercrime in 2021, up from US$2,900,000 in 2020. Besides, the results of a study by Accenture show that malware is the most expensive type of cyber-attack, and Kaspersky reported a 14% boost in the number of unique malware in 2019 over 2018. In addition to these reports, there are various reports from national and international agencies that the types and sophistication of cyber-attacks are increasing [6, 7]. Microsoft Digital Defense Report also shows that the criminals behind these attacks are now spending significant time, money, and effort to develop scams that are sufficiently sophisticated to victimize increasingly savvy professionals [8]. Moreover, IBM[2], in collaboration with Ponemon Institute, reports that the average time to identify and contain a data breach in 15 studied countries/regions has stayed consistent in 2019 and 2020. However, in some regions and countries such as Scandinavia, United Kingdom, South Korea, India, Australia, and Brazil, this time has increased. The faster the data breach can be identified and contained, the lower the costs. While this time has increased in these countries, the same report shows that they have increased their investment in deploying new technologies such as security orchestration, automation, and response solutions to save the cost of data breaches.

In addition to these reports, the main scientific venues such as the New Security Paradigm Workshop (NSPW) and the Workshop on the Economics of Information Security (WEIS), or other workshops held by leading research centers including U.S. Naval War College's Center for Cyber Conflict Studies the question of the soundness of the cybersecurity economics models have been raised under the concepts like paradigm shift, science of security, or the need for new security paradigm indicating a growing dissatisfaction on how cybersecurity economics is treated in the research and practice. For example, these studies [9, 10, 11, 12, 13] presented at NSPW challenge current security paradigms adopted by researchers and practitioners. They suggest different approaches to drive the field of cybersecurity economic forward. At WEIS, Grossklags et al. argue that security decisions follow different security paradigms, often reflected in different organizational structures, due to diversity of security practices [14]. Moreover, at the workshop on "Cyber, Security and Economics: Challenges to Current Thinking, Presumptions and Future Cyber Defense Transformations", hosted by NWC's Center for Cyber Conflict Studies (C3S), David Mussington[3] stated that "There is problem in cyber policy, and that problem is that we can't speak with enough specificity about the problem in order to find solutions that actually work. Hence, economists need to talk to cyber people so they can make progress toward a shared goal of understanding the environment better and measuring effects." Chris Demchak[4] also added at this workshop, and then she elaborated in her paper [15], that cybersecurity researchers are operating with some deep presumptions. These presumptions are being undermined by the realities of national cyber insecurity. Therefore, it is necessary to lay out the disconnects in order to help innovate the strategies and policies effective systemically against the emerging and deeply cybered challenges.

[1] https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/

[2] https://www.ibm.com/security/digital-assets/cost-data-breach-report/

[3] The director of the Center for Public Policy and Private Enterprise at the University of Maryland

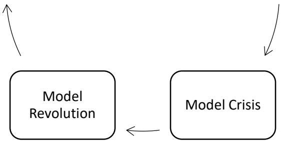
[4] The director of NWC's Center for Cyber Conflict Studies (C3S)

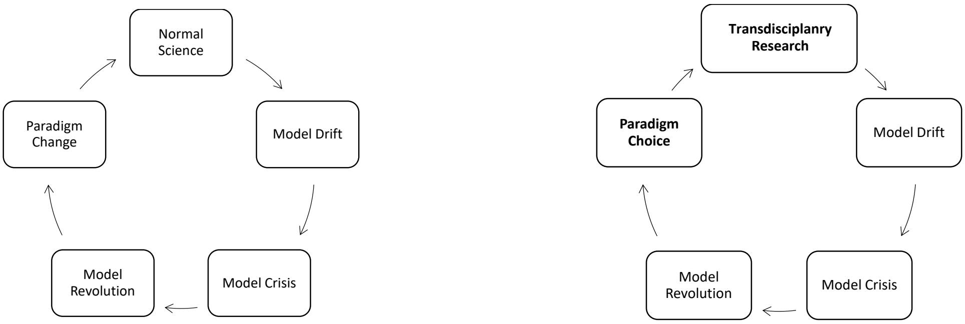
These findings imply that the research on cybersecurity economics has not been able to provide a good explanation for real-world cybersecurity phenomena. Consequently, this study questions the appropriateness of the paradigm that our research follows. The failures mentioned above can be rooted in technical, legal, or organizational measures employed to maintain and enhance information assets' security. They can be assessed in the level of individuals, groups, organizations, or nations as a whole. As many technical and behavioral standards, policies, regulations, and norms emerge from decentralized repeated decisions of many heterogeneous actors operating in dynamic, complex environments, these failures are also introduced by ignorance of these environments' characteristics and lack of a clear set of tools to approach certain problems. [16] and [17] argued that cybersecurity economics is a powerful tool to analyze security failures. The literature of this field also shows that concepts and theories from other fields, such as behavioral, institutional, and evolutionary economics, have made their way into the economics of cybersecurity. However, the empirical evidence and the significant anomalies we mentioned above show that the field of cybersecurity economics is thrown into a state of paradigm crisis.

Kuhn stated that paradigm crisis is followed by a scientific revolution and should be responded with a search for a revised disciplinary matrix [18]. These anomalies can not be explained by the currently accepted paradigm within which scientific progress has thereto been made. Therefore, he suggested paradigm shift. This concept has become a cliché with many meanings, including the several meanings of the word "paradigm" as used by Kuhn in his original publication. While the introduction of new technologies, including Internet and Artificial Intelligence, has created paradigm shift in the way business is conducted or research is directed [19], the discourse on paradigm shift has been incoherent in economics and social science literature because of the different uses of the term and the different levels of sophistication in its application [20]. Moreover, the paradigm shift in some disciplines like social science has been like a fad. For others, the discussion of a paradigm shift is more of an awareness and, at best, correction practice. However, the arguments about a multi-paradigmatic approach and pluralism is viewed useful in helping us better define the nature and limits of our research.

Consequently, as Figure 1 shows, we modified the Kuhn Cycle of Scientific Revolution and suggest that research on cybersecurity economics can benefit from multi-paradigmatic approaches. The research on cybersecurity economics started with one paradigm and one schools of economic thought (i.e., neoclassical economics) [21, 1]. Then, important problems were observed in cybersecurity economics studies and practices. However, paradigm restrictions and contending theories led to emerge of new problems and not efficient solutions. Adoption of multi-paradigmatic approaches empowers the researchers and practitioners to see the problems from different perspectives and their solutions are explored, assessed and developed using multiple paradigms. Conceptualization of multi-paradigmatic research in this field moves us towards transdisciplinary research defined as "research efforts conducted by investigators from different disciplines working jointly to create new conceptual, theoretical, methodological, and translational innovations that integrate and move beyond discipline-specific approaches to address a common problem [22]." The key idea of transdisciplinary is moving beyond disciplines and breaking down the boundaries between traditional disciplines and creates new ways of looking at existing and emerging issues. This is different from interdisciplinary research, which simply combines two or more varying disciplines and perspectives. In our proposed cycle, it is probable to observe model drift and model crisis due to the ever-changing nature of cyberspace and cybersecurity. However, multi-paradigmatic approach help to identify the problems more efficiently and propose richer solutions.

Based on the conjecture formed followed by our inductive reasoning, will now formulate our argument in more detail: while adopted paradigms have not been able to respond the described crisis, they still





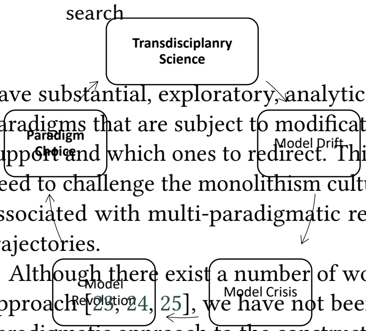
(a) The Kuhn Cycle of Scientific Revolution

(b) Our Proposed Cycle in Cybersecurity Economics Research

Figure 1: Our proposition to foster multi-paradigmatic approaches in cybersecurity economics research

have substantial, exploratory, analytical, and interpretive potentials. Since research advances within paradigms that are subject to modification and control, researchers need to decide which paradigms to support and which ones to redirect. This study sets out to open up academic discussions concerning the need to challenge the monolithism culture in cybersecurity economics research and upgrade the values associated with multi-paradigmatic research as criteria for assessing research papers and academic trajectories.

Although there exist a number of works in sociology that discuss the need for a multi-paradigmatic approach [23, 24, 25], we have not been able to find a related work on theorizing the nature of multi-paradigmatic approach to the construction and development of cybersecurity economics model. Hence, this paper can be an initiative to consider the methodological and conceptual challenges arise when studying cybersecurity economics as a research area. The paper is organized into four main sections. Section 2 presents an overview on cybersecurity economics research. Section 3 discusses the background of multi-paradigmatic approach and defines terms that we use in this paper. Section 4 puts forward the feasibility of the multi-paradigmatic research in practice. Section 5 provides a more substantive contribution to cybersecurity economics by outlining four practical guides that may help design multi-paradigmatic research in cybersecurity economics. These are illustrated with a critical evaluation of three examples of recent studies in Section 6. Finally Section 7 concludes the paper and outlines the limitations and future work.



2. An Overview on Cybersecurity Economics

Currently, there is no consensus on a definition of the term cybersecurity economics. Multiple studies have created their definitions, most of which are broad. Probably the most accepted definition for cybersecurity economics is an area concerned with providing maximum protection of assets at the minimum cost [1, 26]. However, Rathod and Hämäläinen adopted a wider perspective to the economics of cybersecurity based on strategic, long-term thinking incorporating economics from the outset [27]. They stated that cybersecurity economics and analysis provides benchmarks for the economic assessment of national and international cybersecurity audits and standards. It also provides policy recommendations to align policies and regulations to ensure trust within a digital environment. Additionally, Ahmed argues that cybersecurity economics addresses the issues of protection of Information and Communications Technology (ICT) applications designed to facilitate the economic activities that normally face cybercrimes that cost the companies and countries a significant amount of money and disturb the economic and financial activities around the globe as has been indicated in ICT-based sustainable development [28].

Despite the many different definitions of cybersecurity economics, all of these studies point out that cybersecurity economic situations are characterized by direct and indirect interdependencies among the agents involved. Each agent's behavior affects the available options of other agents and even the results that they can achieve. Given a particular situation and different options, which option do agents choose and why? Does the outcome satisfy them? Does it unintentionally leave other agents worse off while it has been an optimal decision for some of them? What is the role of government in compensating for the limitations of markets in achieving mutually beneficial exchange in the cybersecurity market?

To answer these questions, we would imply that it is crucial to be aware that cybersecurity economics covers a broader range of situations than exchanging products and services for money. Therefore, this paper defines cybersecurity economics as a field of research which offers a socio-technical perspective on economic aspects of cybersecurity such as budgeting, information asymmetry, governance, and types of goods, to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems. A socio-technical perspective is essential for understanding and managing the state of cybersecurity today, as well as how to enhance it moving forward. This field of study includes organizations having to decide how to value their assets and scarce resources and adapt economic theories to practice in complex, uncertain environments. Cybersecurity economics studies include how the role of individual and organizational behavior in developing a security culture; forces motivating stakeholders to invest in cybersecurity provision; market structures and regulatory structures; and, environmental, institutional and distributional consequences of the social decision situations. The studies also investigate the cybercrime economics and motivation, tools, and interest of actors in today's underground marketplaces.

Cybersecurity economics studies established their foundations and premises on different schools of economic thought[5]. The question of which schools are most appropriate for cybersecurity economics research has been a focus of concern for some time. From the perspective of a particular school of thought, the primary problems can be divided into four categories: scarcity, uncertainty, dominance, and change. Since there has been a growing interest in and commitment to neoclassical economics, the primary literature of cybersecurity economics focuses on scarcity and optimal allocation of resources. However, this is evidenced by a shift in recent publications that other problems such as uncertainty and change have also draw the researchers' attention. This diversity of problems is because cybersecurity economics draws on and provides nexus for many diverse and multidimensional issues such as budgeting, interdependent risks, information asymmetry, governance, and types of goods. Cybersecurity economics must concern itself with the general evolution of digital ecosystems and human behavior and relationships. Thus, it has to draw upon different schools based on the underlying assumptions and a vast range of disciplines such as technology, sociology, psychology, ethics, and mathematics.

[5] While a full explanation of why some researchers take specific school of thought is beyond the scope of this paper, some scholars put schools of thought with different ideas into a single paradigm, or, as we support in this study, separate a school of thought into different paradigms [29].

We emphasize that all these schools of economic thought are scientific and informative. They look at economic phenomena from their particular paradigmatic viewpoints, and together they provide a more balanced understanding of the economic phenomenon under consideration. However, the purpose of this paper is to describe a process whereby a researcher reflects upon differing research paradigms in the field of cybersecurity economics. This field of research requires more studies on research methodologies and conundrums and dilemmas of research experienced in the research process. This work is an initiative to direct the research efforts towards these topics. The next section, we present a brief background on multi-paradigmatic approach and define the terms to be used to make the position advocated in this paper as clear as possible.

3. Background and Definitions

The real world, according to Bhaskar, should be seen as ontologically stratified and differentiated [30]. That is, it consists of a multitude of structures that create the events that occur and do not occur. Adopting a particular paradigm is like viewing this world through a particular instrument and focus on certain aspects of the situation. Research studies have been trying to deal effectively with the full richness of the real world. These studies are not single, discrete events. They are processes that proceed through a number of phases which pose different tasks and problems for the researchers. In some phases, the usefulness of research methods is different. However, combining a range of methods may yield better results. The advantages of multi-method studies are highlighted by Tashakkor and Teddie [31]. However, our argument is a strong one in support of multi-paradigmatic approach, suggesting that it is important to utilize a variety of paradigms in cybersecurity economics research. While research methods are systematic tools used to find, collect, analyze, and interpret information, paradigms determine how members of research communities view both the phenomena their particular community studies and the research methods that should be employed to study those phenomena. For example, dealing with only what may be measured or qualified, or subjectively ignoring social and political contexts of cybersecurity produces different, and sometimes incompatible, results which causes perplexity[6].

There is a need for further clarification of just what is meant by multi-paradigmatic approach, what is useful about these approaches, if the academic debate is to progress and if practitioners are to achieve the greatest benefits from adopting them. We start by defining some terms to be used in Table 1. These terms are open to many interpretations. Therefore, we recognize that these are not claimed to be correct in an absolute sense. Moreover, a multi-paradigmatic research design space provides freedom of well-informed choice and the potential for transformative research design. The key to envisioning a multi-paradigmatic research design space is to imagine paradigms not as all-encompassing frameworks but as referential systems of knowledge generation.

As Table 1 shows, by the term paradigm we mean a specific academic framework for conceptualising, investigating and communicating about the world. Each paradigmatic view about the world's constitution, structure, values, and assumptions is known to be valid. Although paradigms might resemble worldviews to some extent, they are not so all-encompassing. The notion of paradigm has been translated differently in differnet fields. For example, Govianni Dosi defines technological paradigm as an outlook, a set of procedures, a definition of the relevant problems, and of the specific knowledge related to their solution [33]. A paradigm, in that context, is then a collectively shared logic at the convergence of technological potential, relative costs, market acceptance, functional coherence and

[6] Complicated and baffling situations that you are unable to deal with or understand.

Term	Definition
Research Paradigm	Universally recognized scientific achievements that, for a time, provide model problems and solutions for a community of practitioners. Each paradigm generates and develops theories, concepts, and means of experimentation, instrumentation, and equipment which are different from those of other paradigms [32].
School of thought	A school of economic thought is a group of economists who share common ideas about economic philosophy, hold similar opinions on how the economy functions, and usually apply similar methodologies in their analyses.
Methodology	Theory of how research should be undertaken, including the theoretical and philosophical assumptions upon which research is based and the implications of these for the method or methods adopted. The epistemology (the philosophy of how we come to know) explicitly drives the methodology (the practice of how we come to know)
Epistemology	The nature of knowledge. That is, they are assumptions about how one might go about understanding the world, and communicate such knowledge to others. That is, what constitutes knowledge and to what extent it is something which can be acquired or it is something which has to be personally experienced.
Ontology	The very essence of the phenomenon under investigation. That is, to what extent the phenomenon is objective and external to the individual or it is subjective and the product of individual's mind.
Method	Techniques and procedures used to obtain and analyse research data, including for example questionnaires, observation, interviews, and statistical and nonstatistical techniques.
Multi-method Research	Use of more than one technique in different phases of research (i.e., data collection, analysis, interpretation, and evaluation).
Multi-paradigmatic Approach	A process to systematically and thoughtfully listen, understand, appreciate, and learn from multiple paradigms, values, standpoints, and perspectives, and bring them together on research projects that we are working on.

Table 1
Definition of Important Terms

other factors. However, in this study we focus on research paradigms as defined in Table 1. Table 2 shows four popular paradigms and their associated methodologies employed in the cybersecurity economics literature. This is not a comprehensive list and we can find studies that have adopted other paradigms such as Emanacipatory, Positivism, and Pragmatism. The variety of these paradigms suggests that adoption of multiple paradigmatic views would provide the researchers and practitioners with a greater appreciation of problem situation (discussed in Section 5) than any of them could by itself. Since each paradigmatic view brings with it its own set of practical methodologies (some of them are outlined in Table 2), the multi-paradigmatic approach increases the number and widens the variety of methods which can potentially be employed in a research project.

Nevertheless, we recognize, like Kuhn, the incommensurability (but not incompatibility) of paradigms due to their contrasting ontology, epistemology and methodology. The advocates of the single paradigm research argue that paradigms are incommensurable and incompatible which means that two paradigms should/could not be used the in context of the same study [34]. This idea is based on the fact that there are quite different epistemological, ontological and methodological assumptions that underpin different

Paradigm	Description	Methodologies
Functionalist	It sees the world objectively and requires logical proofs and deductions, verifiable facts and hypotheses, exact and certain measurements.	System Theory, Socio-technical Systems Theory, Contingency Theory, System Dynamics, Organizational Cybernetics
Interpretivist	It sees the world subjectively and recognizes individual differences, the social world, and it accepts that we are unpredictable.	Social Systems Sciences, Soft Systems Methodology, Robustness Analysis
Post-modernist	It holds a unique appreciation of the limitations of human understanding and biases. It knows little about the depth and complexity of the world and questions reflexively the very bases of our assumptions.	Critical Pragmatism, and Local Systemic Intervention
Critical Realism	It sees the world as being complex and organised by both overt and hidden power structures. It also perceives the social world as being orchestrated by people and institutions.	Chaos and Complexity Theories

Table 2
Four Popular Paradigms in Cybersecurity Economics Literature

paradigms. The incommensurability of the paradigms has left the multi-paradigm debates without proper theoretical grounding for their use as an approach to research and practice. There are known approaches such as atheoretical pragmatism [35], complementarism [36], and metaparadigmatic [24] to the problem of paradigm incommensurability[7]. Moreover, the successfully adoption of this approach in several fields such as business, management [38, 39], organizational behavior, and system science [23] reflects the feasibility of our proposition. Landry and Banville [40] and Mingers [41] also have strong arguments in favor of desirability of pluralist methodology in the research field of information systems. In addition, single-paradigmatic research has been criticized by two well-established research paradigms; interpretivism [42], and criticalism [43, 44]. The interpretive research paradigm is concerned with context-based understanding of individual's thoughts and values, and social actions. As social values and actions became more important in today's societies, researchers began to embrace the critical paradigm. This paradigm concerns with social equity, diversity and sustainability. These research philosophies support multi-paradigmatic approaches to conduct inquiries that are not limited to one aspect or one agent in socio-technical systems.

In this paper, the fundamental idea of a multi-paradigmatic approach in cybersecurity economics research is 1) dialectically listen to different paradigms, disciplines, theories and research stakeholders perspectives; 2) create a practical research plan by combining important ideas from competing epistemological values; 3) conduct the research ethically; 4) facilitate dissemination, understanding, and utilization of research findings for both other researchers and practitioners; and 5) continually evaluate the research outcomes and utilization process to analyze if the research is having the desired socio-technical impacts. This approach is advantageous due to its capability in approaching dynamic and complex situations. It also empowers researchers to remain open to drawing upon new research methodologies and paradigms if new and unexpected problems eventuate. To be multi-paradigmatic does

[7] Since Discussing these approaches is beyond the scope of this paper, we suggest to read [37].

not permit the researcher to be less rigorous or ethical in the research process, rather it entails a heavier burden of research thoroughness [45]. We see paradigms as useful constructs to aid understanding. They are not claimed to be the only and the best aids. They help in differentiating various perspectives that exist regarding a given phenomenon. There is no single paradigm that can capture the essence of reality and apprehend the totality of that phenomenon.

Since academic models are inevitably the products of a partial view point, they will always be biased [46]. Hence, a multiplicity of paradigms and perspectives is required to represent the complexity and diversity of phenomena and research problems. The next section views multi-paradigmatic approach as one of the elements significant to the growth in cybersecurity economics. According to this perspective, the establishment of a multi-paradigmatic approach requires that different disciplines be observed; these being sociology, psychology, behavioral science and what might be described as social psychology. Therefore, the next section discusses the feasibility of adopting this approach.

4. Feasibility of a Multi-Paradigmatic Approach in Cybersecurity Economics Research

The construction of cybersecurity economics models, and more recently, decision support systems, has undoubtedly been driven by pragmatic concerns of practitioners and decision makers to secure their environment (e.g., organizations, governments, or groups). It has also been influenced by the desire of the professional associations, primarily standard and technology institutes (e.g., NIST or NIS-Directive) to codify what they consider "best" or "good" practice to guide practitioners and to provide basis for professional qualifications and quantification. The resulting focus on underlying multidimensionality, uncertainty, and complexity indicates that tt is time to go beyond a narrow, limited view of reality and embrace a multidimensional worldview of multiple interconnected realities that possess the will and the vision to enhance the cybersecurity posture of our societies. We understand that going beyond involves transforming consciousness to higher levels of awareness and understanding of oneself, others, and the complex interconnectedness of all things. Thus, one might ask, "Is multi-paradigmatic approach feasible in cybersecurity economics research?"

The answer to this question arises two conceptual challenges. First, note that this proposition can be conceptualized in different ways: 1) it might hold that multi-paradigmatic approach should support and encourage researchers to adopt a variety of research paradigms and does not specify when and how they should be used, 2) different paradigms are viewed as compatible, consistent, and commensurable such that each paradigm would be seen appropriate for a particular research context and set of assumptions, 3) as advocated in this paper, all research situations in cybersecurity economics context are seen as inherently complex and multidimensional, and thus should benefit from different paradigms. Second, when used in cybersecurity economics research, different paradigms often produce mixed knowledge that incorporate issues from both abstract and concrete disciplines. One can make a strong case that this knowledge causes confusion and question the usability of it in practice and context.

To address these challenges, we describe the multi-paradigmatic approach in cybersecurity economics research as a process of i) examining critically personal and professional values and beliefs, ii) exploring how worldviews have been shaped and governed by largely invisible social and cultural norms, iii) appreciating and understanding the intertwined role of institutions in reducing uncertainties and establishing sustainable, secure cyberspace, and iv) delineating future scenarios as away to anticipate challenges, opportunities, and threats for organizations and governments' contingency planning. This process produces a style of research that synthesizes divergent insights. The results of this research are more likely to be accepted and used because of participatory nature of cybersecurity[8]. Therefore, we emphasize that multi-paradigmatic approach is a process that evolves dialectically. It requires much effort and skill to accomplish, deal with, and understand. This approach can be viewed as a team or group process where members are purposively included. They have different perspectives that are important for the research or evaluation of the results and outcome. In this sense, the group can help to mediate some tensions withing the context of cybersecurity such as 1) micro, meso and macro levels in decisions, 2) treating cybersecurity as a private good or public good, 3) individual needs, local needs and national needs, 4) order and chaos in cyber crisis management, and 5) individual to institutional perceptions and values.

We must also recognize that this process has philosophical (e.g., paradigm incommensurability), cultural (e.g., reluctance and resistance in adoption of a multi-paradigmatic approach among the research community), psychological (e.g., the demands of moving between fundamentally different sets of assumptions), and practical (e.g., establishing a diverse research community working on cybersecurity economics) problems . It is also true that a filed of research cannot aim to discover everything about everything. It must have defined boundaries and particular questions to answer. However, a multi-paradigmatic approach does not ask for impossible. It simply suggests establishing a dialectic discourse and realizing a rational consensus in which a research situation within cybersecurity economics is influenced by a range of various factors that can change the richness and validity of the results. Moreover, these problems can be alleviated to some extent when the research is organized into a research program. That is, the result and conclusions of individual research projects, which might be largely single paradigmatic, can be linked to others that adopt a different paradigm by other researchers. This results in the overall research program being rich and multi-paradigmatic. Consequently, we found this approach to be feasible and practicable. Hence, the multi-paradigmatic research within cybersecurity economics should be viewed as a regulatory focus that suggests a match between orientation to a goal and the means used to approach that goal. The next section of this paper offers some practical guidance for adoption of a multi-paradigmatic research and three examples of research that have adopted such approach.

5. Practical Guide for Multi-paradigmatic Approach

We have so far argued that multi-paradigmatic approach in cybersecurity economics research is both desirable and feasible, although there are a number of challenges to be overcome. However, a valid question that arises and may concern researchers is: how can we utilize this multi-paradigmatic character, as described, for the benefit of our research and practice? In this section, the first part suggests some practical guidance to adopt a multi-paradigmatic approach in a systematic way. The second part illustrates these guides with three examples of multi-paradigmatic research within cybersecurity economics.

Understanding the problem and making decision about which methods are appropriate to solve that problem has been the first part of a long-established method to formulate the research design. In order to utilize the multi-paradigmatic character we must rethink this part to accurately determine and examine the possible contribution of different paradigms in the specific issue under study, and discuss it with

[8] Cybersecurity, as defined in Section 2 is a set of activities that involves particular people (individuals or groups), organizations, governments, and institutions taking part in it.

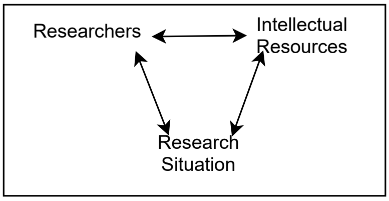


Figure 2: The relationships of researchers, research situation, and intellectual resources forms the research context for the issues under study.

other members of research group or community. Hence, we suggest that three sets of relationships need to be considered first to determine both the initial actions taken and planning or design of the research process. Figure 2 shows these sets. The research situation includes stated aims, objectives, research questions together with stakeholders, funding bodies, and particular types of institutions (e.g., regulatory agencies, standards bodies, and cybersecurity associations). The next set is the researcher or researchers engaged within the research situation. The intellectual resources consist of theories, research methods and methodologies, and frameworks that could potentially be relevant to the research situation. Two sets of researchers and intellectual resources are also interrelated as the required resources are not necessarily within the researchers' current capabilities. These relationships cover the complex interaction of people, ideas, knowledge, social and institutional practices, and technology.

As one of the contentions of this study, in the development of cybersecurity economics research, little attention has been paid to these relationships, particularly the role of researchers in the research context and their relationships to both the intellectual resources and research situation. The position of a researcher, or a group of researchers in a department or faculty, is influenced by many factors ranging from the nature of an individual's training to the tradition of a research group and the level of sophistication about the epistemological issues involved. This position impacts on the researchers' practical and critical view creating the false impression that cybersecurity economics research is far away from the world of practitioners. Therefore, a group of researchers conducting theoretical or practical research in a conscious, cooperative and reflective manner is bound to integrate critical elements in their efforts, since any issue that arises in their studies has socio-technical dimensions. It should be noted that it is not expected to cover all possibilities in a study. However, the research context, as described above, allows us to practically conduct a research that choices are made consciously in the light of full range of prospects, rather than from a very limited repertoire.

After realising relationships in the form of research context, researchers could investigate the issue under study. This investigation can be conducted in several subgroups. Each subgroup can engage in investigation of distinct data since what constitutes data varies depending on the paradigm. Next, they see if they have come to similar or different conclusions. Such setting would help researchers realise all the epistemologies underlying their research, as well as the consequences of each choice they make. It also enables them to recognize and understand the crucial conceptual boundaries of the combinations they use in research and practice. Thus, they would be open to alternative ways of thinking, born from combining elements from different paradigms. This would gradually ensure the key condition for utilizing the multi-paradigmatic approach in cybersecurity economics research. We emphasize that each element drawn from a specific paradigm should be established as a choice, so that the multi-paradigmatic character does not endanger the theoretical cohesion of the research conducted.

It is essential that researchers preserve the epistemic integrity of research methods drawn from various paradigms. In this approach, multiple paradigms serve as referential systems of knowledge creation processes and establishing suitable criteria for validating this knowledge. Therefore, cybersecurity economics researcher draw upon these paradigms and employs a hybridity of research methods with which to address complex, socio-technical research problems associated with the demands of professional practices. They need to ensure that appropriate quality standards, or empirical or experimental epistemic warrants, are used to regulate and justify different type of knowledge produce during the inquiry.

A last, yet significant, step we can add concerns mapping methodologies and assumptions in the research. Various methodologies could be regarded as a complementary set because they each rested upon different assumptions about the nature of some problem contexts. This study has continually stressed the need to challenge fundamental assumptions such as rationality and self-interest behavior. Ardalan says *in order to understand a new paradigm, theorists should be fully aware of assumptions upon which their own paradigm is based [47].* The point is that employing a multi-paradigmatic approach produces emergent and holistic reality constructed according to multiple disciplines and complex epistemological values. Therefore, the success of this approach and appropriately mapping assumptions and methodologies in a particular study requires that researchers thoughtfully dialogue with all validity types relevant to that study. As a starting point for this dialogue, this section identifies and highlights five interconnected core themes with special relevance in cybersecurity economics:

Complexity. There is a growing consensus on the complex nature of both cybersecurity and the economics subjects (i.e., subjects that are formed by a multiplicity of interacting heterogeneous agents that connect dynamically and change their behavior as the interactions unfold.) Agents are asymmetric at different levels, and therefore their capabilities are subject to various constraints such as transaction costs, bounded rationality, market imperfections, to which the actions of the agents must conform. The following characteristics are considered as the common nature of complexity:

- **Heterogeneity, Adaptation, and Evolution:** heterogeneous group, network, or society are distinctly nonuniform in one of the characteristics, conditions, and compounds that define their behavior. Individuals, organizations, and governments operate in networks of complex adaptive groups of agents that interact, adapt, learn, and evolve. For example, humans are adaptive agents in their interpersonal systems, organizations are adaptive agents in regulatory systems, and governments are adaptive agents in political and economic systems. As the interaction among the heterogeneous agents occurs, agents learn and adapt, leading to a systematic and ongoing evolutionary process where both the individual agents and the whole system are subject to change. It is important to learn to flow with the change because we have limited resources and capabilities to fully control the change processes. Therefore, cybersecurity economists need to leverage the best of these changes and deal with interrelated factors that are adaptable and evolving. They also need to empower the decision-makers to capture the contexts and clarify their tactical, operational, and strategic positions to pursue the system's purpose. Heterogeneity, evolution, and adaptation are the most striking features of the complex socio-technical systems that have made one-size-fits-all approaches unlikely to succeed. Moreover, considering these features is important to propose proportionate cybersecurity measures and controls.
- **Nonergodicity.** As we mentioned earlier, change is a constitutive element of digital ecosystems. These systems do not exhibit a nontrivial development on the local and global scale. Their state depends on the unpredetermined path that the system has followed (i.e., path-dependent). Moreover, their development is irreversible, meaning that they cannot meet the same status again that they had met before on their development path. In such systems, even a minor incident for an

agent might significantly affect the overall dynamics of the system during a cumulative process. This property is supported by [48, 49].

- **Phase Transition.** The system shows a phase transition if it undergoes exogenously introduced sudden changes in its characteristics, behavior, or the structural patterns that it generates [50]. Disruptive technological innovations are an example of phase transition in digital ecosystems. It is important to preserve the security of the system and protect the valuable assets after the transitions.
- **Emergence.** In a system, emergence occurs when simple interactions among low-level system components give rise to new and unexpected patterns or properties, disparate from the properties of the system as a whole [51]. In digital ecosystems, which are known as adaptive and self-organizing systems [52], regular modifications to the system, caused by ever-changing agents behavior and interactions, may lead to the creation of unforeseen patterns, properties, or outcomes, thereby exhibiting emergent behavior. Internet and some artificially intelligent application are popular examples of emergence in digital ecosystems. The authors in [53][9] state that security in cyberspace undoubtedly belongs to emergent properties.

Dynamic. Due to the growing interconnectedness in the digital ecosystem, cybersecurity economics decisions are extending from conventional static temporal optimization to dynamical inter-temporal optimization problems [54]. Thereby, an enhanced understanding of individual and institutional dynamics signifies a noticeable change in the direction of cybersecurity economics research. The following are considered as general properties of dynamic systems:

- **Time.** For real-life dynamic socio-technical systems, the performance is usually time-variant. A realistic analysis and a model describing the system's behavior need to take into account both the random and temporal character of the system and include the time-variant uncertainties. Such an analysis is crucial for reducing the costs, improving the sustainability of the systems, and making informed preventive condition-based security-related decisions. This results in more computationally expensive models; however, there are various techniques such as surrogate modeling [55] that facilitate the analysis. Generally, the time-variant analysis methods can be categorized into two types: simulation methods (e.g. Monte Carlo Simulation [56] and Importance Sampling [57]) and analytic methods (e.g. outcrossing rate-based methods [58]) [59].
- **Irreversibility.** Dynamic systems are either time-reversible or time-irreversible. Weiss defines a stationary process $X(t)$ as time-irreversible if $\{X(t_1), X(t_2), ..., X(t_m)\}$ and $\{X(-t_1), X(-t_2), ..., X(-t_m)\}$ do not have the same joint probability distributions for every t_m $(m \in \mathbb{N})$ [60]. Arrow and Fisher noted that the decision problem relating to irreversibility derives from the fact that an irreversible action is sufficiently costly to reverse that this should be taken into account in the initial decision [61]. [62] discusses that in a complex, evolving system that is imperfectly understood, irreversibility should be taken into account since it provides a straightforward way of analyzing strategies that affect the transition probabilities for the system in any given state.
- **Out-of-equilibrium dynamics** By introducing bounded rationality, heterogeneity in preferences, and social interactions, we should not expect to find a unique and stable equilibrium in which agents fully control and adapt all the changes that affect them. It is essential to mention that out-of-equilibrium dynamics are the rule, not the exceptions. The notion of equilibrium has

[9] Only the abstract is in English

lost relevance in orthodox economics after recognizing that economic relations take place in a complex ecosystem. This poses significant challenges to the policy and practical implications of cybersecurity economic models. They are not able to respond to ongoing reality where various goals, preferences, and mental models coexist and coevolve.

- **Non-linearity.** Non-linear dynamic systems behave differently in different regions in the state space. The non-linear adjustment of agents' cybersecurity posture to shocks caused by cyber-attacks, new regulations and budgeting changes is attracting increasing attention in the empirical literature [63, 64]. These studies have found strong evidence of non-linearity in cybersecurity when regulations and investment are used as the variables governing cybersecurity. In a non-linear setting, the adjustment process depends on the sign (positive or negative) and the magnitude of the system's shocks and history. It is important from the policymaking viewpoint because the possibility of structural collapse or institutional degradation increases in non-linear systems.

Interdisciplinarity. cybersecurity is complex and controversial. Hence, cybersecurity economics cannot be understood simply as a single, independent discipline. The insight that interdisciplinarity is necessary is not new. However, to make interdisciplinarity work, researchers would have to spend efforts on finding effective ways to share and understand their discourse and training paradigm-switching capabilities (being able to view and analyze a complex issue from different perspectives). These efforts are not limited to academia but also are essential for policy- and decision-makers. Drawing knowledge from other established disciplines such as cognitive science, information systems, and computational intelligence empowers them to cover modeling, measuring, and managing cybersecurity within the context of stakeholders' tactical and strategic goals.

Social Rules and Institutions. Social rule system theory and complex institutional arrangements are applied to the description and analysis of how agents are organized and structured through their actions and interactions. We demonstrated that cybersecurity economic models connect to reality through economic variables (e.g., ALE, ROSI, and ENBIS) and understanding the economic institutions and social rules. Social rules and institutions profoundly shape the behavior of operating agents and systems. Thus, it is a fundamental error to suppose that they are unlikely to override the preference of agents to pursue their diverse goals. Cybersecurity is governed by institutions that are composed of numerous rule configurations. The rules have strong interdependencies, both with each other and with system conditions. A change in any of these rules produces a different situation and may lead to different outcomes. For example, GDPR impacted the data collected and stored in emerging private, and public blockchain [65]. This regulation has impacted the decisions and created barriers for an organization to embrace this technology.

Ethics. Although explaining the moral behaviors by mainstream economic models is difficult, such ethical foundations have been extended into economic analysis. Consider cyber insurance and cyber policies as two examples. Insurers and insureds in the context of cybersecurity insurance seek their own self-interest, but their behavior is also often honest and honorable. Or, policies, regulations, and rules are typically designed to maximize aggregate welfare in the societies, which is certainly an ethical goal. Therefore, neglecting ethics means ruling out possible explanations of behavior. As we argued before, the goal of cybersecurity economics is to explain and predict the behavior and patterns of the agents and systems, design institutions, and recommend policies and regulations. Therefore, cybersecurity economists should be willing to modify, extend, or reject the methods and approaches that they employ to fulfill this goal based on practical and moral evidence.

6. Examples of Empirical Research

The second part of this section focuses on giving three examples that have followed a multi-paradigmatic approach in their studies. These are good examples, but they are by no means perfect as various limitations are highlighted bellow[10]. First, the study by Gilad et al. has made the dominance modern warfare a focus of attention [66]. The study shows how countries can establish procedures and determine the budgets to optimally allocate cyber-defense resources to prevent harmful cyber-attacks on the complex computer networks that manage their infrastructure, business, security, and government operations. The second example aims to identify and investigate the antecedents of enhanced level of cyber-security at the organisational level from both the technical and the human resource perspective using human–organisation–technology (HOT) theory [67]. Finally, the third study examines the interaction between firms in a specific industry and a strategic hacker by considering industry-specific characteristics including the intrinsic vulnerability, intentions of the hacker, competition between firms, and similarity of security technologies [68].

Study 1: This study accounts for various strategic behaviors and technological capabilities of the agents that are involved in their demonstrated research situation. They draw special attention to the need for coordination and synchronization of the intelligence process across the users of military intelligence, such as policymakers in the government and various security agencies. The mapping between assumptions (budget constraints, heterogeneous maturity levels of both attackers and defenders, and amount of possessed intelligence) and methodologies is followed cautiously supported by the literature and authors' observations. The analytical model inspects the physical, personal, social, and institutional views and assesses the impacts of security intelligence on the country's military capability, national security, and welfare.

Study 2: This study acknowledges the multi-dimensional nature of the cybersecurity economics research. It investigates the determinants for enhanced cybersecurity level in organisations. The determinants are identified through literature review and questionnaires. The results provide significant insights on technical, legal, organizational, and managerial aspects of cybersecurity across different sectors such as healthcare, retail, and education. While this study has not included the social aspects in their constructs and measurement items, it has partially covered the physical, personal and institutional views.

Study 3: Wu et al. consider the strategic hacker's behaviour and industry-specific characteristics to offer a number of managerial implications that could be referenced in the security practice of competitive context. Moreover, they show that different intentions generate different hacker's behaviour. Therefore, it prompts the competitive firms to notice the strategic importance of discriminating against the opponent's intentions and assessing the potential threats in security strategies. The assumptions of this study and research situation direct the authors to employ research methodologies that are appropriate to deal with several real-world conditions such as competitive firms, free-riders, and asymmetric relations.

Evaluating these studies shows that they have developed multi-paradigmatic research wherein a range of ideas were combined to meet the needs of particular research situations. In relation to the argument of this paper, the studies demonstrate clearly the way in which different paradigms, even when applied to the same data, yield different views of the world. Moreover, in terms of the research context (see Figure 2), it is interesting to note how research methods affect the relationship between the research situation and researchers in such multi-paradigmatic studies. However, our evaluation also

[10] It should be noted that our analysis relies on the published studies. We have not investigated the authors' background and their research community for further description of relationships shown in Figure 2

reveals limitations of these particular research studies[11].

Regarding the first study, we pose two critical questions that can be answered considering the research topics that we outline earlier in this section: What is the relative importance of accuracy, quality, and reliability of the military intelligence when assessing the ethical behavior of cybersecurity practitioners in the military or policy-makers? Does the cybersecurity practitioners' belief that a formal code of ethics is necessary significantly change the key elements of effective intelligence? This should have led to empirical investigations and complementary qualitative methods to identify differences in how ethical issues are perceived in such settings. In the second study, there is no qualitative data and little consideration of the social and political aspects of antecedents for enhanced level of cybersecurity. Moreover, the interrelationship of the antecedents is overlooked in this study. This limitation ignores the emergent characteristics in complex socio-technical systems. Techniques such as interpretive structural modelling and analytic network process can be used to address these limitations. Finally, to obtain the equilibrium solution, the third study solves the optimisation problem based on two unrealistic assumptions: 1) the firm's security decisions have been exogenously given, and 2) all players are entirely reasonable and risk neutral. Methods that might help with this could be Cumulative Prospect Value (CPV) [69] or Quantal Response Equilibria (QRE) [70].

Our reflection on the investigation of cybersecurity economics literature shows that to conduct the research successfully requires a multi-paradigmatic approach to be adopted. The objectives of this field of research will be constantly changing and the nature of the inquiry by the researchers and practitioners will be dynamic. Therefore, a multi-paradigmatic approach will facilitate finding solutions to emerging problems and developing responsive and multi-pronged cybersecurity strategies using the outcomes provided by the cybersecurity economics research.

7. Summary and Conclusion

Different paradigms are adopted in cybersecurity economics studies. This paper sets out a statement of the new studies establishing the case for multi-paradigmatic approaches to foster transdisciplinary research in the field of cybersecurity economics. This approach is applicable to a wide range of research contexts in this field and can be considered as a means of transforming the policies, structures and processes of cybersecurity governance and management, and for the purpose of ensuring that both science and technology contribute to sustainable development of secure socio-technical systems. Therefore, this paper discussed the desirability and feasibility of this approach along with some guidelines that can be followed to initiate a multi-paradigmatic research project. While paradigms place severe constraints on the future directions of research development, multi-paradigmatic approach channels opportunities to advance in cybersecurity economics. For example, mutual adaptation of individuals' behavior and technological systems in the wider institutional framework in which organizations operate is an example of multi-paradigmatic research context that develops new knowledge relevant to the enhance governance of cybersecurity. Or, other newly emerging problems such as sovereignty in cyberspace [71], cybersecurity as a public good [72] or ambiguities regarding active cyber defence [73] are among the topics that multi-paradigmatic work on them constructs practical and applicable knowledge.

Moreover, multi-paradigmism is unavoidable if realistic insights and relevance for practical affairs are to be achieved. This is why we aim to sensitize future researchers to develop their work with an explicit

[11] These limitations are not outlined in the studies and they are the result of our critical evaluation

acknowledgment of different ontological, epistemological, and methodological perspectives. However, researchers are not the only actors in a research field. From a practitioner perspective, our paper may motivate practitioners to be more reflective, more ethically aware, and more context-sensitive. From journal and publication channels perspective, our paper emphasizes that the reviewers positively examine the assumptions and the grounds that inform the research process. Moreover, this multi-paradigmatic character can function as an opportunity for dialogue and complementarity. This paper has hinted at the importance on paradigm dialogue directed towards five core themes with special relevance in cybersecurity economics. It also investigated three new studies to discover if this approach can be utilized to offer new perspectives and therefore enrich cybersecurity economics research, providing a deeper understanding of the complex and multifaceted issues under study.

While the manner of employing multi-paradigmatic approach to analyze complex problems in cybersecurity economics is explicated in this work, the way in which methodologies might be combined to change problem situations is not thought through. Our future work will provide a better understanding of this process and presents a framework for the multi-paradigmatic research design. This framework is an important artifact since it helps to prevent confusion in the research process. However, as stated above, multi-paradigmatic approach has been practiced in other fields, and therefore it is important to consider what could be learnt from their experience. Therefore, a systematic literature review on the detailed characteristics of this approach can help to advance this concept among the cybersecurity economics researchers.

References

[1] L. A. Gordon, M. P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security (TISSEC) 5 (2002) 438–457.

[2] J. Willemson, On the gordon & loeb model for information security investment., in: WEIS, 2006.

[3] K. Hausken, Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability, Information Systems Frontiers 8 (2006) 338–349.

[4] M. A. Centeno, M. Nag, T. S. Patterson, A. Shaver, A. J. Windawi, The emergence of global systemic risk, Annual Review of Sociology 41 (2015) 65–85.

[5] M. D. Cavelty, Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities, Science and engineering ethics 20 (2014) 701–715.

[6] I. G. Secretariat, Cybercrime: COVID-19 impact, Technical Report, 2020. URL: https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

[7] C. D. of Federal Bureau of Investigation, 2019 Internet Crime Report, Technical Report, 2020. URL: https://pdf.ic3.gov/2019_IC3Report.pdf.

[8] C. D. of Federal Bureau of Investigation, Microsoft Digital Defense Report, Technical Report, 2020. URL: https://pdf.ic3.gov/2019_IC3Report.pdf.

[9] O. Pieczul, S. N. Foley, V. M. Rooney, I'm ok, you're ok, the system's ok: Normative security for systems, in: Proceedings of the 2014 New Security Paradigms Workshop, 2014, pp. 95–104.

[10] A. Kuehn, M. Mueller, Shifts in the cybersecurity paradigm: zero-day exploits, discourse, and emerging institutions, in: Proceedings of the 2014 New Security Paradigms Workshop, 2014, pp. 63–68.

[11] H. Vescent, B. Blakley, Shifting paradigms: Using strategic foresight to plan for security evolution, in: Proceedings of the New Security Paradigms Workshop, 2018, pp. 28–40.

[12] J. Joque, S. T. Haque, Deconstructing cybersecurity: From ontological security to ontological insecurity, in: New Security Paradigms Workshop 2020, 2020, pp. 99–110.

[13] J. M. Spring, T. Moore, D. Pym, Practicing a science of security: a philosophy of science perspective, in: Proceedings of the 2017 New Security Paradigms Workshop, 2017, pp. 1–18.

[14] J. Grossklags, N. Christin, J. Chuang, Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents., in: WEIS, 2008.

[15] C. C. Demchak, Uncivil and post-western cyber westphalia: Changing interstate power relations of the cybered age, The Cyber Defense Review 1 (2016) 49–74.

[16] H. Asghari, M. van Eeten, J. M. Bauer, Economics of cybersecurity, in: Handbook on the Economics of the Internet, Edward Elgar Publishing, 2016.

[17] M. Felici, N. Wainwright, S. Cavallini, F. Bisogni, What's new in the economics of cybersecurity?, IEEE Security & Privacy 14 (2016) 11–13.

[18] A. Bird, Thomas Kuhn, in: E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy, winter 2018 ed., Metaphysics Research Lab, Stanford University, 2018.

[19] C. Perez, Technological revolutions and techno-economic paradigms, Cambridge journal of economics 34 (2010) 185–202.

[20] T. S. Kuhn, et al., Criticism and the growth of knowledge: Volume 4: Proceedings of the International Colloquium in the Philosophy of Science, London, 1965, volume 4, Cambridge University Press, 1970.

[21] R. Anderson, Why information security is hard-an economic perspective, in: Seventeenth Annual Computer Security Applications Conference, IEEE, 2001, pp. 358–365.

[22] K. L. Hall, A. X. Feng, R. P. Moser, D. Stokols, B. K. Taylor, Moving the science of team science forward: collaboration and creativity, American journal of preventive medicine 35 (2008) S243–S249.

[23] T. D. Bowers, Ontological support for multiparadigm multimethodologies: isomorphic process–structures and the critical moment, in: Proceedings of the 54th Annual Meeting of the ISSS-2010, Waterloo, Canada, 2010.

[24] R. B. Johnson, Dialectical pluralism: A metaparadigm whose time has come, Journal of Mixed Methods Research 11 (2017) 156–173.

[25] L. Wiggins, B. Marshall, Multi-level pluralism: A pragmatic approach to choosing change and improvement methods, in: Managing Improvement in Healthcare, Springer, 2018, pp. 25–41.

[26] R. Bojanc, B. Jerman-Blažič, A quantitative model for information-security risk management, Engineering management journal 25 (2013) 25–37.

[27] P. Rathod, T. Hämäläinen, A novel model for cybersecurity economics and analysis, in: 2017 IEEE International Conference on Computer and Information Technology (CIT), IEEE, 2017, pp. 274–279.

[28] E. M. Ahmed, Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth, Journal of the Knowledge Economy (2020) 1–19.

[29] Y. Changyong, Paradigmatic examination of schools of thought in educational sociology, Chinese Education & Society 35 (2002) 21–38.

[30] R. Bhaskar, A realist theory of science, Routledge, 2013.

[31] A. Tashakkori, C. Teddlie, C. B. Teddlie, Mixed methodology: Combining qualitative and quantitative approaches, volume 46, Sage, 1998.

[32] T. S. Kuhn, The structure of scientific revolutions, University of Chicago press, 2012.

[33] G. Dosi, Technological paradigms and technological trajectories: a suggested interpretation of the determinants and directions of technical change, Research policy 11 (1982) 147–162.

[34] G. Burrell, G. Morgan, Sociological paradigms and organisational analysis: Elements of the sociology of corporate life, Routledge, 1979.

[35] T. D. Bowers, Developments in critical systems theory: On paradigms and incommensurability, in: Proceedings of the 58th Annual Meeting of the ISSS-2014 United States, 2014.

[36] J. Brocklesby, Methodological complementarism or separate paradigm development—examining the options for enhanced operational research, Australian Journal of Management 18 (1993) 133–158.

[37] G. Midgley, J. D. Nicholson, R. Brennan, Dealing with challenges to methodological pluralism: The paradigm problem, psychological resistance and cultural barriers, Industrial Marketing Management 62 (2017) 150–159.

[38] J. Raftery, D. McGeorge, M. Walters, Breaking up methodological monopolies: a multi-paradigm approach to construction management research, Construction Management & Economics 15 (1997) 291–297.

[39] C. Clarke-Hill, H. Li, B. Davies, The paradox of co-operation and competition in strategic alliances: towards a multi-paradigm approach, Management Research News (2003).

[40] M. Landry, C. Banville, A disciplined methodological pluralism for mis research, Accounting, management and information technologies 2 (1992) 77–97.

[41] J. Mingers, Combining is research methods: towards a pluralist methodology, Information systems research 12 (2001) 240–259.

[42] G. Biesta, Pragmatism and the philosophical foundations of mixed methods research, Sage handbook of mixed methods in social and behavioral research 2 (2010) 95–118.

[43] D. L. Morgan, Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods, Journal of mixed methods research 1 (2007) 48–76.

[44] J. A. Maxwell, K. Mittapalli, Realism as a stance for mixed methods research, Handbook of mixed methods in social & behavioral research (2010) 145–168.

[45] P. Feyerabend, et al., Against method, Verso, 1993.

[46] K. Ardalan, Global Political Economy: A Multi-paradigmatic Approach, Springer, 2018.

[47] K. Ardalan, Globalization and finance: four paradigmatic views, Journal of globalization studies 1 (2010) 41–67.

[48] P. Cooper, Cognitive active cyber defense: finding value through hacking human nature, Journal of Law & Cyber Warfare 5 (2017) 57–172.

[49] V. Zimmermann, K. Renaud, Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset, International Journal of Human-Computer Studies 131 (2019) 169–187.

[50] V. N. Kolokoltsov, O. A. Malafeyev, Four-state model of cybersecurity, in: Many Agent Games in Socio-economic Systems: Corruption, Inspection, Coalition Building, Network Growth, Security, Springer, 2019, pp. 133–146.

[51] R. I. Damper, Editorial for the special issue on'emergent properties of complex systems': Emergence and levels of abstraction, 2000.

[52] W. Li, Y. Badr, F. Biennier, Digital ecosystems: challenges and prospects, in: proceedings of the international conference on management of Emergent Digital EcoSystems, 2012, pp. 117–122.

[53] Q. Leilei, X. Ruojin, S. Wenchang, L. Bin, Q. Bo, Cybersecurity challenges from the perspective of emergence, Journal of Computer Research and Development 57 (2020) 803.

[54] M. Kianpour, S. J. Kowalski, H. Øverby, E. Zoto, From cyber incidents to training cognitive situation management, in: 2020 IEEE Conference on Cognitive and Computational Aspects of Situation

Management (CogSIMA), IEEE, 2020, pp. 163–166.

[55] M. I. Radaideh, T. Kozlowski, Surrogate modeling of advanced computer simulations using deep gaussian processes, Reliability Engineering & System Safety 195 (2020) 106731.

[56] V. Roelofs, M. Kennedy, Sensitivity analysis and estimation of extreme tail behavior in two-dimensional monte carlo simulation, Risk Analysis: An International Journal 31 (2011) 1597–1609.

[57] Z. Wang, Z. P. Mourelatos, J. Li, I. Baseski, A. Singh, Time-dependent reliability of dynamic systems using subset simulation with splitting over a series of correlated time intervals, Journal of Mechanical Design 136 (2014).

[58] C. Gong, D. M. Frangopol, An efficient time-dependent reliability method, Structural Safety 81 (2019) 101864.

[59] S. Yu, Z. Wang, K. Zhang, Sequential time-dependent reliability analysis for the lower extremity exoskeleton under uncertainty, Reliability Engineering & System Safety 170 (2018) 45–52.

[60] G. Weiss, Time-reversibility of linear stochastic processes, Journal of Applied Probability (1975) 831–836.

[61] K. J. Arrow, A. C. Fisher, Environmental preservation, uncertainty, and irreversibility, in: Classic papers in natural resource economics, Springer, 1974, pp. 76–84.

[62] C. Perrings, W. Brock, Irreversibility in economics, Annu. Rev. Resour. Econ. 1 (2009) 219–238.

[63] L. Zhang, G. Guo, Observer-based adaptive event-triggered sliding mode control of saturated nonlinear networked systems with cyber-attacks, Information Sciences 543 (2021) 180–201.

[64] A. Nagurney, P. Daniele, S. Shukla, A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints, Annals of operations research 248 (2017) 405–427.

[65] W. E. Forum, Personal data handling, 2020. URL: https://widgets.weforum.org/blockchain-toolkit/personal-data-handling.

[66] A. Gilad, E. Pecht, A. Tishler, Intelligence, cyberspace, and national security, Defence and Peace Economics 32 (2021) 18–45.

[67] S. Kumar, B. Biswas, M. S. Bhatia, M. Dora, Antecedents for enhanced level of cyber-security in organisations, Journal of Enterprise Information Management (2020).

[68] Y. Wu, H. Xiao, T. Dai, D. Cheng, A game-theoretical model of firm security reactions responding to a strategic hacker in a competitive industry, Journal of the Operational Research Society (2021) 1–25.

[69] A. Tversky, D. Kahneman, Advances in prospect theory: Cumulative representation of uncertainty, Journal of Risk and uncertainty 5 (1992) 297–323.

[70] R. D. McKelvey, T. R. Palfrey, Quantal response equilibria for normal form games, Games and economic behavior 10 (1995) 6–38.

[71] M. L. Mueller, Against sovereignty in cyberspace, International Studies Review 22 (2020) 779–801.

[72] M. Kianpour, Heterogeneous preferences and patterns of contribution in cybersecurity as a public good, in: Proceedings of the 13th International Conference on Agents and Artificial Intelligence (ICAART 2021), Scitepress, 2021.

[73] D. Broeders, Private active cyber defense and (international) cyber security—pushing the line?, Journal of Cybersecurity 7 (2021) tyab010.

Chapter 7

Research Paper 3: Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties

Mazaher Kianpour, Harald Øverby, Stewart James Kowalski, Christopher Frantz, *International Conference on Human-Computer Interaction, 2019*

Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties

Mazaher Kianpour(✉), Harald Øverby, Stewart James Kowalski, and Christopher Frantz

Norwegian University of Science and Technology, Gjøvik, Norway
{mazaher.kianpour, haraldov, stewart.kowalski, christopher.frantz}@ntnu.no

Abstract. The most costly cybersecurity incidents for organizations result from the failures of their third parties. This means that organizations should not only invest in their own protection and cybersecurity measures, but also pay attention to that of their business and operational partners. While economic impact and real extent of third parties cybersecurity risks is hard to quantify, decision makers inevitably compare their decisions with other entities in their network. This paper presents a theoretically derived model to analyze the impact of social preferences and other factors on the willingness to cooperate in third party ecosystems. We hypothesize that willingness to cooperate among the organizations in the context of cybersecurity increases following the experience of cybersecurity attacks and increased perceived cybersecurity risks. The effects are mediated by perceived cybersecurity value and moderated by social preferences. These hypotheses are tested using a variance-based structural equation modeling analysis based on feedback from a sample of Norwegian organizations. Our empirical results confirm the strong positive impact of social preferences and cybersecurity attack experience on the willingness to cooperate, and support the reciprocal behavior of cybersecurity decision makers. We further show that more perception of cybersecurity risk and value deter the decision makers to cooperate with other organizations.

Keywords: Social preferences · Behavioral economics · Cybersecurity decision making · Structural Equation Modeling · Theory development · Perceived Cybersecurity Risk

1 Introduction

As Peter Bernstein states, “The capacity to manage risk, and with it, the appetite to take risk and make forward-looking choices, are key elements of the energy that drives the economic system forward” [1]. While risk taking is driving the modern economics systems forward, uncertainties in cyberspace like the evolving threat landscape and human error, are threatening to slow it down. Nations, organizations and individuals are unsure what a good driving strategy in cyberspace is. Individual preferences and behavioral heterogeneity can play an important role in explaining strategic considerations at organizational levels. Hence, humans play a vital role in cybersecurity

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 149–163, 2019.
https://doi.org/10.1007/978-3-030-22351-9_10

strategic decision making, and at the same time, they are often considered the weakest links in this ecosystem [2].

The area of cybersecurity in organizations has three essential properties. First, it consists of heterogeneous interacting, and in some cases, competitive and even adversarial, stakeholders and actors that are characterized by distinct local cultures, structure, machines, and methods [3]. Stakeholders act upon the basis of their own local states at any given time. Second, cybersecurity problems stem from dynamic systems and are driven by the interaction among various stakeholders. These interactions affect future local states and, therefore, create systemic complexity. Third, there are strategic decision makers whose decision processes take into account past actions, potential future actions, and outcomes of other actors. They have heterogeneous motivations, preferences, and benefits. Since these properties are based on the organizations' unique sets of objectives, processes, and resources, it is difficult to see how a one-size-fits-all cybersecurity strategy can be optimal.

The trend toward more globalized production has increased inter-organizational dependencies. Particularly, businesses are forming multi-layered supply chains, as illustrated in Fig. 1. As an externality, security and insecurity can be distributed disproportionately in a supply chain. The coopetition (i.e. organizations may both compete and cooperate at the same time [4]) and interdependent preferences among the organizations face them with a challenge of understanding and measuring the risks that are propagating from them. Recent cybersecurity incidents highlight that it is no longer enough for organizations to focus solely on their in-house cybersecurity defense mechanisms.

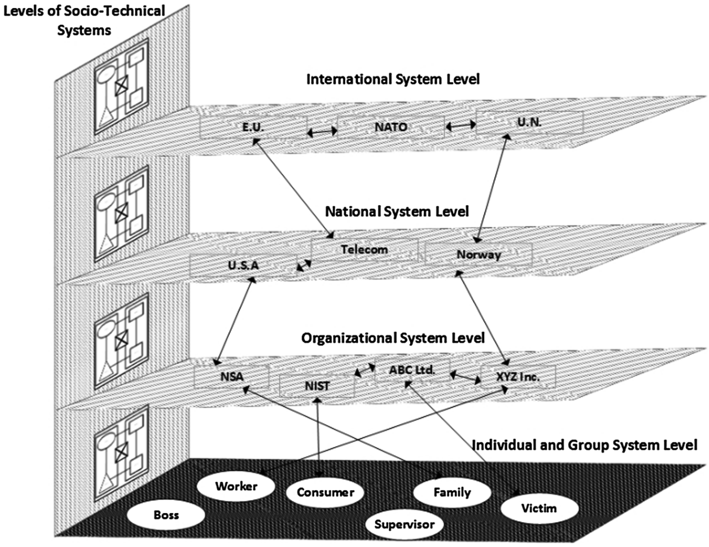

Levels of Socio-Technical Systems
International System Level
E.U.
NATO
U.N.
National System Level
U.S.A
Telecom
Norway
Organizational System Level
NSA
NIST
ABC Ltd.
XYZ Inc.
Individual and Group System Level
Worker
Consumer
Family
Boss
Supervisor
Victim

Fig. 1. Interaction among organizations in a socio-technical system is not limited to the organizational level, but also includes different levels of societal actors such as international systems and governments, groups and individuals levels. Each of these actors has their own particular instruments, which can employ different security controls depending on the nature of the system [3].

According to a study from Kaspersky Lab and B2B International, the most costly cybersecurity incidents for businesses result from the failures of their third parties [5]. This means that organizations should not only invest in their own protection and cybersecurity measures, but also pay attention to that of their business partners. To Provide some examples, in December 2018, Managed Health Services (MHS) of Indiana Health Plan announced that a third party data breach potentially exposed up to 31,876 patients' personal data in one of two security incidents the company disclosed [6]. Moreover, attackers expand their reach by targeting third-party services allowing them to steal more data. A new Magecart attack launched through compromised advertising supply chain in November 2018. Attackers loaded their malicious skimming code on 277 e-commerce websites and used their infrastructure of these companies to breach other companies [7].

Different economics models have been employed to address the challenges in the field of cybersecurity in both technical and social aspects [8–10]. In these models, agents are rational, selfish, and have complete information about other agents. However, in real-world scenarios, agents might be irrational, reciprocal, and have incomplete information about their environment. In this his paper we outline empirical cybersecurity economics examples on how these standard models fail to model real-world scenarios because they do not properly model the problems when they ignore social preferences.

The key research question is how to model heterogeneous incentives and preferences at the organizational level. The major aim is to better understand under which conditions the social preferences have significant effects on cybersecurity. To achieve this, we aim at developing an understanding of the important determinants of the socially optimal level of cybersecurity to prevent market failures.

Moreover, the paper investigates which type of social preferences (Reciprocal Fairness, Inequity Aversion, Pure Altruism and Spitefulness or Envy [11]) is stronger and quantitatively a core motive in the domain of cybersecurity. We have designed a survey to address these questions. The respondents of this survey are cybersecurity team members (Chief Information Security Officers, Information Security Analysts, Security Consultants, etc.) and decision makers in Norwegian organizations (Chief Executive Officers, Board Members, etc.).

This work is structured as follows. Section 2 provides a background on behavioral economics and proposed models to analyze behavioral determinants in cybersecurity. Section 3 proposes our research model and hypotheses. The methodological approach and data collection process is explained in Sect. 4. Section 5 presents the empirical results. Theoretical and practical implications are discussed in Sect. 6. Finally, Sect. 7 concludes this study.

2 Related Work

Behavioral Economics sits at the intersection of psychology and economics. Standard economic theories assume fully rational, completely selfish and forward-thinking decision makers. Analytical models based on these assumptions have failed to predict individuals' behavior. However, behavioral economics provides manifold principles considering less rational behavioral choices and other-regarding, interdependent preferences [12].

The application of behavioral economics has become more widespread, most commonly seen in the health domain, and policymakers use it to investigate how predictable deviations from rational behavior can be utilized to steer people to socially desirable directions. This approach is best employed where individuals need to make quick decisions and select the best possible choice.

Thaler and Sunstein [13] and Kahneman [14] popularized the idea that behaviors can be projected into systems and affect the decisions. However, in 1975, Rogers introduced a popular theoretical model of behavior change focusing on the Protection Motivation Theory (PMT) [15]. This model explicitly points out the methods that individuals can assess and counter cyber threats. Dolan et al. [16] proposed a behavior change framework, so-called MINDSPACE, which describes nine behavioral influencers in relation to cybersecurity behavior change paradigm. They discuss that these influencers play important roles in security-related decision making and behavior.

Briggs et al. state that PMT is a useful model in cybersecurity context as it encourages individuals to better protect their cyber assets from cyber threats [17]. They tried to create an effective link between PMT and MINDSPACE to present an integrated framework. This framework can be used to design long term cybersecurity behavioral strategies. It is claimed that the framework can be applied within organizations and provide important insights to managers and practitioners involved in cybersecurity.

There are a variety of psychological models of behavior that address the interplay of attitudes and behaviors. They recognize the importance of psychological traits and attitudes along with the individual's knowledge and experience in decision making. Many of these models are inspired by the Theory of Reasoned Action [18] and Theory of Planned Behavior [19]. The former identifies two factors that determine behavioral intention and assumes that behavior can be completely controlled. The latter, in contrast, differentiates between perceived behavioral control and actual behavioral control.

A survey by Michie et al. [20] shows that there are 80 available models of behavior change in different contexts. The literature review by Sommestad focuses on relevant psychological models for cybersecurity policy compliance [21]. This study identifies 60 different psychological constructs based on established theories including General Deterrence Theory, Neutralization Theory, Social Control Theory, and Theory of Moral Decision-Making. We will focus here on the Theory of Social Preferences, which is studied in behavioral and experimental economics and social psychology. We use this theory in the cybersecurity field to investigate the effects of other-regarding behavior in decision making under cybersecurity risks and uncertainties.

3 Research Model and Hypotheses

This research aims to find the impact of social preferences on the perceived cybersecurity risk, the perceived cybersecurity value, and the willingness to cooperate in third parties ecosystem to mitigate the probability and impact of future cyber incidents. In the following, we explain our research model, illustrated in Fig. 2, and the hypotheses to be tested in the empirical analysis.

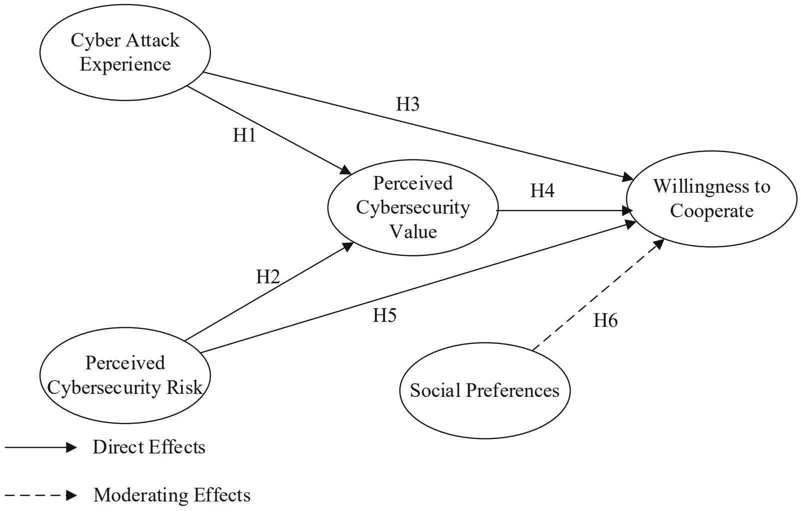


Fig. 2. Research model in path model notation

As Fig. 2 shows, the following hypotheses are proposed to conduct this research:

H1. Cyber attack experience increases the perceived cybersecurity value.

H2. Perceived cybersecurity risk increases the perceived cybersecurity value.

H3. Cyber attack experience increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.

H4. Perceived cybersecurity value increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.

H5. Perceived cyber risk increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.

H6. Social Preferences have moderating effects on the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.

The following latent variables (i.e. research constructs) are used in the proposed model:

Cyber Attack Experience: A cyber attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network [22]. These attacks hit businesses every day and their number is increasing as people are trying to benefit from vulnerable business systems.

According to the third annual report of Ponemon [23], 59% of respondents confirm that their organizations experienced a data breach caused by one of their third parties. 42% of respondents say they had such a data breach in the past 12 months. Additionally, 22% of respondents do not know if they had a third-party data breach in the past 12 months.

Perceived Cybersecurity Risk: Fear of crime consists of two distinct, but highly interrelated, components. First, the rather rational risk perception, which is often stated as the product of the probability of occurrence and the impact of the crime, and second, fear as an emotional feeling of being unsafe [24]. Visser et al. found strong effects of examining prior victimization on perceived risk [25]. Moreover, in a survey by Cisco, 69% of executives indicated that they are not willing to innovate in digital products because of their perceived cybersecurity risks [26]. The finding shows that perceived cybersecurity risk can be a deterrent of cooperation among organizations in digital space.

Perceived Cybersecurity Value: Oscar Wilde said, "A cynic knows the cost of everything and the value of nothing [27]." Cost is a driver for decisions, but not always. Perceived value is what people perceive as the value and worth of a product or service; the higher the perceived value, the more likely it is that they will pay for the product or service.

The reason that we are trying to measure perceived value and understand how it affects the decisions is that they differ from other personal attributes in several ways. Schwartz states that values transcend specific situation and are distinguished from norms, attitudes and specific goals [28]. He also explains that values are observed by subjective importance and they form a unique system of values hierarchies. Values may serve as standards and provide social justifications for behaviors and decisions [29]. Moreover, Sagiv et al. reason that perceived value influences competitive/cooperative behavior and the decisions made [30]. Therefore, to understand and predict the behavior, it is important to consider the perceived cybersecurity value of the agents in the system.

Social Preferences: Game-theoretic predictions are frequently observed in recent experiments on decision making and they have been used to refine behavioral theory. However, explaining decisions outside the laboratory and experimental elicitation of behavior in the context of cybersecurity has not received particular attention in previous studies. We consider that an individual's behavior is affected by three interrelated factors; self-interest, the behavior of others, and the reaction to rewards and punishment.

As a branch of behavioral economics, social preferences describe how economic agents maximize utility considering others' utilities. Differences in social preferences may explain how and why individuals behave in different settings. Social preferences are critical to understand how decision makers scarce resources to themselves and others. These preferences are often dynamic and complex than self-interest.

Willingness to Cooperate: In this study, the willingness to cooperate is defined as the intention of organizations to cooperate with each other to enhance their overall security posture in their third parties ecosystem. These collaborative practices can be performed like creating an incident response team, allocating resources to secure shared critical information, development, and implementation of effective security policies, plans and procedures, etc.

Unlike some studies that only focus on cooperative intentions as the desired behavior, this study also considers the competition among the organizations. The non-selfish motives not only affect cooperation, but also competition incentives. Therefore, we investigate the moderating effects of social preferences on willingness to cooperate in addition to the direct effect of *Cyber Attack Experience*, *Perceived Cybersecurity Risk* and *Perceived Cybersecurity Value*.

4 Research Method

To test the hypotheses outlined in Sect. 3, we employ Structural Equation Modeling (SEM) [31]. In this section, we describe the reasons behind selecting SEM, data collection and the development of the measurement mode.

4.1 Statistical Method

We live in a complex, multivariate world and studying the impact of one or two variables in isolation would seem relatively artificial and inconsequential [32]. Although modeling always omits some aspect of reality [33], using some approaches (e.g. regression-based approaches) may be too limiting for the analysis of the more complex and realistic situations. Haenlein points out the limitations of the methods such as factor analysis, cluster analysis, and discriminant analysis, which were popular statistical methods in psychology and sociology during the 20th century [34].

To overcome these limitations mentioned above, we apply SEM. This method allows us to model the relationships among multiple independent and dependent constructs, and observable and unobservable variables, simultaneously. There are two approaches to estimate SEM parameters: covariance-based or variance-based. Both approaches are similar, however, the covariance-based approach is more suited for confirmatory theory testing and the variance-based approach rather for theory development [35]. We use the variance-based approach, here and in the following just referred to as Partial Least Squares (PLS), because it is widely used for predictive analysis and is an appropriate technique for theory development as done in this study. This method is furthermore applicable even under conditions of very small sample size. Chin and Newsted indicated that PLS can be performed with a sample size as low as 50 [36]. Moreover, PLS can be used to analyzing models with either reflective, formative or both types of indicators [37].

We use the statistical software SmartPLS 3.0 for parameter estimation as it provides all required features for PLS analysis. First, it supports the PLS Algorithm [38] and bootstrapping, which is considered as the broadly used approach for nonparametric statistics in management, social science, and market research studies. Second, this version supports the consideration of missing values.

4.2 Sample Data

Questback, an affiliated online survey tool with Norwegian University of Science and Technology (NTNU), is used to collect the data. Recall that this study is motivated by a need to understand the effective factors of improving overall cybersecurity in organizations. Therefore, we focused on the individuals who make cybersecurity-related decisions in organizations.

This survey was active for two weeks and the link was inserted in one of the Norwegian Business and Industry Security Council (NSR) news articles[1]. This organization serves the Norwegian business sector in an advisory capacity on matters relating to crime.in different organizations in Norway. Upon clicking the survey link, participants were presented with guidelines and the definition of the terms *Third Parties*, *Retaliatory Actions*, and *Cooperation with third parties*. We provided these definitions in order to prevent ambiguous interpretation of questions. Within the questionnaire, responses to all questions were mandatory, but allowed participants to choose "I have insufficient knowledge to answer this question." if they were unsure about the corresponding question. The survey completion time ranged from 8 to 10 min.

As indicated in Sect. 3, the theoretical constructs identified in our model: *Perceived Cybersecurity Risk*, *Perceived Cybersecurity Value*, *Social Preferences*, and *Cyber Attack Experience* are measured based on different 11 questions in the survey. Answers of 8 questions are reported on 11-point ordinal scales, one question in 5-point frequency scales reporting the update of cybersecurity risk levels in the organization, and 2 questions on the binary scale (Yes, No). These questions are adapted from Ponemon's third annual report [23] and IZA's Preference Survey Module [39].

A total of 66 responses were collected over this period, out of which 62 responses were usable for the study[2]. Table 1 shows the sample demographics of the considered responses.

Table 1. Demographic profile of respondents

Communications	**16**
Manager	4
Senior Executive	11
Staff/Technician	1
Defense and Aerospace	**4**
Director	2
Supervisor	2
Entertainment and Media	**1**

(*continued*)

[1] https://www.nsr-org.no/english/category172.html.

[2] We employed Mean Value Replacement, when indicators have less than 10% missing values, and Casewise Deletion, when indicators have more than 10% missing values, as missing value treatment approaches. In this study, we considered "I have insufficient knowledge to answer this question." as missing values.

Table 1. (*continued*)

Manager	1
Financial services	**11**
Director	2
Manager	5
Senior Executive	3
Staff/Technician	1
Industrial and Manufacturing	2
Supervisor	2
Public Sector	**10**
Manager	5
Senior Executive	4
Staff/Technician	1
Retail	**1**
Supervisor	1
Technology and Software	**17**
Consultant	6
Director	3
Manager	2
Senior Executive	4
Staff/Technician	2
Total	**62**

5 Results

To ensure the reliability of the study, we performed the Reliability Analysis to test the internal consistency of related set of questions for each construct. Although Cronbach's alpha is a widely used measurement for internal consistency, it can be easily affected by the number of items in each construct and lead to underestimated results. Hence, we used composite reliability to measure the internal consistency with threshold value of 0.6. Composite reliability is based on factor loadings rather than the correlations observed between the variables.

Convergent validity is another important parameter that refers to the degree which two measures of constructs that theoretically should be related, are in fact related. For convergent validity, the Average Variance Extracted (AVE) of all latent variables should exceed the recommended 0.5 threshold [40].

Table 2 indicates the composite reliability and average variance extracted values of each latent variable. While the values for Perceived Cybersecurity Risk is close to the thresholds, it suggests that the internal consistency and convergent validity of measured variables are acceptable for the study.

After confirming the reliability of the structural model, a complete bootstrapping process was conducted to test the significance of the model at the level of 0.05 confidence interval. We used Bias-Corrected and Accelerated (BCa) bootstrap for estimating nonparametric confidence interval. To ensure the stability of the results, the number of subsamples is 5000. A hypothesis will be accepted only if the test statistics (t-value) is larger than 1.96. Table 3 shows a summary of the hypotheses tests.

Table 2. Composite reliability and average variance extracted values of each latent variable

Latent variable	Composite reliability value	Average variance extracted (AVE)
Cyber attack experience	0.85	0.73
Perceived cybersecurity risk	0.67	0.51
Perceived cybersecurity value	0.94	0.89
Social preferences	0.79	0.58
Willingness to cooperate	0.85	0.73

Table 3. Summary of hypothesis tests

Hypothesis	Original sample (β)	t-Value	Supported?
H1	0.37	2.09	Yes
H2	0.25	1.97	Yes
H3	0.47	4.13	Yes
H4	0.05	0.36	No
H5	0.13	1.59	No
H6	0.30	2.19	Yes

As these results show, Cybersecurity Attack Experience (H1) has a significant positive effect on the Perceived Cybersecurity Value. As for H2, Perceived Cybersecurity Risk has a significant positive effect on Perceived Cybersecurity Value. Cybersecurity Attack Experience (H3) also has a significant positive effect on Willingness to Cooperate. Regarding H4 and H5, Perceived Cybersecurity Value (H4) and Perceived Cybersecurity Risk (H5) have positive effect on Willingness to Cooperate but not statistically significant which suggests that H4 and H5 are rejected. Finally, hypothesis H6 is supported as the results show Social Preferences have significant effect on Willingness to Cooperate.

Finally, to measure the social preferences of the respondents, we used Social Value Orientation (SVO) framework proposed by Murphy et al. [41]. Figure 3 illustrates a graphical representation of the SVO framework.

Figure 4 indicates the ranges within which relevant social preference angles are fallen. These results show that the cooperative behavior among the decision makers in the context of cybersecurity is dominant.

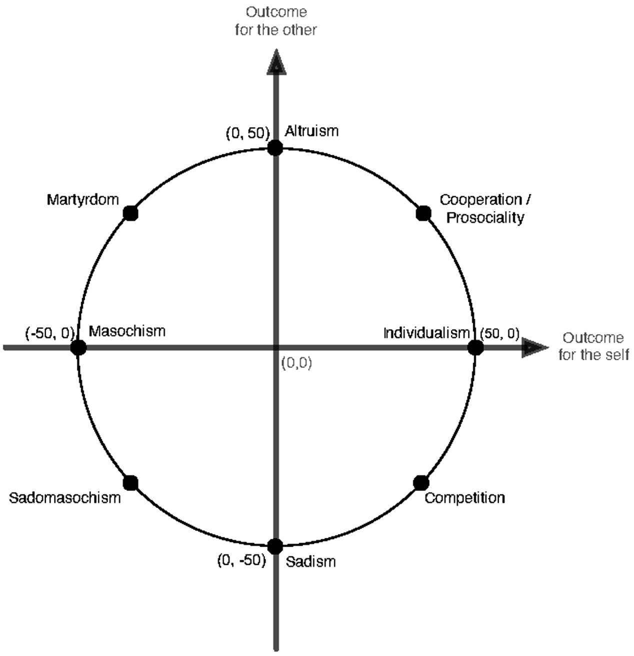


Fig. 3. A graphical representation of Social Value Orientation framework [41].

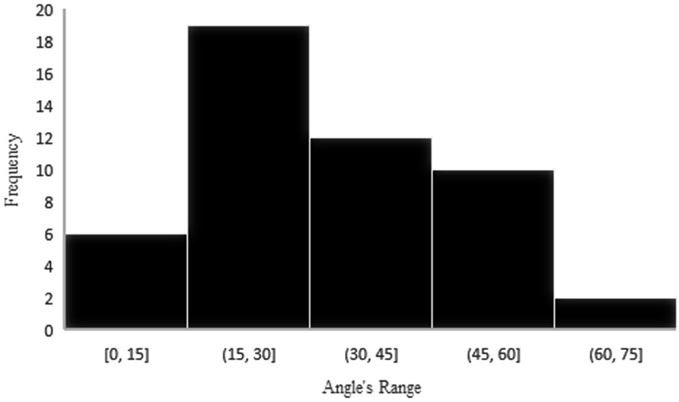


Fig. 4. The ranges of social preference angles

6 Discussion

The significant positive effects of cyber attack experience on willingness to cooperate suggests that organizations that have experienced cyber attacks are more willing to establish or maintain cooperative relationships with other third parties to mitigate the likelihood or impact of future incidents. The consistency between the results of theoretical model and the findings of respondents' social preferences shows that the decision maker's attitude is towards cooperation in the context of cybersecurity.

While the results of this study show that perceived cybersecurity risk and value have positive, but not significant, effects on willingness to cooperate, the related hypotheses are not supported here (hypotheses H4 and H5). A possible explanation is that cybersecurity concerns cause decision makers to delay or ignore cooperation with other organizations. As a result, this lessens their ability to open their network to outside suppliers and third parties.

As for social preferences, the analysis confirms their effective impact on willingness to cooperate. This result suggests that decision makers will reciprocate by adopting positive attitudes to establish or maintain cooperation if other organizations treat them fairly. They even are positive to take retaliatory action against the third parties that cause a cybersecurity incidents or misuse of other organizations' sensitive and confidential information. In this study, a retaliatory action is defined as the discharge, suspension or demotion of a third party, or other adverse business and operational action taken against a third party in the terms and conditions of the contract.

Additionally, the results show that cyber attack experience and perceived cybersecurity risk have significant positive effect on perceived cybersecurity value. However, the mediation analysis of these two variables does not show a significant effect on willingness to cooperate. This outcome can be perfectly explained by the influence of perceived cybersecurity value in opening the door to other third parties.

6.1 Theoretical and Practical Implementation

By testing our research model, this study provides a number of theoretical and practical insights for cybersecurity decision makers to improve their overall cybersecurity posture in their third parties ecosystem. Theoretically, the primary contribution of this study has been to reveal the positive effect of social preferences on the willingness to cooperate among the organizations considering the cybersecurity risks and uncertainties. Previous studies have verified the behavioral models in the context of cybersecurity. This study extends current research and provides evidence that social preferences along with cyber attack experience are essential parts of cooperative willingness.

As the second contribution, this model confirms that perceived cybersecurity risk and value have the strongest impact on the avoidance of cooperation among the organizations. Environmental uncertainties, caused by third parties attacks and weaknesses, and behavioral uncertainty caused by imperfect information or information asymmetry can be two main reasons of this phenomenon. Therefore, our practical implications are mainly directed towards CISOs, but also valuable for other decision makers. To help trusted information sharing, organizations should employ an appropriate, right third party risk management framework based on their structure and business ecosystems. Doing so, they are able to assess the distributed cybersecurity risks in their digital value chain as precise as possible.

7 Conclusions

Cybersecurity decisions are usually not made in a certain, predictable, and isolated environment. Research on the economics of cybersecurity has been largely covered with different perspectives. In this study, we presented a theoretically derived model to explain the impact of social preferences, perceived cybersecurity risk and value, and cyber attack experience on willingness to cooperate in third party ecosystems in the context of cybersecurity. We used variance-based approach of Structural Equation Modeling, so-called Partial Least Square (PLS), to test our research model and analyze the impact of each variable.

The results showed that social preferences and cybersecurity attack experience have significant positive impacts on the willingness to cooperate, and that the dominant preference among the decision makers is towards cooperation and reciprocal behavior. The model also explains that perceived cybersecurity risk and perceived cybersecurity value deter the organizations to cooperate in the context of cybersecurity. The structural equation modeling analysis provides evidence for the small mediating effect of cybersecurity attack experience and perceived cybersecurity risk by perceived cybersecurity value. This highlights the importance of the reduction of victimization and improving the defense controls to enhance the overall cybersecurity posture in the ecosystem.

Our results have some limitations: The composite reliability and average variance extracted values of Perceived Cybersecurity Risk is very close to the thresholds. Future research should overcome this limitation by testing the research model using validated instruments suggested in [42]. The analysis of a single Norwegian organizations sample also limits our results. As Dinev [43] demonstrates the importance of cultural aspects when studying cybersecurity behavior, a more comprehensive picture should be compared between different countries.

Since the results of this study show cooperative behavior among the organization in the context of cybersecurity, it is crucial to understand the forces shaping this cooperation. Moreover, we will investigate the impact of free-riding incentives and externalities of weak cyberdefenses, as the most important problems in cooperation [44], on the overall cybersecurity posture of the ecosystem. Next step of this study is to use the results of this theory to design and develop serious games that help decision makers to understand the cooperation problems and analyze the conditional cooperation and strategic or non-strategic retaliatory actions. The prototype of these games are an extension of CyberAIMs (Cyber Agents' Interactive Modeling and Simulation) [45], a simulation tool for training System and Adversarial Thinking and strategic decision making.

Acknowledgement. We would like to express our special thanks of gratitude to The Norwegian Business and Industry Security Council (NSR) as well as Mr. Adam Szekeres and Mr. EivindKristoffersen Ph.D. Candidates in Information Security, that helped us to design and distribute the survey of this study.

References

1. Bernstein, P.L., Bernstein, P.L.: Against the Gods: The Remarkable Story of Risk. Wiley, New York (1996)
2. Managing Insider Risk Through Training and Culture Report (2016)
3. Kowalski, S.: IT insecurity: a multi-disciplinary inquiry (1996)
4. Øverby, H., Audestad, J.A.: Digital Economics (2018)
5. IT Security: cost-center or strategic investment? (2017)
6. HIPAA Journal: 31,876 Managed Health Services of Indiana Health Plan Members Notified of Impermissible Disclosure of PHINo Title (2019). https://www.hipaajournal.com/31876-managed-health-services-indiana-members-data-breaches/
7. Arghire, I.: New Magecart Group Targets French Ad Agency (2019). https://www.securityweek.com/new-magecart-group-targets-french-ad-agency. Accessed 25 Jan 2019
8. Anderson, R., Moore, T.: The economics of information security. Science (80) (2006)
9. Vishik, C., Sheldon, F., Ott, D.: Economic incentives for cybersecurity: using economics to design technologies ready for deployment. In: Reimer, H., Pohlmann, N., Schneider, W. (eds.) ISSE 2013 Securing Electronic Business Processes, pp. 133–147. Springer, Wiesbaden (2013). https://doi.org/10.1007/978-3-658-03371-2_12
10. Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. (TISSEC) **5**(4), 438–457 (2002)
11. Cartwright, E.: Behavioral Economics. Routledge (2014)
12. Arney, C.: Predictably irrational: the hidden forces that shape our decisions. Math. Comput. Educ. **44**(1), 68 (2010)
13. Thaler, R.H.: Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press, New Haven, London (2008)
14. Kahneman, D., Egan, P.: Thinking, Fast and Slow, vol. 1. Farrar, Straus and Giroux, New York (2011)
15. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. J. Psychol. **91**(1), 93–114 (1975)
16. Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., Vlaev, I.: Influencing behaviour: the mindspace way. J. Econ. Psychol. **33**(1), 264–277 (2012)
17. Briggs, P., Jeske, D., Coventry, L.: Behavior change interventions for cybersecurity. Behav. Change Res. Theor., 115–136 (2017)
18. Fishbein, M., Ajzen, I.: Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research (1977)
19. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)
20. Michie, S., West, R., Campbell, R., Brown, J., Gainforth, H.: ABC of Behaviour Change Theories (ABC of Behavior Change): An Essential Resource for Researchers, Policy Makers and Practitioners. Silverback Publishing (Silverback IS), Croydon (2014)
21. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. **22**(1), 42–75 (2014)
22. Cisco: What Are the Most Common Cyberattacks? (2018). https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. Accessed 25 Nov 2018
23. Ponemon Institute: Data risk in the third-party ecosystem, Ponemon Institute 2016 Research report (2016). http://www.buckleysandler.com
24. Ferraro, K.F., Grange, R.L.: The measurement of fear of crime. Sociol. Inq. **57**(1), 70–97 (1987)

25. Visser, M., Scholte, M., Scheepers, P.: Fear of crime and feelings of unsafety in European countries: macro and micro explanations in cross-national perspective. Sociol. Q. **54**(2), 278–301 (2013)
26. Cybersecurity as a Growth Advantage (2016)
27. Wilde, O., Schmalenbach, W., Leonhardi, A.: Lady Windermere's Fan. Library Editions LLP 4001 (1947)
28. Schwartz, S.H.: Universals in the content and structure of values: theoretical advances and empirical tests in 20 countries. In: Advances in Experimental Social Psychology, vol. 25, pp. 1–65. Elsevier (1992)
29. Sagiv, L., Schwartz, S.H.: Value priorities and subjective well-being: direct relations and congruity effects. Eur. J. Soc. Psychol. **30**(2), 177–198 (2000)
30. Sagiv, L., Sverdlik, N., Schwarz, N.: To compete or to cooperate? Values' impact on perception and action in social dilemma games. Eur. J. Soc. Psychol. **41**(1), 64–77 (2011)
31. Kline, R.B.: Principles and Practice of Structural Equation Modeling. Guilford Publications (2015)
32. Jacoby, J.: Consumer research: a state of the art review. J. Mark., 87–96 (1978)
33. Shugan, S.M.: Marketing science, models, monopoly models, and why we need them. Mark. Sci. **21**(3), 223–228 (2002)
34. Haenlein, M., Kaplan, A.M.: A beginner's guide to partial least squares analysis. Underst. Stat. **3**(4), 283–297 (2004)
35. Henseler, J., Ringle, C.M., Sinkovics, R.R.: The use of partial least squares path modeling in international marketing. In: New Challenges to International Marketing, pp. 277–319. Emerald Group Publishing Limited (2009)
36. Chin, W.W., Newsted, P.R.: Structural equation modeling analysis with small samples using partial least squares. Stat. Strat. Small Sample Res. **1**(1), 307–341 (1999)
37. Fornell, C., Bookstein, F.L.: Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. J. Mark. Res., 440–452 (1982)
38. Becker, J.-M., Ismail, I.R.: Accounting for sampling weights in PLS path modeling: simulations and empirical examples. Eur. Manag. J. **34**(6), 606–617 (2016)
39. Falk, A., Becker, A., Dohmen, T., Huffman, D., Sunde, U.: The preference survey module: a validated instrument for measuring risk, time, and social preferences (2016)
40. Fornell, C., Larcker, D.F.: Evaluating structural equation models with unobservable variables and measurement error. J. Mark. Res. **18**, 39–50 (1981)
41. Murphy, R.O., Ackermann, K.A., Handgraaf, M.: Measuring Social Value Orientation (2011)
42. Featherman, M.S., Pavlou, P.A.: Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum Comput Stud. **59**(4), 451–474 (2003)
43. Dinev, T., Goo, J., Hu, Q., Nam, K.: User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. **19**(4), 391–412 (2009)
44. Bauer, J.M., Van Eeten, M.J.G.: Cybersecurity: stakeholder incentives, externalities, and policy options. Telecomm. Policy **33**(10–11), 706–719 (2009)
45. Zoto, E., Kianpour, M., Kowalski, S.J., Lopez-Rojas, E.A.: A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. Complex Syst. Inf. Model. Q. **18**, 65–75 (2019)

Chapter 8

Research Paper 4: Advancing the Concept of Cybersecurity as a Public Good

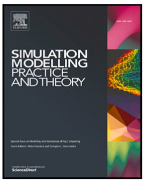
Mazaher Kianpour, Stewart Kowalski, Harald Øverby - Simulation Modeling Practice and Theory, 2022

Simulation Modelling Practice and Theory 116 (2022) 102493

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat



Advancing the concept of cybersecurity as a public good

Mazaher Kianpour [*], Stewart James Kowalski, Harald Øverby

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway

ARTICLE INFO

Keywords:
Cybersecurity economics
Social preferences
Public goods
Agent-based modeling
Collective actions
Heterogeneous preferences
Polycentric governance structure

ABSTRACT

This paper presents an agent-based model of cybersecurity as a participatory public good. Ineffective cybersecurity measures pose serious threats and risks to the development and stability of information societies in the world. Various doctrines and thesis explore how this domain should be treated by the public and private stakeholders. One of these doctrines is cybersecurity as a public good. In this paper, we highlight divergent views about the type of cybersecurity as an economic good. Then, the paper proposes an agent-based simulation model of a repeated public goods game among a set of defenders that are in an uncertain environment with incomplete and imperfect information. In the model, defenders have a probability to choose contribution or being a free-rider, depending on their own preferences and facing with revealed preferences of other defenders. This model implements a utility maximization that applies to each individual, modeling the existence of free-riders, punishments, and interdependency of decisions under a polycentric governance structure. The results of this simulation model show that, over time, defenders update their preferences in reaction to the behavior of other defenders and the experience of cyber-attacks. They indicate a high level of contribution to the provision of cybersecurity as a public good and the effectiveness of decentralized punishment on increasing the contributions. The consistency of the pattern of our results across different empirical studies lends us some reassurance that our model behavior is in quantitative agreement with empirical macro-structures. Furthermore, implementation of a polycentric structure challenges all the relevant agents to take action, and provides more robust environment.

1. Introduction

Evolving malicious cyber activities and increasing cyber risks to individuals, organizations and governments has made cybersecurity a significant challenge and core part of the societal, political and economic decisions [1,2]. The Global Risks Report 2021, published by the World Economic Forum, has categorized cybersecurity failures as the clear and present dangers [3]. This category reveals concern about lives and livelihoods — among them infectious diseases, employment crises, digital inequality and youth disillusionment. Moreover, the increasing value of these assets is becoming more attractive to those who wish to penetrate systems for financial gains, psychological, and reputations gains, or to cause instability. Ensuring cybersecurity through greater awareness and strong multi-stakeholders partnership are crucial for achieving Sustainable Development Goals in a hyper-connected world and societies that rely on digital infrastructure [4]. These features make cybersecurity a global issue that knows no boundaries. Hence, investment in cybersecurity and how this domain should be treated by the public and private sectors has been at issue over the course of the last decade. It also has been controversial if we can avert the tragedy of commons within the context of cybersecurity [5,6].

[*] Corresponding author.
E-mail addresses: mazaher.kianpour@ntnu.no (M. Kianpour), stewart.kowalski@ntnu.no (S.J. Kowalski), haraldov@ntnu.no (H. Øverby).

https://doi.org/10.1016/j.simpat.2022.102493
Received 27 July 2021; Received in revised form 22 October 2021; Accepted 6 January 2022
Available online 19 January 2022

Cybersecurity covers a vast domain that includes designing and development of robust systems against attacks, deployment of methods to detect anomalies and guarantee the system's resilience, and defining response and recovery mechanisms to attacks. Every aspect of cybersecurity is involved in achieving secure, safe, and dependable systems from initial security requirements specification and threat assessment to the provision of all required protective mechanisms, product selections and system security testing. In 2011, Mulligan and Schneider proposed to frame and manage cybersecurity as a public good [7]. While Mulligan doctrine demonstrates rational, defensible and legitimate arguments, it has not gone beyond an acknowledgment that the benefits of cybersecurity are to some degree non-rivalrous and non-excludable. They have not explored the aspects of both cybersecurity and public goods that contribute on efficiency and effectiveness of cybersecurity provision. On the basis of a general interpretation of the theory of public goods, developed by Samuelson, the notion of cybersecurity as a public good aims to reaffirm a collective responsibility to develop cybersecurity and manage cyber-insecurity. This perspective would create the much-needed overarching policy principle to define objectives and means, to bring cohesion to sectoral and specific, purpose-led policies and programs [8]. The leading role of the governments in cybersecurity policies, processes and practices is however increasingly being questioned, largely as a result of the changing dynamics in the global cybersecurity landscape. This is characterized by the increasing involvement of non-state actors in cybersecurity policy and provision, and interconnected trends that result in a dramatic shift in how cybersecurity is managed.

This work is an extension our earlier work in [9] where we focused on heterogeneous preferences and contribution pattern of agents in providing cybersecurity as a public good. In this study, we are not trying to provide normative justification for governments to invest more heavily in cybersecurity as a public good. Conversely, we aim to investigate whether this idea matches the existing theories and how this doctrine affects the resilience of such dynamic and uncertain environments like digital ecosystems. The purpose of our study is two-fold: (i) to construct an agent-based model that captures the main elements of public goods theory (i.e. free-riders problem, effectiveness of punishment, and collective action) and investigate whether it complies with the unique characteristics of cybersecurity (i.e. dynamic and uncertain environment with incomplete and imperfect information, and difficulty in assessing the cybersecurity value and cyber risks), and (ii) to characterize and study the cybersecurity posture under different settings where agents contribute to provide security measures that their benefits are not excludable and rivalrous. We look at how agent-based modeling (ABM) can contribute to exploring macro outcomes of collective contributions of agents to provide cybersecurity as a public good while considering the heterogeneous social preferences of agents. Introduction of social preferences into this model provides us with a better understanding how agents behavior deviates them from the standard model of utility maximization.

We summarize our main contributions of this work as follows:

- Problem formulation: To our best knowledge, this is the first work that quantitatively addresses cybersecurity provision problem from the perspective of public goods theory. In particular, we model and simulate the heterogeneous preferences and patterns of contribution in cybersecurity as a public good.
- Provision mechanism design: We implement a polycentric governance structure to describe a process of decision making where multiple independent actors interact to produce an outcome that is commonly valued. Our scheme can incentivize the agents to participate in the mechanism, and can achieve several desirable security properties such as enhanced cybersecurity posture in the environment and budget balanced.
- The characterization and exploration the impact of different parameters on the agents' evolving strategies and cybersecurity posture when cybersecurity is treated as a public good.

This paper proceeds first by reviewing the types of economic goods and outlines the aspects of cybersecurity that are suggested to be treated as a public good in Section 2. Section 3 discusses how the notion of cybersecurity as a public good has developed over time. We present our basic model and simulation in Section 4. Section 5 demonstrates the results of the simulation and discusses the issues of sensitivity analysis and validation. In Section 6, we discuss the findings and compile several practical implications for promoting cybersecurity as a public good. The paper is concluded in Section 7 with suggestions for future work.

2. Background

To avoid vagueness regarding what cybersecurity entails, we use the definition suggested by [10]: the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users. However, it seems difficult to discuss whether cybersecurity is public or not without first knowing whether it is a good at all. According to economic principles, a good is an object or service that satisfies human wants and provides utility [11]. That is to say, agents value a good and are willing to pay for it. An individual, organization, or a government values cybersecurity and pays for it because they expect their utility increase by utilizing it. They do not pay for cybersecurity per se. They might be willing to pay more for products or services that are provided with top ranked companies and vendors. Rosenzweig argues that cybersecurity is not a singular good. Rather it is a bundle of various goods, some of which operate independently and others of which act only in combination [12].

In 1954, Samuelsen defines public goods as non-rival and non-excludable goods when consumed [13]. The former implies that once the good is produced, it can be consumed by other consumers at no additional cost. The latter, however, is sometimes added and specifies that consumers cannot be excluded from consumption of the good once produced. The classic understanding of a public good based on Samuelson's taxonomy has been much debated and modified over time. Galbraith suggests that public goods are things that do not lend themselves to market production, purchase, and sale. They must be provided for everyone if they are

Table 1
Typology of Economic Goods.

	Rivalrous	Non-rivalrous
Excludable	Private goods *(Cars, apples)*	Club goods *(museum, cable television network)*
Non-excludable	Common Goods *(oil well, national forest)*	Public goods *(national defense, country's financial stability)*

to be provided for anyone, and they must be paid for collectively or they cannot be had at all [14]. However, since Samuelson's definition of types of economic goods has been the base of all discussions on cybersecurity as a public good, this study also relies on this definition. Using rivalrous and excludable characteristics, economic goods can be categorized into four main types. Table 1 shows the typology of economic goods and two examples of each type.

According to the typology represented in Table 1, many security systems such as anti-virus software, intrusion prevention systems, and network firewalls are private goods. However, there are other aspects of cybersecurity, such as threat intelligence and vulnerability information sharing, collective response to cyber-attacks, integrity of elections, and critical infrastructure protection, that have the characteristics of public goods [15]. Goods with the characteristics of public goods are often produced with some form of public assistance (e.g. taxation or other mandates). Accurate production and provision of these goods compared to the level that would be best for society is the main challenge of policy makers. Consumption of a public good by an end-user does not necessarily have to be free of charge, however, it is essential that its costs do not become a discriminating factor, and consequently, determining access and use of it. Some public goods are best created by direct government provisioning, while other may be best created by the all beneficiaries as a participatory public good. Participatory public goods are created best by changing individuals and organizations' incentives through different policies and regulations. For example, there are many reasons (e.g., risk of loss of reputation and trust, liability, negative effects on financial markets, and signals of weakness to adversaries [16]) that why an organization may be reluctant to share information threats and vulnerabilities in its systems. Treating such information as a public good tends to overcome these issues.

It is necessary to consider economic goods not only in their original forms, but also as social constructs and as a result of deliberative policy choices [17]. According to Hagedorn [18] and Kaul [19], with the evolution of social institutions, many goods have developed into mixed types, showing both exclusive and non-exclusive characteristics, since they might change as a result of new technologies, or different policies and regulations that are implemented. Kaul and Mendoza proposed a conceptual framework to evaluate the publicness of the goods according to this perspective [19]. Their framework examines goods according to three criteria.

- Publicness of decision-making is used to assess the participatory nature of the processes (e.g. how to distribute the benefits among the consumers) and decisions (e.g. the level and quality of production) related to the provision of the good.
- Publicness of distribution of benefits is used to assess the equity of benefits from the public goods.
- Publicness of consumption represents the non-exclusiveness across consumers.

While this framework shows an ideal situation and usually goods do not fully meet all the three criteria, it helps policymakers and the public to understand the issues to be addressed through policy tools, institutional changes and new governance settings. Other frameworks have been used to conceptualize and understand the public goods. However, features such as multi-dimensionality, multi-agent and context-dependent processes, uncertainty, and evolution, makes treating cybersecurity as a public good a special topic in public goods economics. Therefore, this study adds to the literature by further extending focus from descriptive discussions to quantitative analysis using an agent-based model.

3. State of the art

The necessity for public–private collaboration, multifaceted strategies, and recognition of the significant role that industry plays in securing the information networks have been the fundamental notions of approaches to cybersecurity in the past decade [20,21]. However, with the raise of dependencies on critical infrastructures and increasing concerns about the consequences of possible cyber–physical incidents, many governments and super-national organizations like European Union (EU) are concerned with the possible failure of the private sector in delivering acceptable level of security in the society without governmental intervention [22,23]. This shift of the concept has lead to the proposals which suggest that cybersecurity needs to be treated as a public good.

Taddeo argues that considering cybersecurity as a public good will be a step in the right direction to support policy and governance approaches that will foster robust, open, pluralistic, and stable information societies [24]. She elaborates managing cybersecurity as a public good brings the advantages of systemic approaches to security, shared responsibilities among different stakeholders; and facilitation of collaboration. Asllani et al. also explores the role of establishing an appropriate legal, social, and ethical framework to enhance cybersecurity [25]. The authors compare the cybersecurity with safety and conclude that financing of cybersecurity by taxes justifies the significant role of governments in enhancing cybersecurity. Comparison of cybersecurity with other public goods is not limited to public safety and other researchers also compared it with public health. Sedenberg and Mulligan evaluated different cybersecurity information sharing proposals leaning on the analogous public good-oriented field of public health, and proposed some recommendations to orient cybersecurity policies towards adopting the doctrine of public cybersecurity [26].

The studies by McCarthy [27], Assaf [28], and Shore et al. [29] also discuss that cybersecurity appears to have the character of a public good. These studies question rational choice approaches and classic solutions that suggest public goods should be provided by the governments to avoid market failures. However, the incapability of the governments in providing the public good of cybersecurity on their own is also supported by [30]. Hence, they propose solutions based on public–private partnerships to overcome the problems of treating cybersecurity as a public good. The effectiveness of these solutions has been the focus of analyses such as [31–33]. The concern of these analyses is determining institutional forms, policy processes, and levels of government intervention through which partnerships can most effectively provide cybersecurity. Drawing from this interdisciplinary literature, Shackelford used the concept of polycentric governance to describe how cybersecurity as a public good should be regulated [34].

Reviewing the literature shows that there are different arguments favoring treating cybersecurity as a public good. There are also several studies that have incorporated this perspective in their game-theoretical analyses that capture essential characteristics of decision-making to protect assets withing an environment. Bauer and Eeten argue that cybersecurity has strong public good characteristics, although it is mostly provided by private stakeholders at a cost [35]. Varian's exposition supports this argument. Varian observed that the success of reliability (as a critical component of security) decision-making depends on joint protection by all the agents in a network [36]. Moreover, he posits that the computation of the protection level will often take the form of a public good contribution function with non-excludable and non-rival benefits or consequences. As a result, individuals may be able to free-ride on others' efforts or suffer from inadequate protection efforts by those members that have a decisive impact on the overall protection level in the environment.

Grossklags et al. continue Varian's work by adding another action available to the individuals. They can decide to self-insure themselves from harm. Consequently, the security games developed by Grossklags et al. consider share qualities of private (on the insurance side) and public (on the protection side) goods [37]. Johnson et al. extend these security games by modeling network security investments that account for the choice between the hybrid goods of collective protection and individual mitigation and externally provided market insurance. Their study shows that several equilibria with full market insurance exist and, consequently, market insurance has a place in security games [38].

Unlike [37,38], this work assumes only public components have a constant marginal impact across the range of investment opportunities. Therefore, in this study, individual agents decide strategically on how their security investment reduces the probability mass in the loss distribution function of all agents. Furthermore, their works look at homogeneous population of fully rational agents with perfect information. Therefore, our work adds to the research literature by (1) considering heterogeneous population of agents, where every agent has different utility function, (2) exploring the impact of decentralized punishment under a polycentric governance structure, and (3) featuring bounded rationality under uncertainty concepts.

However, the public goods theory plays a relatively minor role in both cybersecurity policy and practices. Although appraisal of these arguments are beyond the scope of this research, we attempt to quantitatively analyze whether the context of cybersecurity complies with this theory, and employing this theory maintains the robustness and resilience of such dynamic and stochastic environment in presence of various externalities. In the next section, we develop a model that addresses the interdependence among the agents and captures the impact of social preferences and punishment on their average contribution to enhance their cybersecurity posture. Cybersecurity posture is used to describe the cybersecurity capabilities of a country, organization or business and collective efforts to protect their assets. It refers to the overall defense mechanisms in place to tackle malicious cyber activities. This metric relates to any kind of security measure, including policies, staff training, and intrusion prevention systems. In this model, we assess the cybersecurity posture of the organizations by the number of failed attacks against them and their resources after each period.

4. Model

This section presents our agent-based model (ABM). ABM is a class of computational models that can simulate a complex macro-level system (e.g., digital ecosystem) based on formally assumed simple behavioral rules of individual agents (e.g., people, organizations, or governments), learning algorithms, and evolutionary settings. By simulating micro-level agents' behavioral processes (e.g., organizations' willingness to contribute) and interactions with each other (e.g., punishing free-riders), it allows the detection of macro-level pattern variations (e.g., cybersecurity posture) caused by individual agents' behavioral changes, which is hardly observable using traditional analytical models. ABM shows advantages in revealing the hidden causal mechanisms driving the macro-level developments in complex systems like digital ecosystems [39].

Digital ecosystems are highly complex socio-technical systems, in which autonomous and heterogeneous decision-making entities, hereafter called agents, operate, interact, and evolve. When some of the problems in such systems resolved with traditional analytical models, the multifaceted realities are largely simplified to build theories with generalizability at the expense of accuracy [39]. The unrealistic assumptions (e.g., homogeneity, linearity, and equilibrium) often fail to gauge the complex behavioral patterns [40]. ABM instead allows agents to be heterogeneous in behavioral patterns, make boundedly rational decisions based on imperfect information (collected or interpreted), perform evaluations based on interactions with each other and the environment, and adapt based on their experiences and environmental changes [41]. ABM is thereby a well-suited tool for identifying causal mechanisms of change in the security or in-security of the digital ecosystems where agents do not act out fully rational. ABM can be employed to produce an accurate prediction of future system patterns [42]. It functions as an explanatory tool when empirical data is unavailable. It enables the researchers to conduct experiments with possible scenarios simulated and compare their outcomes to identify reasonable explanations and propose theoretical advances, without having to be anchored to existing empirical evidence [43]. The rest of this section, describes our underlying model. Table 2 shows the list of notations used to describe this model.

Table 2
The list of notations used in the model.

Notations	Meaning
g_i	Monetary gain of the defender i
c_i	Contribution of defender i to provide cybersecurity
γ_j	The cost incurred by the punisher j
λ_i	Penalty of punishing i
R	Resource of agents
c_i	Contribution of i
p_{ij}	Probability of punishing j by i
p_{ji}	Probability of punishing i by j
Defenders	All the agents that belong to the defense group
defender	An agent that is a Defender
Attackers	All the agents that belong to the offense group
attacker	An agent that is an Attacker
W/O punishment	Without punishment
W/ punishment	With punishment

4.1. The basic model

The classical setting of a Public Goods Game (PGG) models an economic or social group of n agents, termed Defenders, whose strategies include either Contribute or Defect. If an agent contributes, she invests a quantity c into the public pool whereas defectors do not contribute anything. In our study, we add another group of m agents, termed Attackers, whose strategy is to attack one or more of the Defenders to gain financial benefits. The attackers target one of the Defenders and conduct an attack. The Defenders prevent or minimize the risk of these cyber-attacks by employing security measures (SM). Security measures may include: physical access controls, staff training, encryption technologies, and architectural approaches, among others.

In our model, each of the defenders has an initial resource of $R > 0$, expressed in monetary units. The organizations simultaneously decide on their respective contributions $c_i \geq 0$ to invest on SM as participatory public goods. The total contributions towards the cybersecurity provision using these measures is $C = \sum_{i=1}^{n} c_i$. The monetary gain of the defender $i \in n$ is given by

$$g_i = \begin{cases} R - c_i + ROSI & W/O\ punishment \\ R - c_i + ROSI - \gamma_j p_{ij} - \lambda_i p_{ji} & W/\ punishment \end{cases} \tag{1}$$

where ROSI is the return on security investment by all contributor agents arising from implementation of security measures. In the public goods theory literature, this private benefit is called the marginal per capita return (MPCR). In a standard PGG, the contributions of agents are multiplied by an enhancement factor. This amount is then equally distributed among all the agents of the PGG regardless of their contributions. In our model, however, we calculate this variable as follows:

$$ROSI = \frac{ALE - (ALE \times (1 - RM)) - AC_{SM}}{AC_{SM}} \tag{2}$$

where ALE, RM and AC$_{SM}$ are the annual loss expectancy, mitigated risk by implementation of the security measure, and the annual cost of deployment and maintenance of the security measure, respectively. On the other side, the return on the conducted attack for the attackers will be calculated by:

$$ROA = \frac{EMG - (EMG \times RM) - Cost_{att}}{Cost_{att}} \tag{3}$$

where EMG and $Cost_{att}$ are the expected monetary gain and cost of the conducted attack, respectively. ROSI and ROA are computed by using quantitative indexes and defense/attack trees presented in [44]. When the computation of ROSI and ROA is complete, the agents have two options; selecting security measures that maximize ROSI or minimize ROA. The first thing that the agents can do is to eliminate, if any, sets with negative value of ROSI as they do not represent profitable investments. Then, some of the agents can invest in security measures that maximize ROSI, while some of them can invest in measures that minimize ROA. The agents evaluate effectiveness and profitability of measures as well as their deterrent effect on attackers. According to the result of this evaluation, they can change their strategy.

Eq. (1) shows two expressions to calculate the gain of Defenders: with punishment (w/ punishment) and without punishment (w/o punishment). In case of punishment, the contributors are allowed to punish the non-contributors (i.e. free-riders). The punishers incur certain costs (γ) to perform the punishment, and subsequently, they impose a penalty (λ) on the agents who are punished. Since punishment incurs expenses on both sides, it is likely that contributors ignore punishment considering the cost of punishment and their social preferences. The attackers play an important role in inducing more contributors as experience of attack increases the willingness to cooperation among the defenders [45].

As [45] argued, social preferences models with risk aversion may break down into two main elements of self-regarding and other-regarding preferences. With this in mind, we express our utility function as below:

$$\pi_i(g_i, g_j) = g_i - \alpha_i\ max[g_j - g_i, 0] - \beta_i\ max[g_i - g_j, 0] \tag{4}$$

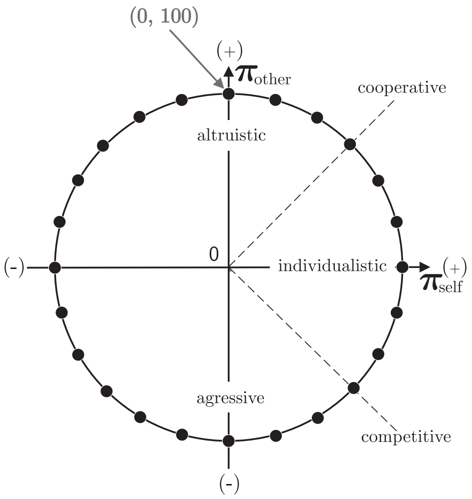


Fig. 1. Social orientation value ring is used to illustrate how individuals weigh their own payoffs vs. the payoffs of one or more others.

where α_i and β_i represent the constant elasticity of substitution in this function to exhibit the elasticity of the ratio of other-regarding preferences and individualism, respectively. Fig. 1 depicts these two elements. In our model $-100 \le \alpha_i \le 100$ and $0 \le \beta_i \le 100$. We have considered two possible types of other-regarding preferences which exhibit altruism and envy (aggressive). Defenders are initially endowed with certain values for α and β, but these values can change through the time. While the Defenders act to maximize their utility, it is the prevalence of their preferences (i.e. internal norms) that determines the social norm in the long-term. The literature shows that different social norms generate multiple equilibria within the environment [46,47]. It also shows that the norms evolve over time, according to the actual contribution of the individuals [48,49].

The static equilibrium of this game, when all the quantities have unchanging values and organizations are self-regarded, is zero contributions ($\forall i \in n : c_i = 0$). In this case, the Defenders fail to provide cybersecurity. Furthermore, [50] shows that the social optimum will be achieved under $\forall i \in n : c_i = R$. However, in the presence of externalities and other preferences included as a part of our study and the context of cybersecurity, these fundamental theorems do not hold. In an evolutionary context, agents are not considered fully rational [51]. Therefore, they do not necessarily act a Nash equilibrium found from rational analysis. Agents are allowed to change their strategy after each round of the game. In our model, the evolution of strategies follow certain evolutionary rules, in which agents evaluate their payoffs comparing their fitness with those of the rest of the population. In this model, we assume that the Defenders report their amount of contributions after each round. Therefore, the Defenders can infer the percentage of contributors and free-riders. The level of free-riding influences the Defenders' probability of contribution in the next round. Therefore, Defender i compares her payoff of the last two rounds (the recency-biased is 1). The probability that i contributes in round $t+1$ obeys a saturated Fermi function of the payoff difference, and is calculated as follows

$$Prob(contribution) = \frac{1}{1 + e^{\frac{\pi_i^t - \pi_i^{t-1}}{k}}} \tag{5}$$

where k is the percentage of free-riders in the population. This means that although the probability of contribution is a function of changes in the agents' utility, it is also based on the level of contributions observed in the environment in the current round. When $k = 0$ (i.e., there is no free-rider), the agents keep their strategy, with probability 1, in round $t+1$ since it has a better payoff. If $k \to \infty$ (i.e., all the Defenders are free-riders), the Defenders update their strategies with probability of $1/2$, regardless of the payoff difference. The agents do not know the contribution probability of other agents but can infer the amount of contribution in each round. k has been considered fixed in the literature of evolutionary public good games for simplicity. However, we relate this variable to the dynamic percentage of free-riders to characterize the stochastic uncertainties in the game dynamics an incorporate interdependencies and reciprocity in our model.

The free-riding problem, in which a self-interested defender seeks to free ride on other's contribution, is likely to exist in any collective action. In this model, we implement a decentralized punishment strategy by contributors to explore the effectiveness of this strategy in maintaining, or perhaps increasing, the average level of contribution by the Defenders. Experimental studies show the importance of decentralized punishment (i.e. punishments are carried out without the intervention of a central authority by the individuals) in promoting the cooperation among the agents [52–54]. Therefore, the contributors can target those who defect. Eq. (6) gives the probability of punishing j by i if the contribution of i is more than a defined threshold. The punishment would be carried out by i if $p_{ij} = 1$.

$$p_{ij} = min\{\frac{|arctan(\beta, \alpha)|\ \lambda_j - \gamma_i}{2\gamma_i}, 1\} \tag{6}$$

Agent i chooses one of the free-riders proportionally to their payoff. In our model, this obeys from the Moran rule where probability of choosing agent j is given by

$$Prob(punishing\ j) = \frac{\pi_j}{\sum_{l=1}^{N} \pi_l} \tag{7}$$

This rule uses the global knowledge about the payoffs of the Defenders. It should be noted that both Fermi and Moran rules are purely stochastic when describing the probabilistic dynamics in a finite population of constant size N.

Assuming that the preferences of all the agents are separable, Dufwenberg proposes a general equilibrium for the conditions that other-regarding preferences exist in the market, particularly if it is competitive [55]. Another promising solution to efficiently provide the public good is the implementation of Lindahl equilibrium, which achieves optimum social welfare for the public good economy at a Nash equilibrium. The existing Nash implementation literature involves several mechanisms with desirable economic properties such as integration of static and dynamic settings and budget balance [56–58]. However, there are two unaddressed issues in the literature of equilibrium implementation for public good provision. First, the existing approaches cannot perfectly incentivize agents to contribute in the process of public goods provision. Therefore, the free-riding problem cannot completely be avoided [59]. Second, for the constrained public good provision problem (i.e., the principle that agents face with some constraints such as constitutional or legislative, for a public good provision mechanism to be implemented), there does not exist an agent adaptation policy that is guaranteed to converge to the equilibrium. This motivates us to propose a polycentric governance structure with a proper economic mechanism to resolve these two issues. The basic idea of polycentric governance is that any group facing some collective problem should be able to address that problem in whatever way they best see fit [60]. We implement our model under this structure because (1) the polycentric structure recognizes that diverse organizations and governments operating in a multi-level environment can create policies to increase cooperation and compliance levels by enhancements of flexibility and adaptability over time, and (2) it contributes to the solution of free-rider problem since a central governance unit is often incapable of managing collective action problems such as efficient response to cyber attacks.

4.2. Agent-based simulation

The agent-based simulation presented in this paper implements the impact of an agent's social preferences on the decision to cooperate or not cooperate in the provision of cybersecurity as a participatory public good (i.e., requires the beneficiaries to contribute in provision of the good). Thus, we implement our model as a polycentric governance structure to describe a process of decision making where multiple independent actors interact to produce an outcome that is commonly valued [61]. The outcome is protection of their resources and mitigation of the consequence of attacks by implementing the security measures with specific cost and applications. In case of an attack, if the measure is implemented adequately, the attack fails and at the end of the period, the calculated ROSI is shared equally among all the defenders. Otherwise, the impact of the conducted attack will reduce the attack target's resource and add to the attacker's resource.

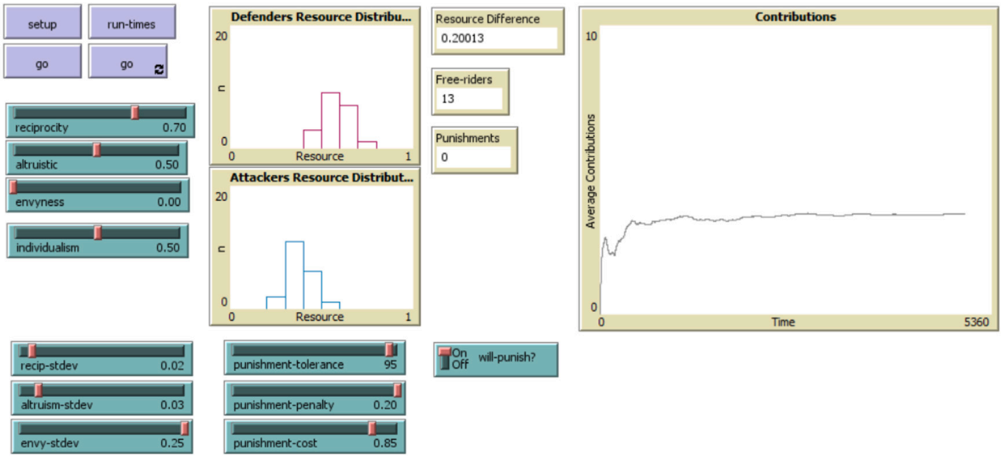
Four cyber attacks with different levels of impact may occur in each round. The impacts and costs of these attacks are extracted from the Ninth Annual Cost of Cybercrime Study by Accenture and Ponemon Institute [62]. This study reports findings of field research conducted over several months across 11 countries in 16 industries. The findings give us good insights into the economic impact of cyber-attacks and benchmarking cybersecurity investments. The information that we extracted from this study includes the total cost by attack type and the core process-related activities that drive a range of expenditures to implement cybersecurity measures.

The Attackers have no information regarding the implemented measures and Defenders. However, Defenders have the information regarding the contributions of other defenders. Accordingly, to store this information and introduce the reciprocity behavior into the model, all the defenders have their own memory which stores the attacks that have occurred to them, the defenders that they have punished and the defenders that were punished by. To address the problem of recency bias [63], the model assumes that the players outweigh the experience of the most recent round compared to the previously played rounds. This study does not explore the impact of variable recency bias and memory length of the agents.

The model is written in NetLogo 6.1.1 and each tick of the simulation represents one day. The simulation period is 365 steps (equivalent to one year). The probability of cooperation for each defender in each period is based on personal motivation, level of resource, and experience. The defenders do not know the contribution probability of the other defenders and the attack likelihood, however, they are able to observe if any contribution is made or if any attack has occurred. Thus, the game is implemented with incomplete and imperfect information among the agents.

The following occurs in each tick of the simulated process:

1. Decisions and Actions: Each defender decides whether to contribute or defect, according to their probability of contribution (Eq. (5)). The Defenders who decide to punish another agent carry out the punishment. Each attacker selects a target according to their resources and costs of the attack, and conducts the attack against the selected target. The impact of these attacks can be mitigated by the security measures that the Defenders can implement through their collective action.
2. Payout Distribution: Each agent get the payout from their decision. The Defenders get the payout from their collective action and the attack (those who have been targeted). The Attackers get the payout of the attack, whether it has been a success or failure.
3. Updating Strategies: Depending on the cooperation levels within the Defenders and the received payouts, each defender updates their probability of contribution and punishment according to Eqs. (5)–(7).



reciprocity 0.70
altruistic 0.50
envyness 0.00
individualism 0.50
Resource Difference 0.20013
Free-riders 13
Punishments 0
recip-stdev 0.02
altruism-stdev 0.03
envy-stdev 0.25
punishment-tolerance 95
punishment-penalty 0.20
punishment-cost 0.85
On Off will-punish?

Fig. 2. A Screenshot of the agent-based model implemented in NetLogo 6.1.1.

Table 3
Parameter values for the attacks.

Attack	Probability of Attack	Attack Cost (×10^3\$)	Attack Impact (×10^6\$)
A1: Malware	0.25	50	2.6
A2: Web-based attacks	0.20	60	2.3
A3: Denial of service	0.20	70	1.7
A4: Malicious insider	0.15	65	1.6

Table 4
Parameter values for security measures.

Security Measures	Security Investment (×10^3\$)	Annual Cost (×10^3\$)	RM_{A1}	RM_{A2}	RM_{A3}	RM_{A4}
CM1: Security intelligence and threat sharing	100	25	0.6	0.5	0.4	0.5
CM2: Advanced identity and access management	80	30	0.4	0.6	0.4	0.6
CM3: Cyber and user behavior analytics	110	30	0.5	0.5	0.4	0.6
CM4: Cryptography technologies	100	5	0.4	0.5	0.3	0.4
CM5: Automated policy management	80	45	0.5	0.4	0.3	0.5
CM6: Enterprise governance, risk, and compliance	300	50	0.5	0.5	0.4	0.5

Fig. 2 shows the user interface of the implemented simulation which enables us to change the mean values of social preferences of the Defenders. The values that is assigned to each agent can be dispersed by using the standard deviation sliders. This interface also shows the distribution of resource among the Defenders and Attackers. This distribution changes over time due to successful or failed cyber-attacks, investment on security measures, and return on security investment. The number of free-riders and the spending on the punishment is also among the outputs that this interface shows. Tables 3 and 4 show the values for input parameters of cyber attacks and security measures, respectively.

5. Results

This section presents the results from the agent-based simulation. The results show that the model replicates the general features of public goods theory and presents the outcomes of the players decision in the game focusing on their social preferences. First, we look at pure social preferences (Reciprocity Ratio = 0) with and without punishment. Fig. 3 shows the average contributions made by the defenders to protect their environment and maintain their robustness in 15 years (5500 ticks). The figure shows that punishment dramatically promotes contribution. It also shows that altruistic preferences increases over time whereas the individual and aggressive preferences reach a constant level of contribution after the first five periods of the simulation.

Reciprocity affects the choice of those who choose later. Figs. 4 and 5 show the results of simulation run in cooperative and competitive modes, respectively, with different reciprocity ratio. As we observe, the possibility of punishment alters the results in both modes. In cooperative mode with punishment, increase in reciprocal behavior increases the average contribution. In contrast, without punishment, increase in reciprocal behavior decreases the contributions among the defenders. The reason of this phenomenon is inequity aversion which is described in [64,65].

Inequity aversion is the preference for fairness and resistance to incidental inequalities. With higher reciprocity ratio, defenders care more about interpersonal comparisons of their own payoff and the payoffs of others. Therefore, increase in contribution of

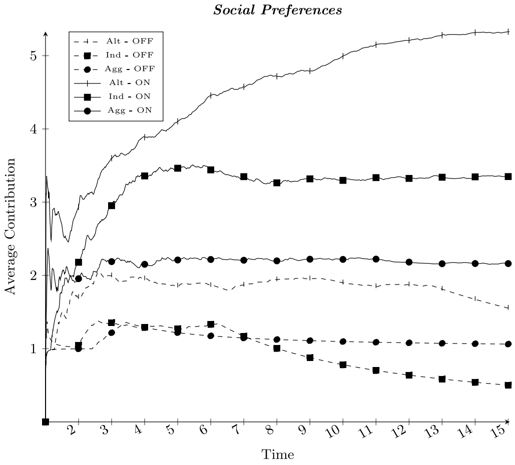


Fig. 3. Social Preferences with punishment (ON) and without punishment (OFF).

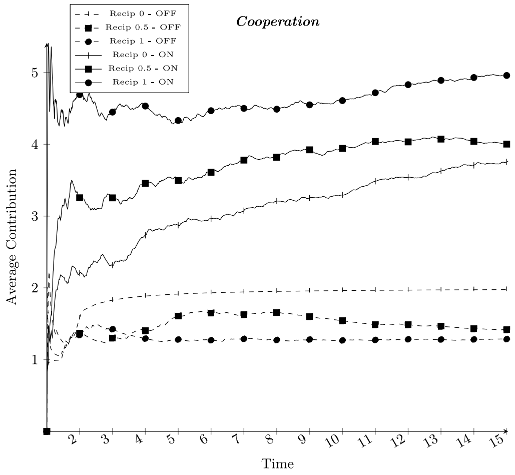


Fig. 4. Cooperation with punishment (ON) and without punishment (OFF).

others motivates an agent to contribute more, and vice-versa. Moreover, the results show that despite the heterogeneous preferences among the agents, the fluctuation in contributions occur in the first 6 decision periods, then, Defenders settle onto a homogeneous behavior to contribute in provision of cybersecurity and maintain the resiliency of the environment. To put it more generally, we observe that in a dynamic and stochastic environment, logic at the level of the system cannot be easily inferred from logic at the level of the agents.

From the pattern in Fig. 6, we can see that the cooperative defenders gain and protect more resources by contribution in the deployment of security measures. On the contrary, individualistic behavior cannot protect the defenders' resources, as a result, the advantages of contribution would be further strengthened. By analogy, with changing the behavior from individualistic to other-regarding preferences, the Defenders get resistance against the attacks impacts. Thereby, the environment will form a dominant strategy which will promote the cooperation efficiently.

From a theoretical perspective, it is important to explore whether decaying contributions converge to the free-riding level (i.e., Nash Equilibrium). However, determining the range of contributions in final decision periods is a difficult task and there are no experimental research, to our best knowledge, that have conducted public goods game similar to our game design (i.e., conditional cooperation with repetition and dynamic marginal per capital return and the presence of exogenous factors such as cyber-attacks that might change individual behavior). Hence, we cannot explore the degree of corroboration between our simulations and empirical experiments. Nevertheless, we refer to two significant experimental studies by Ledyard [66] and Fischbacher et al. [67] due to their substantial number of experiments conducted on public goods in the former and incorporation of social preferences in the latter.

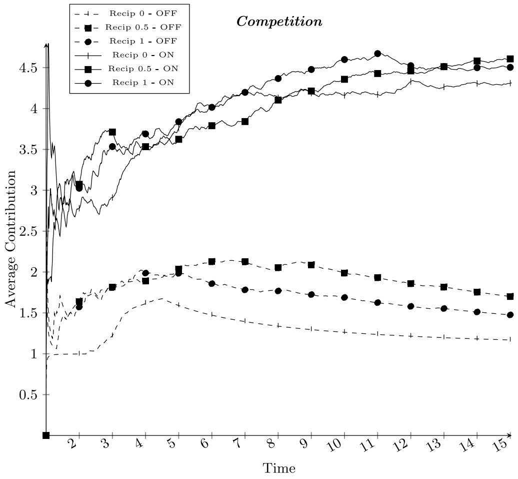


Fig. 5. Competition with punishment (ON) and without punishment (OFF).

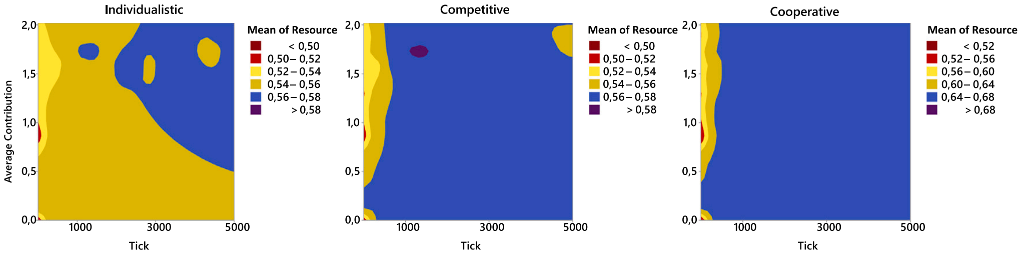


Fig. 6. The distribution of the agents' resource level in three different behavior. All results are obtained for $N = 20, \gamma = 2, \lambda = 3$. Increasing the average resource shows that deployment of the security measures has been successful in mitigation of the attacks impacts. We found the same pattern of change as the cost and penalty of punishment increased.

While Ledyard shows that final period contributions may be as low as 4% and as high as 37%, Fischbacher et al. report the range from 10% to 15% of the endowment. Fig. 7 shows the probability distribution of contributions (average of the final 5 decision periods in 100 simulation runs) for $N = 20$. About 25% of the Defenders have contributions of 10% or less above the free-riding level. Almost 75% of them between 10% to 30%, and the contribution of 5% of the Defenders reaches more than 30% of the free-riding level. We conducted sensitivity analysis on the number of Defenders and repeated the simulation for $N = 4$. The results show more contributions than group size $N = 20$. Therefore, the results indicate that contributions do not reach the free-riding level and most of the Defenders have contributions between 5% and 15% above free-riding level.

5.1. Sensitivity analysis

Sensitivity analysis (parameter variability) technique consists of changing the values of the inputs and parameters of a model to determine the effect upon the model's behavior or output. We used the quantitative approach to investigate both direction and magnitudes of the outputs. The outputs that we examined in this study are the number of free-riders, the spending on punishments by contributors, and change of preferences through the time. Fig. 8 show the result of our analysis on the number of free-riders in cooperative mode, with and without punishment. As this figure shows, the number of free-riders increases with the increase in reciprocity ratio if contributors do not punish the non-contributors. We observed the same trend in competition mode. As we pointed out earlier, this shows the change of preferences in this highly interdependent and dynamic environment.

We further investigated the punishment behavior in detail. Fig. 9 shows the average amount that contributors spend on punishment over 15 periods. This is the average amount of 100 runs of the simulation. In all conditions, the differences between the amount of punishment is not significant. This indicates that punishment functions to facilitate contribution. However, this tendency was weaker for individualistic Defenders. We derived a hypothesis based on this observation: the punishment expenditure of the individualistic agents ($\beta > 25$) is lower than other agents regardless of the cost of punishment and preference of other agents. To test the statistical significance, the difference in punishment expenditure of all preferences was calculated and analyzed using

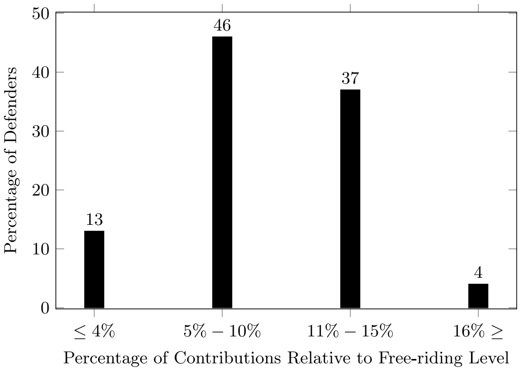


Fig. 7. Probability distribution of average contributions during the last five decision periods of 100 simulation runs ($N = 20$).

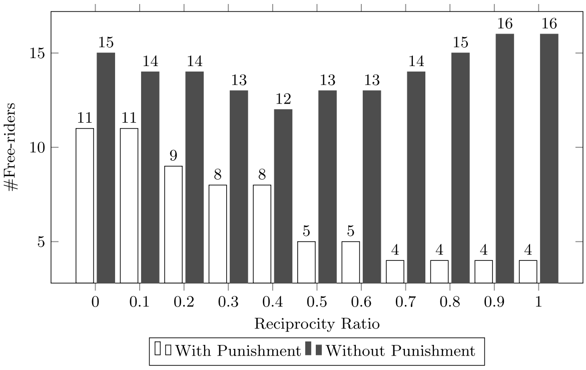


Fig. 8. Impact of reciprocal behavior on the number of free-riders in cooperative mode ($N = 20$).

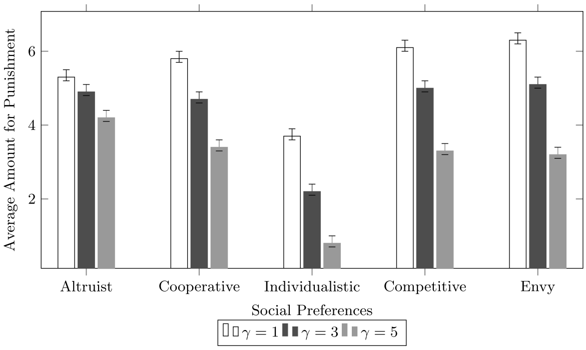


Fig. 9. The average spending on punishment by the contributors over 15 periods. ($N = 20$, Reciprocity Ratio = 0.5, Average of amounts in 100 runs of simulation).

the Mann–Whitney U test with Bonferroni correction. The punishment expenditure of the individualistic agents was significantly lower than altruistic ($Z = 2.711, p = 0.006$), cooperative ($Z = 3.181, p < 0.001$), competitive ($Z = 3.264, p < 0.001$), and envy ($Z = 2.793, p = 0.034$) agents. Therefore, this hypothesis is supported. In addition, we examined how the agents change their punishment expenditure level after increasing the cost of punishment. The results show that the cost functioned to change agents' willingness to punish, however this function was weaker in Altruistic preference than in other preferences. This finding provides support for the theory of "altruistic punishment" [68], which posits that individuals punish, although the punishment is costly for them and yields no material gain.

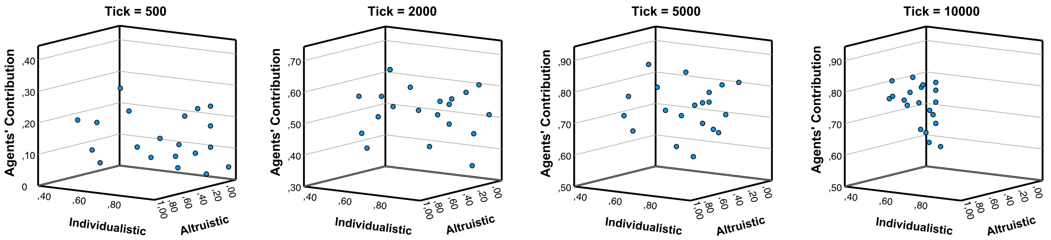


Fig. 10. Change of preferences over the time ($N = 20$, With Punishment).

Since the introduction of punishment promotes the level of contribution, it is meaningful to detect the potential reason for this phenomenon. In order to analyze the inherent nature of this promotion, we describe the density of contribution under the time series by plotting the change of proportion of individualistic and altruistic agents in Fig. 10. In the first 500 ticks, the non-contributors are in a dominant position to the contributors. In fact, we know that every agent tend to choose defection because they would have a high payoff value in the first steps. As time goes, the individualistic strategy will gradually disappear and the level of contribution rises to a certain level. This shows that the temptation of defection cannot compete with the dominating force with intensive externalities, and causes collective action towards provision of cybersecurity as a public good.

5.2. Validation

The model validation is a process of assessing the degree to which the model is a reasonable representation of the real world from the perspective of the model's intended applications. A clear understanding of the phenomena to be described by the model and testing the simplest behavior rules are the key to reliable ABM validation [69]. Validation has a rigorous-relevance issue. The most rigorous validation is data based, however, in order to conduct a rigorous validation for such a complex problem, we require collection of data for many years. Therefore, we employ other methods of validation in this study. Sargent proposed different methods of validity for simulation models [70]. This paper mainly studies the result of framing and managing cybersecurity as a public good, rather than specifically predicting the agents behavior in the environment. Therefore, we only test replicative validity (i.e. comparison to other models and determining the internal stochastic variability in the model).

There are four levels of model performance for replication validity [71]. Since, it would not be realistic to achieve the highest level (i.e. the model behavior is in quantitative agreement with empirical micro-structures, actual human behavior) due to inherent uncertainty in human behavior and the random events in reality, we satisfy the criteria of the third level which is quantitative agreement with empirical macro-structures. The results of this simulation model are compared with empirical data from previous studies [67,72,73]. The presented results show that the agents behavior in this model under all the conditions (i.e. with punishment, without punishment and reciprocity) is in line with the empirical data. For example, our results presented in Fig. 8 replicates the experimental results in [64]. Fehr and Schmidt show that only one free-rider can cause a large number of inequity-averse conditional contributors to behave selfishly, and therefore, cause the emergence of the free-riding behavior in the population.

6. Discussion and practical implications

In this section, we reflect on the central points of this work and combine the various findings into a general discussion. First, this paper provided a quantitative analysis to capture the main elements of public goods theory and investigated whether it complies with the characteristics of cybersecurity. We delineated that treating cybersecurity as a public good under a polycentric governance structure and decentralized punishment mechanism, enhances the cybersecurity posture of the environment. As discussed in Section 3 cybersecurity posture is an important macro-level metric to measure the success of collective actions undertaken by operating agents to provide cybersecurity as a public good. The lack of formalized and quantitative studies constitutes a substantial shortcoming in the studies focused on cybersecurity as a public good. We tackle this problem by integrating a variant of public goods game into the design of an agent-based model.

Admittedly, this approach does not provide a general solution to the missing formalization of this notion. However, incorporation of several well-established concepts in the game such as social preferences, evolutionary elements of strategies, and heterogeneity of the boundedly rational agents enabled us to computationally model this notion. Our results are based on the assumption that agents change their strategies and their social preferences are not stable. In the literature of cybersecurity economics, previous studies have included the learning and evolutionary dynamics in their models [74,75]. However, this is the first study that has incorporated these principles in the settings that agents treat cybersecurity as a public good. Moreover, the agents in this study are programmed to be responsive to factors such as marginal per capita return, punishments, and the contribution of other agents in addition to cyber attacks and their payoffs. Therefore, this study adopts a multi-paradigmatic approach (i.e., a process to systematically and thoughtfully listen, understand, appreciate, and learn from multiple paradigms and perspectives, and bring them together on research projects that we are working on), drawing knowledge from behavioral economics and evolutionary economics to make the results more prosperous and reliable.

The classic public goods game assumes that selfish and rational behavior of the players leads to suboptimal outcomes. Therefore, the unique Nash Equilibrium is not to contribute anything. However, there is no work that developed or tested a formal statement of this conjecture in the context of cybersecurity with the presence of negative and positive externalities, social preferences, and cyber-attacks. Incorporating these factors into our model leads to inconsistencies with prediction based solely on the induced utility. The results presented here support that contribution for provision of cybersecurity as a public good does not adequately reflect the Nash equilibrium of the game implied purely by self-interested and utility-maximizer agents. Far-from-equilibrium or out-of-equilibrium features have been articulated in complex adaptive systems and computational sociology literature [76]. Agent-based modeling has proved particularly useful in representing these systems and formalizing and testing explanations of cooperative/competitive dynamics. Comparing to variable-based approaches like statistical or mathematical modeling, ABM allows us to simulate emergence of macroscopic regularities, including change of preferences or increased contribution even in competitive mode, over time from interactions of autonomous and heterogeneous agents.

By systematically analyzing the influence of different model parameters, we gained further important insights: First, the results demonstrate that the decay to free-riding occurs only if agents are not able to punish the non-contributors and reciprocity is the dominant behavior of the agents. However, with possibility of punishment, the simulations demonstrate that agents adopt an evolutionary strategy towards the provision of cybersecurity as a public good and create a robust environment. In other words, the simulation results for our baseline model suggest that the environment forms a dominant strategy which promotes the cooperation efficiently. Furthermore, our simulations have been able to exhibit altruistic punishment and inequity aversion preferences in the agents' decisions. In this connection, it is important to mention that the success of providing cybersecurity as a public good was predominantly enabled by the dynamic level of contributions based on the agents' experience of being a victim, punished, or number of existing free-riders. We implemented this parameter (i.e., level of contribution) time-dependent. This allowed the agents to recover if too many successful attacks targeted their resources.

Drawing on our findings and discussions, we may now compile several practical implications for future debates promoting cybersecurity as a public good. Note that these implications are far from being exhaustive and should be regarded as an initiative for in-depth analysis.

1. **Cybersecurity as a multi-dimensional and complex process:** The nature of the goods or services being offered by institutional market agents such as businesses, unions, and nonprofits directly influences the scale of the institutions' market participation, ranging from global to local. For example, the contemporary telecommunications market is more efficient at the global and national scale. The global market in this sector is dominated by global institutions. On the other hand, the certain markets that require regional or local planning and expertise are inappropriate for a wide stage. However, a particular type of market, for example cybersecurity, is not limited to a single scale of operation with different institutional agents serving different customers (people or other institutions) territories.
   Cybersecurity requires the support and active participation of authorities at different levels (local, regional, national, and international) [77]. The authorities have a duty to develop sustainable policies and plans, and to cooperate with many stakeholders in different sectors (e.g., civil society, public services, academia, financial institutions, etc.). Within this cooperation, contradictory interests are predictable since cybersecurity is unavoidably burdened with many uncertainties. These uncertainties may entail opportunities for some stakeholders, and simultaneously, may pose risks for others.
   This is just one of the multi-dimensional aspects of institutions within the context of cybersecurity. Another aspect is that agents might take an adversarial stance against each other in pursuit of opposing goals. We see this phenomenon playing out in state-sponsored attacks against other states under cyber-enabled economic wars [78]. Alternatively, considering the collective response to a cyber attack as a public good, as stakeholders have their own interests, they may choose to misreport their private information to improve their own benefits. For example, if the general goal is to ensure fairness among stakeholders in terms of recovery from a recent cyber attack, the victims can report more damage in order to receive more resources than they deserve. To our best knowledge, no existing work has addressed the utility maximization problem under such private information misreport settings.
2. **Limitations of the definition of public goods:** Considering the aforementioned aspects and changes and evolution to which institutions are subject over time, it is necessary to determine the path and arrangements that promote transition towards sustainability[1] and avoid dysfunctional markets. Research conducted in the area of cybersecurity as a public good is grounded in Public Goods Theory. However, from a theoretical perspective, the Samuelson's narrow definition of public goods presents several conceptual and operational limitations within the context of cybersecurity that leaves it prone to dysfunctionality:

   - Excludability/rivalry criteria do not consider the social construction of the problems and decision-making processes related to the cybersecurity strategies to be implemented.
   - Territorial and collective dimensions of the cybersecurity strategies to be implemented are ignored and therefore, collective action problems or social dilemmas emerge.
   - The technical and institutional innovation, and the knowledge and competencies that are required to effectively implement the policy tools are not recognized adequately.

[1] Sustainability transitions refer to "long-term, multi-dimensional and fundamental transformation processes through which established socio-technical systems shift to more sustainable modes of production and consumption" [79].

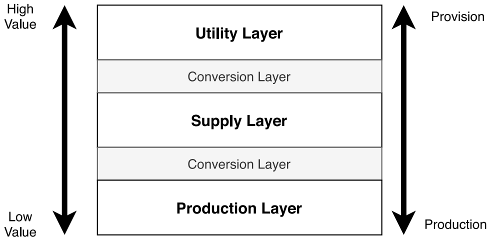


Fig. 11. Cybersecurity as a public good: Distinguishing between layers.

3. **Production vs. Provision:** Oakerson and Parks [80] defined the provision as public decisions about which goods and services to provide by public means, which private activities to regulate, how much public revenue to raise and how to raise it, what quantities of each service to provide and what quality standards to apply, and how to arrange for and monitor production. They also defined production as transforming input resources to make a product or render a service. The key insight of Ostrom et al. was that public provision did not require public production by the same governmental unit [81]. As the technology became more complex, vendors and third-party maintainers have started to play a role, along with regulators, each of which can be governed in quite different ways depending largely on the institutional arrangements. Therefore, a multi-layered perspective can improve the understanding, translating and deploying this insight.
   Fig. 11 illustrates the three main layers that we suggest to distinguish when treating cybersecurity as a public good. The utility layer corresponds to the cybersecurity itself with the characteristics of non-excludability and non-rivalrous. At this layer, the society as a whole drives utility from cybersecurity collectively. The supply layer determines the manner in which cybersecurity is offered. Finally, the production layer transforms the resources into products or services that are critical for the security of a digital ecosystem. An example of this is when a new cybersecurity product or service is produced, it will be certified in accordance with certain certification schemes (nation-wide or region-wide) and supplied by operational infrastructure providers. Then, the potential utility that is enabled by the supply layer will be accessed by the society as a whole. The characteristics of public goods at the supply or production layer might be different. For instance, the patent of the products or services can transform them into a private good. Therefore, these two layers are mostly affected by organizational and policy-related changes. These layers can be linked in various ways. In any case, the value, effectiveness and usability of cybersecurity relies on the value-added processes, scarcities and vulnerabilities of the ecosystem. Therefore, conversion layers draw a path associated with the efficiency in the use of cybersecurity to follow by the all actors over time.

Cybersecurity is characterized by interdependencies among people, organizations and governments, and it varies in the scale at which those interdependencies occur. Hence, with regard to the implications of our research, we posit that this multi-layered perspective enables the balance in cybersecurity from bottom-up voluntary approaches and collaboration, and avoids from heavier regulations. New institutional arrangements by distinguishing between the good itself, the provision and the production of the good, and the efficiency related to the path from production to provision of the good, should be designed to create a secure and resilient environment.

7. Conclusion

We presented a model that explores the interdependence of individual decisions in a repeated public goods game, in which cybersecurity is a public good. This model, under a polycentric governance structure, maps agents' preferences to choices of contribution and punishment. Repeated interactions among the defenders that remember their experience of cyber attacks, punishments, and contributions by others, results in a convergence of individual preferences and emergence of a cooperative behavior. Heterogeneity of agents is represented by heterogeneous social preferences with different reciprocal behavior, various level of resources, and different source of incentives. All these parameters affect the probability of the contribution and punishment of non-contributors.

The numerous externalities in the context of cybersecurity and difficulty in assessing the cybersecurity value and cyber risks cause misaligned incentives and information asymmetry. These, in turn, contribute to poor cybersecurity investment and management. However, this study suggests that the theory of public goods should play a more significant role in how we treat cybersecurity in the fast developing societies to maintain robust and resilient digital ecosystems. Moreover, it shows that maintaining the resilience of the systems promotes the collective actions among the defenders to combat the future attacks. This highlights the importance of experience and strongly interdependent decisions that changes the status of the environment radically. In addition, a sensitivity analysis revealed that the average contribution is markedly influenced by an effective decentralized punishment mechanism. The consistency of the pattern of our results across different empirical studies lends us some reassurance that our model behavior is in quantitative agreement with empirical macro-structures.

This is the first implementation of a public goods game in the context of cybersecurity to investigate whether the theory of public goods complies with this domain. This study is a starting point for research in quantitative analysis of the doctrine of public cybersecurity. Although the results of our study show that a polycentric governance structure has been effective to achieve collective action in the face of fluctuations and disturbance changes, development of a feasible plan for the private and public sectors to effectively manage cybersecurity as public good is beyond the scope of this article. However, we offer several avenues for future research.

In the future, we aim to investigate different types of economic efficiencies in this domain and explore the factors that define the efficient and optimized situations (e.g., optimized resource allocation to security measures) in this context. Moreover, by employing the social structure and institutional economics, future work can focus on the design and analysis of utility, provision, and production layers of cybersecurity, and propose a constructive and practical institutional arrangement to treat cybersecurity as a public good. Moreover, our model could be extended in several ways, for instance, by implementing more complex attack and defense scenarios, creating alliances of defense, or by capturing the impact of the attackers' dynamic pattern of behavior. Yet, a series of additional analyses could be done using the present model, for example, to shed light on the actual role of different distributions for resources or probabilities of cyber attacks.

References

[1] D. Geer, E. Jardine, E. Leverett, On market concentration and cybersecurity risk, J. Cyber Policy 5 (1) (2020) 9–29.

[2] R. Anderson, C. Barton, R. Bölme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, M. Vasek, Measuring the changing cost of cybercrime, 2019.

[3] M. McLennan, The Global Risks Report 2021, World Economic Forum.

[4] U. Nations, Resolution Adopted by the General Assembly on 6 July 2017. Work of the Statistical Commission Pertaining to the 2030 Agenda for Sustainable Development, United Nations New York, NY, 2017.

[5] F. Filgueiras, V. Almeida, The digital world and governance structures, in: Governance For The Digital World, Springer, pp. 7–42.

[6] S.J. Shackelford, Cyber War And Peace: Toward Cyber Peace, Cambridge University Press, 2020.

[7] D.K. Mulligan, F.B. Schneider, Doctrine for cybersecurity, Daedalus 140 (4) (2011) 70–92.

[8] F.B. Schneider, E.M. Sedenberg, D.K. Mulligan, Public Cybersecurity and Rationalizing Information Sharing, Technical Report, International Risk Governance Center (IRGC), 2016.

[9] M. Kianpour, Heterogeneous preferences and patterns of contribution in cybersecurity as a public good, in: Proceedings Of The 13th International Conference On Agents And Artificial Intelligence (ICAART 2021), Scitepress, 2021.

[10] D. Schatz, R. Bashroush, J. Wall, Towards a more representative definition of cyber security, J. Digit. Forensics Secur. Law 12 (2) (2017) 53–74.

[11] M. Milgate, Goods and Commodities, Palgrave Macmillan UK, London, 2008, pp. 2512–2516.

[12] P. Rosenzweig, Cybersecurity, the Public/Private'Partnership,'and Public Goods, Hoover Natl. Secur. Law Task Force (2011).

[13] P.A. Samuelson, The pure theory of public expenditure, Rev. Econ. Stat. (1954) 387–389.

[14] J.K. Galbraith, The Affluent Society, Houghton Mifflin Harcourt, 1998.

[15] E. Krahmann, Security: Collective good or commodity? Eur. J. Int. Relat. 14 (3) (2008) 379–404.

[16] E. Gal-Or, A. Ghose, The economic incentives for sharing security information, Inf. Syst. Res. 16 (2) (2005) 186–208.

[17] I. Kaul, P. Conceicao, K. Le Goulven, R.U. Mendoza, Providing Global Public Goods: Managing Globalization, Oxford University Press, 2003.

[18] K. Hagedorn, Particular requirements for institutional analysis in nature-related sectors, Eur. Rev. Agric. Econ. 35 (3) (2008) 357–384.

[19] I. Kaul, R.U. Mendoza, Advancing the concept of public goods, Provid. Glob. Public Goods: Manag. Glob. 78 (2003) 95–98.

[20] T. Tropina, Public–private collaboration: Cybercrime, cybersecurity and national security, in: Self-And Co-Regulation In Cybercrime, Cybersecurity And National Security, Springer, 2015, pp. 1–41.

[21] M. Kianpour, Knowledge and Skills Needed to Craft Successful Cybersecurity Strategies, in: Norsk IKT-Konferanse For Forskning Og Utdanning. No. 3, 2020.

[22] J.H. Choi, K. Han, Implications of false alarms in dynamic games on cyber-security, 2020, Available at SSRN 3660197.

[23] R. Pittiglio, F. Reganati, F. Ricci, C. Tedeschi, Cybersecurity, personal data protection and crime prevention from an Italian perspective, in: The Palgrave Handbook Of Corporate Sustainability In The Digital Era, Springer, pp. 131–156.

[24] M. Taddeo, Is Cybersecurity a Public Good?, Springer, 2019.

[25] A. Asllani, C.S. White, L. Ettkin, Viewing cybersecurity as a public good: The role of governments, businesses, and individuals, J. Legal Ethical Regul. Issues 16 (1) (2013) 7.

[26] E.M. Sedenberg, D.K. Mulligan, Public health as a model for cybersecurity information sharing, Berkeley Technol. Law J. 30 (3) (2015) 1687–1740.

[27] D.R. McCarthy, Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order, Politics Gov. 6 (2) (2018) 5–12.

[28] D. Assaf, Models of critical information infrastructure protection, Int. J. Crit. Infrastructure Prot. 1 (2008) 6–14.

[29] M. Shore, Y. Du, S. Zeadally, A public-private partnership model for national cybersecurity, Policy & Internet 3 (2) (2011) 1–23.

[30] M. Dunn-Cavelty, M. Suter, Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection, Int. J. Crit. Infrastructure Prot. 2 (4) (2009) 179–187.

[31] M. Carr, Public–private partnerships in national cyber-security strategies, Int. Aff. 92 (1) (2016) 43–62.

[32] A.D. Givens, N.E. Busch, Realizing the promise of public-private partnerships in US critical infrastructure protection, Int. J. Crit. Infrastructure Prot. 6 (1) (2013) 39–50.

[33] R.J. Harknett, J.A. Stever, The new policy world of cybersecurity, Public Adm. Rev. 71 (3) (2011) 455–460.

[34] S.J. Shackelford, Toward cyberpeace: Managing cyberattacks through polycentric governance, Am. UL Rev. 62 (2012) 1273.

[35] J.M. Bauer, M.J. Van Eeten, Cybersecurity: Stakeholder incentives, externalities, and policy options, Telecommun. Policy 33 (10–11) (2009) 706–719.

[36] H. Varian, System reliability and free riding, in: Economics Of Information Security, Springer, 2004, pp. 1–15.

[37] J. Grossklags, N. Christin, J. Chuang, Secure or insure? A game-theoretic analysis of information security games, in: Proceedings Of The 17th International Conference On World Wide Web, 2008, pp. 209–218.

[38] B. Johnson, R. Böhme, J. Grossklags, Security games with market insurance, in: International Conference On Decision And Game Theory For Security, Springer, 2011, pp. 117–130.

[39] E. Bonabeau, Agent-based modeling: Methods and techniques for simulating human systems, Proc. Nat. Acad. Sci. 99 (suppl 3) (2002) 7280–7287.

[40] S. Nicholls, B. Amelung, J. Student, Agent-based modeling: A powerful tool for tourism researchers, J. Travel Res. 56 (1) (2017) 3–15.

[41] E. Kiesling, M. Günther, C. Stummer, L.M. Wakolbinger, Agent-based simulation of innovation diffusion: a review, Cent. Eur. J. Oper. Res. 20 (2) (2012) 183–230.

[42] E. Bruch, J. Atwell, Agent-based models in empirical social research, Sociol. Methods Res. 44 (2) (2015) 186–221.

[43] R. Willer, K. Kuwabara, M.W. Macy, The false enforcement of unpopular norms, Am. J. Sociol. 115 (2) (2009) 451–490.

[44] S. Bistarelli, F. Fioravanti, P. Peretti, F. Santini, Evaluation of complex security scenarios using defense trees and economic indexes, J. Exp. Theor. Artif. Intell. 24 (2) (2012) 161–192.
[45] M. Kianpour, H. Øverby, S.J. Kowalski, C. Frantz, Social preferences in decision making under cybersecurity risks and uncertainties, in: International Conference On Human-Computer Interaction, Springer, 2019, pp. 149–163.
[46] H.P. Young, Social Norms, University of Oxford, 2007.
[47] B. Morsky, E. Akçay, Evolution of social norms and correlated equilibria, Proc. Nat. Acad. Sci. 116 (18) (2019) 8834–8839.
[48] M. Kandori, The erosion and sustainability of norms and morale, Jpn. Econ. Rev. 54 (1) (2003) 29–48.
[49] B.C. Eaton, M. Eswaran, The evolution of preferences and competition: a rationalization of veblen's theory of invidious comparisons, Can. J. Econ. 36 (4) (2003) 832–859.
[50] R.M. Isaac, K.F. McCue, C.R. Plott, Public goods provision in an experimental environment, California Institute of Technology, 1982.
[51] D.T. Kenrick, V. Griskevicius, J.M. Sundie, N.P. Li, Y.J. Li, S.L. Neuberg, Deep rationality: The evolutionary economics of decision making, Soc. Cogn. 27 (5) (2009) 764–785.
[52] M. Olson, The Logic Of Collective Action: Public Goods And The Theory Of Groups, Second Printing With A New Preface And Appendix, vol. 124, Harvard University Press, 2009.
[53] E. Ostrom, J. Walker, R. Gardner, Covenants with and without a sword: Self-governance is possible, Am. Political Sci. Rev. 86 (2) (1992) 404–417.
[54] B. Herrmann, C. Thöni, S. Gächter, Antisocial punishment across societies, Science 319 (5868) (2008) 1362–1367.
[55] M. Dufwenberg, P. Heidhues, G. Kirchsteiger, F. Riedel, J. Sobel, Other-regarding preferences in general equilibrium, Rev. Econ. Stud. 78 (2) (2011) 613–639.
[56] L. Hurwicz, Outcome functions yielding Walrasian and Lindahl allocations at Nash equilibrium points, Rev. Econ. Stud. 46 (2) (1979) 217–225.
[57] T. Kim, A stable Nash mechanism implementing Lindahl allocations for quasi-linear environments, J. Math. Econom. 22 (4) (1993) 359–371.
[58] F. Vega-Redondo, Implementation of lindahl equilibrium: an integration of the static and dynamic approaches, Math. Social Sci. 18 (3) (1989) 211–228.
[59] T. Saijo, T. Yamato, Fundamental impossibility theorems on voluntary participation in the provision of non-excludable public goods, Rev. Econ. Des. 14 (1) (2010) 51–73.
[60] M.D. McGinnis, Costs and challenges of polycentric governance: An equilibrium concept and examples from US health care, 2011, Available at SSRN 2206980.
[61] K. Carlisle, R.L. Gruby, Polycentric systems of governance: A theoretical model for the commons, Policy Stud. J. 47 (4) (2019) 927–952.
[62] K. Bissell, R. LaSalle, P. Cin, Ninth Annual Cost of Cybercrime Study, vol. 6, Ponemon Institute, Dublin, Ireland, 2019.
[63] C. Hasan, Making sound security investment decisions, J. Inf. Priv. Secur. 6 (1) (2010) 53–71.
[64] E. Fehr, K.M. Schmidt, A theory of fairness, competition, and cooperation, Q. J. Econ. 114 (3) (1999) 817–868.
[65] G.E. Bolton, A. Ockenfels, ERC: A theory of equity, reciprocity, and competition, Amer. Econ. Rev. 90 (1) (2000) 166–193.
[66] J.O. Ledyard, 2. Public Goods: A Survey Of Experimental Research, Princeton University Press, 2020.
[67] U. Fischbacher, S. Gachter, Social preferences, beliefs, and the dynamics of free riding in public goods experiments, Amer. Econ. Rev. 100 (1) (2010) 541–556.
[68] E. Fehr, S. Gächter, Altruistic punishment in humans, Nature 415 (6868) (2002) 137–140.
[69] P. Ormerod, B. Rosewell, Validation and verification of agent-based models in the social sciences, in: International Workshop On Epistemological Aspects Of Computer Simulation In The Social Sciences, Springer, 2006, pp. 130–140.
[70] R.G. Sargent, Verification and validation of simulation models, J. Simul. 7 (1) (2013) 12–24.
[71] R. Axtell, J. Epstein, Agent-based modeling: Understanding our creations, Bull. Santa Fe Inst. 9 (4) (1994) 28–32.
[72] A. Falk, U. Fischbacher, A theory of reciprocity, in: CEPR Discussion Paper, 2001.
[73] J.A. Lacomba, R. López-Pérez, Cooperation, in: Experimental Economics, Springer, 2015, pp. 105–123.
[74] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, A. Martin, An evolutionary game-theoretic framework for cyber-threat information sharing, in: 2015 IEEE International Conference On Communications (ICC), IEEE, 2015, pp. 7341–7346.
[75] H. Hu, Y. Liu, C. Chen, H. Zhang, Y. Liu, Optimal decision making approach for cyber security defense using evolutionary game, IEEE Trans. Netw. Serv. Manag. 17 (3) (2020) 1683–1700.
[76] W.B. Arthur, Out-of-equilibrium economics and agent-based modeling, Handb. Comput. Econ. 2 (2006) 1551–1564.
[77] S. Kowalski, IT Insecurity: A multi-disciplinary inquiry, 1996.
[78] M. Kianpour, Socio-technical root cause analysis of cyber-enabled theft of the US intellectual property–the case of APT41, 2021, arXiv preprint arXiv:2103.04901.
[79] J. Markard, R. Raven, B. Truffer, Sustainability transitions: An emerging field of research and its prospects, Res. Policy 41 (6) (2012) 955–967.
[80] R.J. Oakerson, R.B. Parks, The study of local public economies: Multi-organizational, multi-level institutional analysis and development, Policy Stud. J. 39 (1) (2011) 147–167.
[81] V. Ostrom, C.M. Tiebout, R. Warren, The organization of government in metropolitan areas: a theoretical inquiry, Am. Political Sci. Rev. 55 (4) (1961) 831–842.

Chapter 9

Research Paper 5: Analysis of institutional design of EU cyber incidents and crises management as a complex public good.

Mazaher Kianpour and Christopher Frantz. Presented at the Annual Conference of Institutional Grammar Research Initiative (IGRI June 20-22, 2022) – Under review in Policy Studies Journal.

This paper is awaiting publication and is not included in NTNU Open

Chapter 10

Research Paper 6: Designing serious games for cyber ranges: a socio-technical approach

Mazaher Kianpour, Stewart Kowalski, Erjon Zoto, Christopher Frantz, Harald Øverby - *2019 IEEE European symposium on security and privacy workshops (EuroS&PW)*

Chapter 11

Research Paper 7: Promoting Secure and Sustainable Behavior in Digital Ecosystems Through Gamification

Mazaher Kianpour and Stewart Kowalski - *Handbook of Research on Gamification Dynamics and User Experience Design, 2022*

ISBN 978-82-326-6045-2 (printed ver.)
ISBN 978-82-326-5418-5 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU
Norwegian University of
Science and Technology