

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)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

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 RiskIQ¹ 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, IBM², 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 Mussington³ 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 Demchak⁴ 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/>

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

⁴The 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

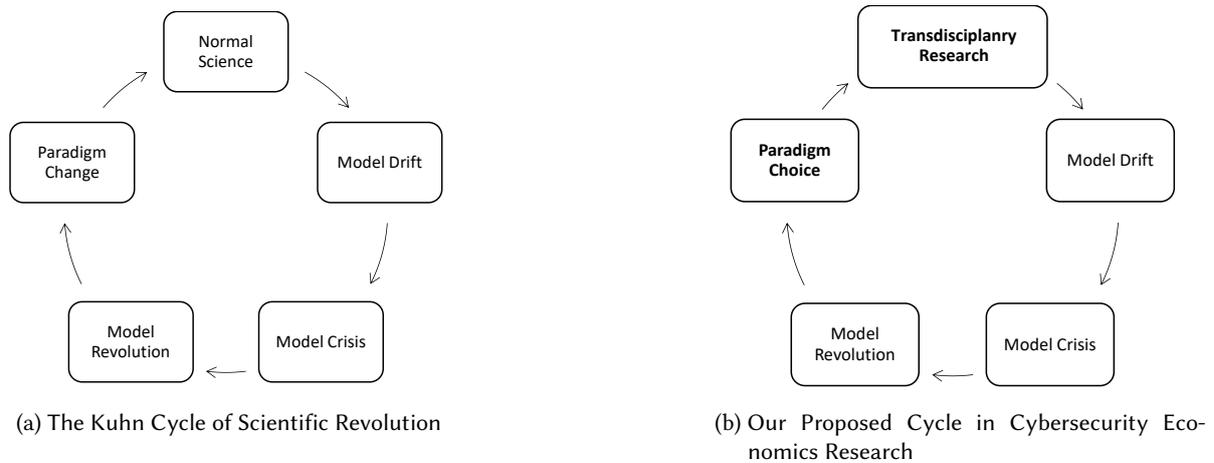


Figure 1: Our proposition to foster multi-paradigmatic approaches in cybersecurity economics research

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 thought⁵. 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.

⁵While 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 perplexity⁶.

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 different fields. For example, Giovanni 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

⁶Complicated 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 Emanicipatory, 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 incommensurability⁷. Moreover, the successful 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

⁷Since 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 it 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 cybersecurity⁸. 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 within 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 field 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

⁸Cybersecurity, 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.

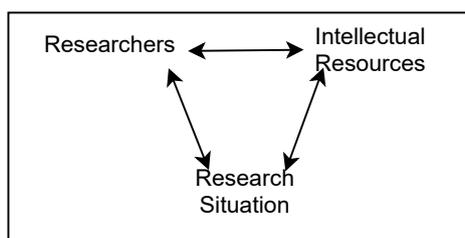


Figure 2: The relationships of researchers, research situation, and intellectual resources forms the research context for the issues under study.

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 unpredicted 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 $\{X(t_1), X(t_2), \dots, X(t_m)\}$ and $\{X(-t_1), X(-t_2), \dots, X(-t_m)\}$ 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

⁹Only 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 below¹⁰. 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

¹⁰It 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 studies¹¹.

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

¹¹These 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. Willemsen, 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. Cavelti, 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 complementarity 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 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. Ardalán, *Global Political Economy: A Multi-paradigmatic Approach*, Springer, 2018.
- [47] K. Ardalán, 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. Kozłowski, 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.