Towards a Typology of Interdisciplinarity in Cybersecurity

Trade, Choice, and Agnostic-Antagonist

Kocksch, Laura Anna; Sørensen, Estrid

Published in:
NSPW '23

DOI (link to publication from Publisher):
10.1145/3633500.3633510

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Towards a Typology of Interdisciplinarity in Cybersecurity: Trade, Choice, and Agnostic-Antagonist

Laura Anna Kocksch*
laurak@ikl.aau.dk
The Techno-Anthropology Lab, TANTlab
Aalborg University
Copenhagen, Denmark

Estrid Sørensen
estrid.sorensen@rub.de
Faculty of Social Science
Ruhr-University Bochum
Bochum, Germany

ABSTRACT

Cybersecurity research increasingly involves non-engineering disciplines, such as psychology, social science and law [41]. In this paper, we argue that cybersecurity research is not only reshaped through new methods and concepts of these adjacent fields, but also through shared interdisciplinary practices. Existing literature on interdisciplinarity in cybersecurity is primarily concerned with defining ideal models that are based on ideals, rather than in empirical research of how interdisciplinarity is formed in practice. We offer an ethnographic analysis of interdisciplinary formats based on our four-year participation in the ongoing interdisciplinary cybersecurity PhD programme SecHuman at the Ruhr-University Bochum, Germany. The PhD programme brings together engineers, social scientists as well as humanities scholars. Drawing on methods and literature of ethnographic science and technology studies (STS), we attend to eight different interdisciplinary formats and analyse how they shape cybersecurity research: its logics of accountability, of innovation, and of ontology [3]. This leads to a typology of five modes of interdisciplinarity that can be found in the PhD programme: 1. choice, 2. subordinate-service, 3. integrative-synthetic, 4. trading, and 5. agonistic-antagonistic. Based on our empirical findings, we discuss how each mode shapes cybersecurity, and conclude with suggestions of how to craft interdisciplinary formats in the field.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*; • **Social and professional topics** → *Computing organizations.*

KEYWORDS

Usable Security, Interdisciplinarity, Science and Technology Studies, Collaboration, Practice Research

ACM Reference Format:
Laura Anna Kocksch and Estrid Sørensen. 2023. Towards a Typology of Interdisciplinarity in Cybersecurity: Trade, Choice, and Agnostic-Antagonist. In *New Security Paradigms Workshop (NSPW '23), September 18–21, 2023, Segovia, Spain.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3633500.3633510

*Both authors contributed equally to this research.

NSPW '23, September 18–21, 2023, Segovia, Spain

ACM ISBN 979-8-4007-1620-1/23/09.
https://doi.org/10.1145/3633500.3633510

1 INTRODUCTION

The general move from the term "IT-security" with more technical associations to the notion of "cybersecurity" testifies to the area of research having developed from a mono-discipline of engineering and computer science to a multi-discipline involving researchers from a variety of backgrounds; from engineering to law, political science, psychology, cultural and media studies, economics, anthropology, etc. [40, 41]. When the PhD programme SecHuman[1] started its activities in 2016, the question of how to organise interdisciplinary collaboration in cybersecurity research had not been an issue of academic scrutiny. The PhD programme thus hardly had a model to follow as to which formats of interdisciplinary collaboration would be most desirable in cybersecurity research [2].

Science and technology studies (STS) scholars Andrew Barry and Georgina Born [3] emphasise that interdisciplinarity is not only a matter of how colleagues from different disciplines collaborate. It also contributes to shaping and re-shaping fields of study by re-orienting:

a what the field is responsive to (the logic of accountability),
b what becomes the desired outcome of the field (logic of innovation),
c what is understood as the problems and research objects of the field (logic of ontology).

While a heated debate has arisen over the question of whether cybersecurity ought to be treated as a science that devises fundamental laws [32], we lean on approaches that analyse the "mechanisms" and concrete practices of cybersecurity research [31]. In this article, we focus in particular on *formats* of interdisciplinarity, which are the concrete material settings and activities in which interdisciplinary collaboration unfolds, such as shared lectures, workshops, or two-on-two teams. We suggest these formats as sites in which the three logics become negotiated. The SecHuman PhD programme serves as an empirical case to analyse and critically assess the combination of logics in different modes.

Studies of how to practically organise interdisciplinarity in cybersecurity research and education are rare [36]. The existing literature mainly aims to develop models for interdisciplinary cybersecurity research. These models are not founded on empirical evidence of how interdisciplinary cybersecurity research is done in practice and

[1] SecHuman - Security for Humans in Cyberspace, Interdisciplinary PhD programme funded by the Ministry of Culture and Science of North Rhine-Westphalia, Germany: https://sechuman.ruhr-uni-bochum.de/
[2] SecHuman is by no means the first interdisciplinary cybersecurity PhD programme. This makes it even more surprising that a systematic review of the modes of interdisciplinarity performed in such programmes is lacking

with what effects, of what is studied, and how. While existing models are useful for planning cybersecurity research and educational programmes, no studies exist of how such models are performed in and performative of the material practices of working together in an interdisciplinary fashion. In our literature review, we turn to empirically based literature from the field of STS that engage with interdisciplinary research in general – i.e. beyond cybersecurity research. A central source is Barry and Born's [3] work, which is based on analyses of various interdisciplinary projects that allow the authors to develop a vocabulary for differentiating between *modes of interdisciplinarity* and between the distinct logics they unfold. Mobilising and extending Barry and Born's vocabulary, this paper identifies *five* different modes of interdisciplinarity in the formats of the SecHuman PhD programme:

(i) choice mode
(ii) synthetic-integrative
(iii) subordinate-serving
(iv) trading mode
(v) agonistic-antagonistic mode

Modes (i) and (ii) are part of Barry and Born's vocabulary, while the choice and the trading modes were developed through our research, as will be discussed below. Each mode combines the three logics mentioned above (a – c) differently, which constitute their specificity. Although Barry and Born's vocabulary is highly functional in differentiating epistemic goals, relations, and scopes of inquiry across interdisciplinary projects, it does not consider concrete individual formats nor the material compositions and tools that are devised in each mode. With this paper, we seek to close this gap by providing a study of the concrete material practices of interdisciplinary collaboration. Furthermore, and more importantly, we aim to understand the specific modes of interdisciplinary collaboration in cybersecurity. By equipping cybersecurity with an understanding of practical interdisciplinary formats as sites where its research is coordinated, produced and (possibly) contested, cybersecurity scholars can actively seek alternative ways of thinking about the field's interdisciplinarity. In other words, we offer a typology for devising formats that may facilitate an "opening" of the field [24].

While cybersecurity research faces a set of challenges (namely, a shifting object of study, i.e., code; adversarial developments and secrecy [31]), this article points to the specific challenges involved in researching cybersecurity *in an interdisciplinary fashion*. Through our suggested terminology of modes, variances become visible in how disciplinary knowledge is integrated, subordinated, traded or reflected upon. The aim of this article is therefore to provide an empirically founded typology of modes of interdisciplinarity in SecHuman, thereby contributing to reflections within the community upon existing and alternative ways of thinking about the field of cybersecurity research: its object of study, what is considered innovation, and what scholars are accountable for. We see particular need to further elaborate the agonistic-antagonistic in cybersecurity research, while not replacing other modes. The typology should be understood as both an attempt to put forward a vocabulary to grasp different interdisciplinary practices in SecHuman and as a way of informing the systematic planning and organising of interdisciplinary encounters in cybersecurity more broadly. Being able to sort future efforts into the five modes may aid to critically reflect about goals and assumptions in interdisciplinary cybersecurity projects.

The data analysed is based on an ethnographic processing of the authors' four-year intense participant-observation in the PhD programme SecHuman. Additionally, the analysis draws on a participatory workshop that was devised to discuss interdisciplinarity among the programme's members. The workshop evolved around a semantic network graph of co-occurring terms in publications of the PhD programmes' members, which the authors prepared for this purpose. The combined approach allows us to enhance our understanding of virtues and deficits of different practical formats for interdisciplinary work in cybersecurity. The analysis is a case-study and does not aim for generalisation of its findings. Instead, the aim is to specify a vocabulary for understanding interdisciplinary formats in cybersecurity research. Results are presented below in three sections that describe and analyse eight different formats, of which each performs the modes and logics of interdisciplinary cybersecurity in different ways.

2 RELATED WORK

The call for interdisciplinarity in technological research started in the 1970s as the US Congress established a Technology Assessment institution to present early warnings to prevent negative impacts of technology [17]. The Chernobyl nuclear power plant disaster in 1986 added intensity and emphasis to the need of more than technical perspectives on technology development. Consequently, the notion of innovation -– and indeed responsible innovation [13] – was introduced to replace the idea of progress as solely technical, and to emphasise the integration of technical and societal change.

Cybersecurity was born into this scientific and political situation, and thus into a climate of interdisciplinary demands. However, it was also born out of mainly engineering and computer science departments, and it continues to hold a strong conviction to produce quantitative results and technical solutions [15]. This has the effect that most studies of cybersecurity are centred around specific, often isolated, technical functions and issues pertaining to specific vulnerabilities. This limits the scope of interdisciplinary collaboration to testing the usability or "effects" of technical solutions. More and more authors emphasise the need for a broader scope to include more complex social relations involved in cybersecurity [1, 10, 11], for example, research that takes wider ethical and political considerations into account [12]. Choras et al. [8, p. 280-1] argue for an opening of cybersecurity research by recommending to:

- not only focus on critical infrastructures, but attending also to citizens and smaller companies or institutions,
- not only focus on highly professionalised hackers and cyberattacks, but attending to more amateurish IPR violations, cyberstalking, child pornography, etc.,
- not focus on single algorithms and tools, believing that they can save the world but attending also to offline and non-technical measures for cybersecurity.

Choras and colleagues develop the THOR model to embrace a holistic approach to "all cybersecurity issues", which they divide according to different types of activities needed: Technical, Human, Organizational (institutional co-ordination efforts) and Regulatory,

thus the acronym THOR. They, thereby, discourage activities in cybersecurity that "might be seen as individual silos or islands [for the sake of] a coordinated and joined up approach where all parties talk to each other" [8, p. 292]. The THOR model became the foundation for the CAMINO (Comprehensive Approach to cyber roadMap coordINation and development) roadmap aimed at reaching more effective measures against cybercrime and cyberterrorism. This roadmap identified 60 objectives and 250 milestones for cybersecurity [8]. Such numbers indicate the complexity of the task and need for further explication of how interdisciplinarity can facilitate critical and holistic cybersecurity research. So far, authors primarily point to the different interdisciplinary areas of expertise that are necessary to bring together to study security in cyberspace, and the CAMINO project reaches an impressive level of detail in doing so [8]. However, in order to overcome the attention to isolated issues in cybersecurity, a further opening is needed that may be reached through the investigation of interdisciplinary modes. Knowing what modes perform what kind of interdisciplinarity, and accordingly, how cybersecurity is practised, allows scholars of the field to develop and choose formats more strategically.

Ramirez [29] identifies four academic fields engaged in current cybersecurity research: politics, computer science, management, and social science, and states a lack of collaboration and communication between these disciplines [29]. Ramirez and Choucri [30], in response, suggest the four disciplines could assemble around four areas, or what STS scholars have termed 'concerns' [21]: policy, infrastructure, business and general. Similar to other scholars [7], Ramirez suggests the lack of interdisciplinary collaboration and communication in cybersecurity research is caused by the diversity of terminologies applied to deal with cybersecurity issues. Accordingly, he proposes a standardization of cybersecurity vocabulary with a number of fixed and rigorously defined terms, which should be applied exclusively. In other words, the challenges of the multidisciplinarity of cybersecurity is purportedly solved by formulating a new unitary grammar for cybersecurity. Developing a singular language suggests the development of cybersecurity as a new homogeneous discipline, rather than continuing as a genuinely heterogeneous and interdisciplinary field with the internal tensions and challenges that also exist in the everyday life of cybersecurity.

Let us follow up on the latter point by turning to STS, which itself is an interdisciplinary field of study concerned with a large variety of issues of the social, material, discursive and political components of scientific and technological developments [39]. STS has not addressed the interdisciplinarity of cybersecurity, but has early on investigated the principles and patterns of interdisciplinarity in various different areas, and repeatedly discovered that successful interdisciplinary collaboration does not rely on shared language and methods, but on tools and spaces for connecting across differences [14, 33]. Drawing on experiences from climate research, and from an STS perspective, Barry and Born [3] turn the question concerning interdisciplinarity around by asking not *whether* interdisciplinarity may be helpful in solving specific problems, but instead by asking why we have come to require of interdisciplinarity to solve specific problems, and what new relations and attentions are shaped through interdisciplinarity. Rather than asking how cybersecurity's problems can be solved through interdisciplinary collaborations, we ask in line with Barry and Born what kind of cybersecurity results out of different modes of interdisciplinarity. This approach shifts attention to how interdisciplinarity unfolds in practice and shapes the object it studies. Barry and Born suggest three modes and three logics of interdisciplinarity. The modes identify different ways of working together across disciplines:

Disciplines working together in an *integrative-synthetic mode* add up by each attending to a different area of a well-defined problem or by combining methods or concepts to solve this problem. In the case of cybersecurity this interdisciplinary mode works well for disciplines that share the same basic assumptions about what counts as technical and as social, about the value and character of scientific results and their societal relevance, etc. Cryptographers and psychologists work together successfully in this mode: the former take care of coding, the latter take care of individual humans. This clear division of labour ensures that the disciplines avoid challenging each other's theoretical and methodological commitments.

The *subordination-service mode* establishes a relationship between disciplines in which one is in service of the other. The service discipline typically fills in for the absences in the other discipline. The ELSI concept – ethic, legal and social implications (of for instance cybersecurity) – suggests this mode of interdisciplinarity, allowing science or engineering to continue their ways of working by letting philosophy, legal, and social science take care of the commitments that these lack abilities to attend to.

Barry and Born's [3] *agonistic-antagonistic mode* refers to interdisciplinary work that is founded in a dissatisfaction or critique of specific disciplines' way of working. At the basis of this mode is a wish not just to solve specific problems better or to gain particular insights, but to change the way in which disciplines do so. The agonistic-antagonistic mode seeks to shape a new *transdiscipline* that challenges the ontological assumptions specific to prior disciplines. This transdiscipline differs from the two modes mentioned above in that it is irreducible to the partaking disciplines. This last mode of interdisciplinarity is, we suggest, not yet fully articulated for cybersecurity research.

Different from the two other modes, the agonistic-antagonistic mode holds promises for new ways of understanding cybersecurity as not either – nor both – a technical, psychological, legal, social and philosophical problem, but as a phenomenon that combines and configures technical and social relations, political and legal structures, and psychological and philosophical ideas in new ways and thus allow not only for solving problems but for understanding problems in novel ways. It generates an "ontological opening" of cybersecurity, as suggested by Liebetrau and Christensen [24, p. 31].

We use these modes as a point of departure for proposing a typology of modes of interdisciplinarity in SecHuman. The typology helps identify differences between and specificities of interdisciplinary approaches. Additionally to the modes, Barry and Born [3] point to three *logics of interdisciplinarity*: accountability, innovation and ontology. According to the authors, these logics are core justifications for interdisciplinarity, just as they govern the trend towards interdisciplinarity. In this paper we refrain from attending to the logics and rationales that mobilize and govern interdisciplinarity in cybersecurity and inquire into the socio-material formats for configuring interdisciplinary practices, or to the effects of each logic: a. Inquiring about *accountability effects* we analyse what the

interdisciplinary formats make scholars responsive or accountable to, such as their own discipline, shared concerns or indeed to a transdiscipline. b. We follow *innovation effects* by asking what innovation interdisciplinarity is expected to provide in each format, and we analyse c. *ontology effects* by asking what new problems and empirical objects are generated through the disciplinary formats along with novel desires and subjectivities. By way of the modes and logics of interdisciplinarity, the specific characteristics of interdisciplinary formats and their differences can be identified, described and analysed.

Stubbe's [34] discussion paper is in line with Barry and Born's thinking, and offers an empirical evaluation of eleven interdisciplinary research projects. The projects were all funded by the German Federal Ministry for Education and Research within the frame programme "Bringing Technology to the Human" (Technik zum Menschen bringen). As a representative of the VDI/VDE Innovation + Technik GmbH, which is the organisation administering the Ministry's research funding schemes, Stubbe evaluated the 'integrated' character of the projects. Integrated research is defined as a holistic research perspective that sees the relation of human and technology not as a purely technical question, but also as an opportunity to approach societal challenges and opportunity for changes in perspectives. Interdisciplinarity, Stubbe states, is a crucial component of integrated research. He explains that the creative potential of this kind of research does not unfold if it is only set to legitimate or regulate existing research. While this corresponds to a critique of Barry and Born's integrative-synthetic mode of interdisciplinarity, a further point rejects what Barry and Born understand as the subordination-service mode: we do not need ELSI-research in technological projects simply to control or to implement ELSI components, Stubbe [34] maintains. Ethics committees exist for this purpose. Stubbe seems to support the agonistic-antagonistic mode when stating that integrated research needs to investigate the effects and values of ethical, legal and social aspects in technological research. This implies that ELSI aspects cannot be set prior to a research project but need to be identified during research practice and to be assessed and evaluated in this process.

Providing cybersecurity research with a stronger sense of its own scientific paradigmatic commitments and repertoires has been a strategy to go beyond being 'just engineering' [32]. As a response to the repeated claim that cybersecurity lacks a scientific sensitivity, Spring et al. [32] suggest emphasising why scientific approaches produce unsatisfactory results in cybersecurity. They argue that cybersecurity research has been judged according to a positivist paradigm, i.e. by an attempt to find irrefutable truths. By proposing to judge cybersecurity with a new set of criteria developed from the philosophy of science, they offer a new direction for cybersecurity research. In an interdisciplinary collaboration that resulted in a book publication, Metcalf and Spring [26] further advance what quality criteria cybersecurity research might impose on itself, asking the fundamental question "how to perform a good study in the field of cybersecurity" [26, p. 2]. This question is in no way banal, as it requires a conversation about what methods and practices of cybersecurity are granted valid. Our approach of identifying interdisciplinary formats and the effects of their logics of accountability, innovation, and ontology resonates with such attempts to understand the composition of cybersecurity.

To conclude, the literature on interdisciplinary cybersecurity research is currently searching for ways to combine the various disciplines it sees necessary for solving cybersecurity problems. It thereby often calls for a shared language of cybersecurity. Science and technology studies literature, on the other hand, tends to state the productivity of different disciplinary and transdisciplinary perspectives and vocabularies. It inquires what arrangements of disciplines make up interdisciplinarity and how they relate. In his evaluation of interdisciplinary research projects, Stubbe [34] confirms the potentials of the heterogeneous perspectives, and he even emphasises the need for 'disturbances' of path-dependent disciplinary viewpoints. Even though Stubbe emphasises that "the more concrete the better" is the core principle for the ability for interdisciplinary collaboration, very little literature exists that analyse how interdisciplinary research is conducted in practices. Barry and Born note that one of their interview partners stated that "I don't think we sat down and worked out a model of interdisciplinarity" [3, p. 17]. As is the case in most interdisciplinary projects, this project partner points to how they developed their cooperation in the process without paying explicit or strategic attention to how this could be done in the most relevant way. In our analysis below, we seek to remedy this. We apply Barry and Born's vocabulary to analyse the interdisciplinary formats that were applied and developed in the interdisciplinary cybersecurity PhD programme.

3 FIELD AND METHODS

The research field of this study was the interdisciplinary cybersecurity PhD programme SecHuman. The still ongoing programme gathers scholars from engineering, law, psychology, linguistics, social anthropology, media studies and mathematics. A core feature of the PhD programme are its six *Tandems*, which each consists of one student and one Principal Investigator (PI) from an engineering or science discipline and one student and one PI from the social sciences, humanities, law, psychology, or linguistics. The Tandem format is praised for its innovativeness and gained a mentioning in a US National Academies of Sciences, engineering, and Medicine report on future proved academic research [9]. Apart from the interdisciplinary Tandems, the programme devised seven other interdisciplinary formats, which are the object of this article: *Weekly Colloquia*, *Dummy Lectures*, *Summer Schools*, *Lab Visits*, *Shut-Up-And-Write Sessions*, *a discussion about a Semantic Network Graph*, and *a Scenario Exercise*. Some of these were planned from the beginning, others emerged later, partly as student initiatives.

The study in this article draws primarily on observations from the first four years of the PhD programme. It combines three different methods into a blended method analysis and case-study: participant observations, a participatory workshop, and discussions about a network graph. Even though interdisciplinarity was not the focal topic of our research in SecHuman, we were committed as STS scholars to reflecting our own research practices [23], and soon became curious about how the programme collectively shaped its object of study through different formats and modes of collaboration between the disciplines. We were members of the programme as PhD student (first author) and PI (second author). Additionally, we were participant observers taking field notes during gatherings

and discussing our observations with other participants of the programme for verification. The simultaneous positions as observers of and participants in a field of study implies certain challenges, which are common to ethnographic researchers, and reflected upon in the research process [18]. A variety of techniques was applied to distance the observers' perspective from the participants' perspectives, such as alienation, perspective-switching, and a naturalistic description style. This does not mean that the descriptions provided in this article are neutral. In general, ethnography rejects the possibility of a 'view from nowhere' [28] in any method and requires instead nuanced accounts of observations in order for readers to assess the plausibility of interpretations. Such are provided in the results section below.

Additional to our own ethnographic observations, we organised a Participatory Workshop on interdisciplinarity with the programme's PIs and PhD students in the summer of 2019. We used the workshop to collect further information about members' perspectives on interdisciplinarity. The participants were invited to engage in an interdisciplinary scenario, and we used their ways of doing so to identify different kinds of interdisciplinary collaborations. The Scenario Exercise is described in more details below.

The third method was to prepare a semantic network graph of co-occurring terms in 16 articles published by the programme's members. We applied the semantic analysis tool CorTexT Manager [6] and subsequent visualisation in Gephi [4] to identify semantic interrelations between the terms in the publications. We describe the method in more detail in the result section below. Instead of serving as a representation of the research group and their vocabulary, we utilised the graph as a tool to elicit conversations about interdisciplinarity during a workshop, where the graph was presented and commented on by programme's members.

As an ethnographic study, the analysis attends to everyday practices of the cybersecurity researchers. Its focus is not on university or disciplinary structures, nor on legal or regulatory conditions for academic institutions. In an ethnographic study, these are understood as embedded in the everyday practices, rather than making up an external foundation for practice. As the analyses show, particular commitments to disciplines as well as concepts of what counts as innovation and as the object of study of a discipline are negotiated and defined in everyday scientific practice. Practices are thus not less complex or far-reaching than are structures and institutional conditions; they are enacting the latter. Moreover, studies that attend to academic conditions and structures tend to remain silent about the ways in which everyday intellectual work of scientists is realized in practice. The latter is what this article offers.

The 'graphic' part of the term 'ethnographic' points to the methodology's analytic procedure, which is characterised by a series of analytic re-writings of the original data. First, the data from the three methods were combined into ethnographic descriptions of the programme's interdisciplinary formats. Next, we applied Barry and Born's [3] three modes of interdisciplinarity as a heuristic for analysing the ethnographic descriptions of the formats. This means that we compared the ethnographic descriptions with the modes of interdisciplinarity outlined by Barry and Born to identify similarities, differences and variations. None of the descriptions were identical to Barry and Born's modes of interdisciplinarity, which gave rise to re-writing the ethnographic descriptions of the formats to account for the differences, variations and combinations of modes. For those of our ethnographic descriptions that were entirely different from Barry and Born's modes, we analysed how they were different and how they could be characterized as new modes, while remaining within the principles of Barry and Born's heuristic, i.e., by attending to the logics of interdisciplinarity. This resulted in extending Barry and Born's heuristic into a new typology that includes *two new modes*: trading mode and choice mode. The result section presents the modes of interdisciplinarity we identified in our ethnographic analysis of the formats.

As a case study of interdisciplinary formats, the paper has no ambition to be representational of interdisciplinary work in cybersecurity elsewhere, nor is it the aim to present generalizable results. Rather, the empirical material is applied to develop a typology of interdisciplinary cybersecurity that is helpful for understanding, analysing and planning interdisciplinary cybersecurity research and educational programmes. The typology developed is not exhaustive but suggested as an initial vocabulary for analysing interdisciplinary cybersecurity research practices. It is our hope that colleagues will take up our efforts and, in the years to come, refine and complement them as more interdisciplinary cybersecurity research and educational programmes are established.

4 RESULTS: FORMATS OF INTERDISCIPLINARY CYBERSECURITY

In this section, we present our descriptions and analyses of the interdisciplinary formats in SecHuman's cybersecurity research.

4.1 Trading Mode of Interdisciplinarity

4.1.1 Tandems. The core interdisciplinary format of the programme were the Tandems. As introduced above, these were composed in the collaboration between one engineering, mathematics or computer science PhD project and one social science or humanities PhD project. The PhD students of each Tandem met regularly to discuss their individual projects and aspects of working together. While this format had been laid down from the outset of the PhD programme, it was realised in many different ways over time and through the collaboration processes. Following Barry and Born's modes of interdisciplinarity, we can distinguish between two different modes in which interdisciplinarity was performed through the Tandem format.

Two of the six Tandem projects resonated with Barry and Born's [3] description of the subordinate-service mode. One of the projects took its point of departure in the recognition in engineering that in order to attack a system, hackers need to learn how the system works. One means of protecting a system is thus to configure it in a way that hampers attackers' ability to learn how the system works. This process is known as obfuscation. However, engineering holds little knowledge about how people learn, and accordingly, this Tandem involved a psychology team to add expertise on learning processes to the project 'in service of' the computer science research question, as Barry and Born would put it.

The research question of another Tandem was defined by the linguistic team. This discipline has long attended to how to identify unknown authors, for instance of extortion letters or to verify

Table 1: Sub-ordinate Service and Synthetic-Integrative Mode of Interdisciplinarity

Format	Mode of Interdisciplinarity	Mode of Disciplinarity	Logic of Accountability	Logic of Innovation	Logic of Ontology
Tandem	Sub-ordinate Service	Territory with Permeable Boundaries	Accountability to Add to Other Discipline's Research Problem	Desires for New Empirical Objects/Tools	Disciplinary Positioned Exchange with Other Disciplines
Tandem	Synthetic-Integrative	Territory with Permeable Boundaries	Accountability to be Integrated into Other Discipline's Research Problem	Desires for New Empirical Objects/Tools	Disciplinary Positioned Exchange with Other Disciplines

the authenticity of a supposed author of a text. The linguistic Tandem partner team was interested in creating a machine learning system that could automatically identify unknown authors. Since linguistics lack the expertise to develop machine learning systems, a Tandem partner from engineering was included to fill in this gap.

Our description of these two interdisciplinary Tandems resonates with Barry and Born's subordinate-service mode of collaboration. The authors describe how the master discipline, – those formulating the research question (in the first case engineering, in the second linguistics) – extends its object of study, which in the first case was hackers' learning processes (for engineering) and in the second case a machine learning tool (for linguistics). Contrary to how Barry and Born describe the subordinate-service mode, we observed in SecHuman that also the serving disciplines, psychology in the first Tandem and engineering in the second, extended their empirical field and thus their object of study. Much critique of ELSI programmes [2] overlook that not only science and technical disciplines expand their area of study in collaboration with ELSI disciplines. Also ELSI partners encroach onto the areas of technical and science disciplines they 'serve'. Although the research question was primarily defined by one of the Tandem partner teams, the collaboration unfolded in both Tandems teams by both disciplines contributing to solving a different aspect of a well-defined problem and by combining methods or concepts to solve this problem, Barry and Born describe this as characteristic of the synthetic-integrative mode of interdisciplinarity. Although the process of problem definition resembled the subordinate-service mode, the research process unfolded in a synthetic-integrative mode. Table 1 summarises the logics of accountability, innovation, and ontology in the subordinate-service mode and the synthetic-integrative mode of interdisciplinarity in SecHuman.

The area of empirical research objects was expanded in engineering in the obfuscation-Tandem, and a tool was added to linguistics in the author-identification Tandem. Yet, the basic theoretical assumptions of the disciplines were not affected by the interdisciplinary collaboration, and the innovation logic was limited to the expansion of empirical area and to the addition of a tool. According to Stubbe [34], this mode is less promising in terms of delivering novel epistemic insights to the disciplines. The effect on the accountability logic of the two Tandems was also minimal. While working closely together on a shared problem, the epistemic horizon of the PhD scholars of the Tandems was a PhD degree in each their own disciplines. Each scholar remained solely accountable to their own discipline.

The interdisciplinary collaborations of the four other SecHuman Tandems were often talked about in the PhD programme as 'less close'. This meant that the research was not combined to provide answers to one shared, pre-defined question, nor to solve one and the same problem. Instead, the Tandems' two teams had each their disciplinary approaches and each their own concepts, empirical objects and research questions. Each Tandem worked under a shared headline (digital forgetting, privacy and human rights, surveillance, and corporate IT-Security), and met regularly to discuss their work, but did not feel the urge to be epistemically accountable to the Tandem partner team. Nor did the exchanges have effects on the ontological logic in terms of introducing novel concepts, problems or research questions.

The analogy of a Tandem bicycle indicates two persons driving in the same direction, both putting force into the shared course and both contributing to keeping the balance, while only one is steering. This image resembles best what Barry and Born call the subordinate-service mode of interdisciplinarity. Although some Tandems were designed in a subordinate-service mode, the tandems quickly outgrew this relationship.

The mode of interdisciplinarity we observed was thus different to Barry and Born's three modes. For this reason, we have added a mode to the typology. Peter Galison's [14] notion of *trading zone* proved helpful to understand the collaboration in the 'less close' Tandems. We coin it a *trading mode* of interdisciplinarity. Galison developed the metaphor of trading in his analysis of collaboration practices across different paradigms of physics. He observed that scholars would find norms, rituals and vocabulary for collaborating, although they never fully understood each other's areas of study. Trading zones are not specific to physics. They are often formed in interdisciplinary collaboration, regardless of the participating disciplines. The 'less close' Tandems created such trading zones in which collaboration from the two disciplines would find modes of exchange. However, also the other Tandems used these formats for exchange to 'trade' between their works. Some disciplines traded their desire for extending empirical areas and tools, others used the Tandems for less binding trading of ideas. For all, the Tandems allowed interdisciplinary exchange while not intervening into their ontological logic and epistemic commitments.

The trading mode of interdisciplinarity was accompanied by a specific rendition of disciplinarity: Disciplines were considered territories with permeable boundaries, allowing new objects and tools to enter the discipline. The characteristics of disciplines as trading with each other, but not allowing interventions into their ontological logic, was supported by the condition that each PhD

Table 2: Trading Mode of Interdisciplinarity

Format	Mode of Interdisciplinarity	Mode of Disciplinarity	Logic of Accountability	Logic of Innovation	Logic of Ontology
Tandem	Trading	Territory with Permeable Boundaries	Accountability to own Discipline	Desires for New Empirical Objects/Tools	Disciplinary Positioned Exchange with Other Disciplines

Tandem partner would graduate in their own discipline. The trading mode enabled Tandem Partners to engage in a bounded interdisciplinarity that could be kept afar from their own discipline. There is a need to study the effects of the interdisciplinary Tandem format in contexts that are not subjected to such disciplinary constraints on its outcome, but allow interdisciplinary PhD theses. The interdisciplinary logics of accountability, innovation, and ontology may in these cases overspill the trading zones into the final outcome. Table 2 summarises the logics of interdisciplinarity in the trading mode of interdisciplinarity that was characteristic to the Tandems formats.

As we shall discuss below, the bounded interdisciplinary productivity of the Tandem format did not mean that no further interdisciplinarity was produced in the PhD programme. Other formats were involved and contributed to interdisciplinarity.

4.2 Choice Mode of Interdisciplinarity

Colloquia, lectures and summer schools are formats that are common in academic settings. While they were designed to serve exchange within disciplines, they are also well-known across disciplines. In the following, we analyse what logics of accountability, innovation and ontology they brought forward for interdisciplinary cybersecurity in SecHuman, and suggest they realised interdisciplinarity in a mode of choice.

4.2.1 Weekly Colloquium. While the Tandems were mainly helpful for connecting pre-established disciplinary competencies in pairs, the whole group of thirteen PhD students met once every week in a colloquium in which the student presented their research. The weekly colloquium was the main format that allowed PhD students insights into each other's work across the Tandems. The frame of this format was pre-set and provided only limited opportunity for variation: Students gave a 20-minute presentation of their work in a lecturing or "broadcasting" [35] style, followed by questions. Despite the extreme differences between the disciplines, everyone was familiar with this format, and they all knew very well the possible roles of the ritual and how to fill them. Although the PhD students made a large effort during their presentations to address listeners from other disciplines, it quickly became a characteristic of the Colloquium that most listeners understood very little of the presented content. However, speakers and listeners were accountable to the format and to conducting the ritual correctly. Doing so generated a confident social space in a group characterised by difference. In disciplinary settings where speakers and listeners share vocabulary and epistemic commitments, the colloquium format was a space in which the value of their utterances was put to the test for speakers, where they were required to be accountable to the listeners. The weekly colloquium created social events where academia was done together, but where there was no expectancy of accountability to the epistemic commitment of PhD students from another discipline and novel ontological effects were unlikely to occur.

4.2.2 Dummy Lectures. PhD students' difficulties in understanding the others' work across disciplines came as no surprise. Because unfamiliarity with other disciplines was expected, the programme chairs had devised the lecture series "social science and humanities for engineers" and "IT-security for social scientists and humanities." These soon became known among the students as "Dummy Lectures". The introduction to engineering and cryptography was taught by one professor and distinctly focused on cybersecurity problems. The instructors of the social science and humanities lectures changed, with a new discipline introduced nearly every week: law, psychology, media studies, science and technology studies, linguistic, pedagogics. The engineering lectures were problem oriented, taught cryptography skills and involved homework. The social science and humanities lectures were mostly conceptually oriented and involved discussion. The Dummy Lecture formats, more than anything, taught students the different practices, rituals and habitus of the disciplines. Compared to the Weekly Colloquia, the Dummy Lectures required of the students to be accountable to foreign disciplines, mostly in a subordinate-service mode of interdisciplinarity. This was particularly the case for the social science and humanities students, as they needed to pass an exam in cryptography at the end of term. This indeed made some students complain that cryptography was performed as a master discipline, to which they themselves were enacted as subordinates. And, more importantly, the separation of the PhD programme in two groups – one attending the engineering lectures, the other one attending the social science lecture – left it to students to find out how the other discipline could be a relevant contribution to their own discipline. In conversations, the PhD students did not express any ontological effects of the Dummy Lectures, or in other words, the Dummy Lectures performed cybersecurity in disciplinary ways as a matter of cryptography in engineering, and as debates in the humanities or social science. Their participation in the lectures had more the character of a tourist gaze [37] i.e., a distant and brief view of insulated events that remain with the spectator only as detached memories. Like tourists, the PhD students' visit to the other disciplines had neither accountability, nor ontological effects.

4.2.3 Summer Schools. The first of SecHuman's annual international Summer Schools was on usable security. As a field of study that involves user perspectives in the development of IT-security, the organisers imagined it could work well as a boundary topic [33] to which all the involved disciplines in the programme could relate. This was indeed the case, but it also turned out that while all students could relate superficially to the topic, no student could engage with it in-depth. The format that became an issue of debate for the students.

Table 3: Choice Mode of Interdisciplinarity

Format	Mode of Interdisciplinarity	Mode of Disciplinarity	Logic of Accountability	Logic of Innovation	Logic of Ontology
Colloquium, Dummy Lectures, Summer Schools	Choice	Self-sufficient, Integrating External Components Upon Choice	Accountability to Own Discipline	Distant Judging of Other Disciplines	Stabilise Own Discipline

The humanities and social science students found it surprising that instructors at the Summer School lectured for several hours every day without leaving time for discussion. When the second authors of this paper mentioned this observation to a mathematics professor during the Summer School dinner, he responded bewildered: "why would you want discussion?" He explained that it is common for mathematics conferences that only five to ten people in the audience can follow the explanations during the first minutes of the talk, and only one person might follow the argument until the end of the presentation. This answer points to two important insights: First, it confirms Barry and Born's emphasis that the imagery of disciplines as homogeneous is flawed. Disciplines are heterogeneous and contain marked differences, contradictions, and lack of mutual understanding. Secondly, disciplines organise their exchange in different ways. In social science and humanities, discussions of research presentations are core to scholarly culture. Scholars are expected to be able to relate to almost any topic in their (sub)discipline, also those of which they are not experts. This explains well why scholars of the social science and humanities' Dummy Lectures all focussed on the disciplines' basic concepts and methods. These connect different topics and research areas within the discipline, and enable scholars to engage in discussions outside of their own narrow area of expertise, as well as they shape their desire. While the basics of computational models were also a topic in the Dummy Lectures of engineering, the specificities of cryptography were given more weight.

This brief detour back to the Dummy Lectures emphasises how different formats for scholarly exchange shape scholarly desires and criteria for assessing scientific work. This necessarily gives rise to disconcertment [38] in interdisciplinary exchange. In relation to the Summer School, this led PhD students to advocate for changes. The second Summer School thus involved more and different topics and included more discussion. While this was highly appreciated, the PhD students still found that the Summer School dealt too remotely with the approaches and topics of their interests. Accordingly, the organising of the third Summer School in 2019 was allocated to the PhD students. They gathered in smaller groups of neighbouring disciplines, of which each organised one day of the Summer School. This included a wider range of formats, such as discussion rounds, hands-on exercises and group work in addition to traditional lectures.

Which mode of interdisciplinarity was realised through the Colloquium, the Dummy Lectures and the Summer Schools? These three formats were less engendering collaboration than serving as platforms offering curated insights into established disciplines. As platforms of broadcasting [35] the formats did not change students' primary accountability to their own disciplines. Whatever they heard or learnt in the Colloquium, the Dummy Lectures and the Summer School, could only mobilise desires and epistemic curiosity, if it could be transferred or translated into the vocabulary and commitments of each individual students' home discipline. For each of the students of different disciplines, this was obviously only possible a very limited part of the time, which gave rise to dissatisfaction and frustration around the Summer School participants. The Colloquia, Dummy Lectures and Summer School formats all presented themselves as offers from the different disciplines. The participants' chance of intervening into and challenging their disciplinary informed research questions, methods, basic assumptions and commitments was minimal.

Even though the format of researchers presenting their work verbally to others in lectures was more suitable for scholars of the same (sub)discipline, the format is widespread in interdisciplinary exchange. Yet, this format is not covered by any of Barry and Born's modes of interdisciplinary work. The mode of interdisciplinarity of the Colloquium, the Dummy Lectures and the Summer Schools resonates better with Mol's [27] work on the logic of choice. We accordingly term the mode the *choice mode*. The choice mode implies presenting a phenomenon – in this case, different approaches within cybersecurity – as an offer. The ones to whom an approach is offered can make an individual choice to accept the offer and include the ideas of the approach in their own work, or refrain from including them.

It involves a lot of investment to make people commit to offers, such as going to a Colloquium every week, attending to Dummy Lectures for an entire semester and sitting in on Summer Schools for a whole week and listening to a large bouquet of different topics. These arrangements invite the shaping of scholarly subjectivities that judge individually and choose selectively, and who have the desire and will to choose for themselves among the goods on offer. Consequently, it yields a commitment of cybersecurity to optional approaches, models and vocabularies for scholars to choose between. If someone rejects the offer of one discipline, then he or she is simply not considered this discipline's target audience. In the choice mode scholars can opt in or opt out, but they cannot intervene or engage in what Barry and Born [3] call the logic of ontology: the questions asked, the objects attended to, and the relations generated by the different approaches. These remain within the disciplinary realm and out of reach for other disciplines.

The choice mode of interdisciplinary shapes separate approaches to cybersecurity as optional and as a matter of disciplinary informed individual choice, rather than turning interdisciplinarity into a collective endeavour, which we shall return to below. Scholars' desires and accountabilities remain directed towards their own disciplines, and their attitudes towards the other disciplines are characterised

by distant judging observation [35]. Table 3 summarises the logics of interdisciplinarity in the *choice mode* of interdisciplinarity that was characteristic to the Colloquium, Dummy Lectures and Summer School formates.

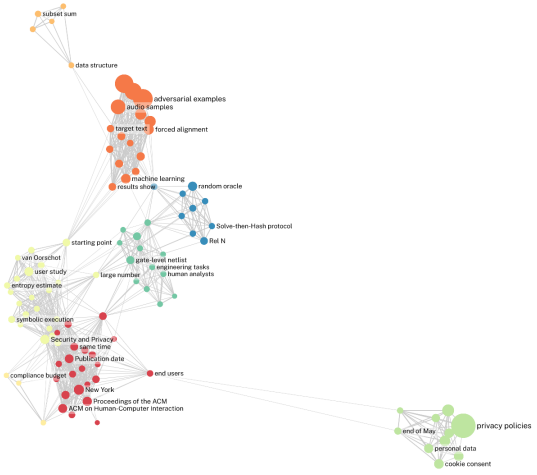
4.3 Agnostic-Antagonistic Mode of Interdisciplinarity

4.3.1 Lab Visits. After two years of sharing the discussed interdisciplinary spaces the group of PhD Students in the programme had come to know each other well and they formed a small community. However – or maybe for this reason – some of the students wished to get beyond the broadcast-like formats of the choice mode. A shift in the interdisciplinary formats was desired as students began organising what they called "Lab Visit", physical tours through each other's offices, workstations, labs, or archives. During the Lab Visits, students presented their work in their own offices and labs surrounded by the machines, instruments, papers and books they worked with on a daily basis. This brought the scholars in touch with the actual practices of each other's research rather than only with concepts, approaches or graphs of technological functions represented on slides or blackboards. Interestingly, when discussing this new format, some students argued that their own workplaces were considerably dull and there would be "not much to see", for instance on a cryptographer's desk. Visits to their offices, however revealed that in their daily practice the cryptographers worked intensely with whiteboards and that their offices were covered with sketches, calculations and working devices, which were surprising to the scholars of the other disciplines. The Lab Visits opened up for new opportunities to engage with the other disciplines in new ways and to contextualise the many presentations they had heard and seen. The disciplinary devices and work practices provided insights into the building blocks, tools or mediators of the disciplines, thus unravelling and demystifying the construction process of the other disciplines' knowledge [20, 22]. This is important, since knowledge about such devices, techniques and practical activities are key aspects of the professional vision [16] that disciplinary experts apply to understand each other's work. Providing access to the components of professional vision – such as devices, techniques and practical activities – enable non-experts an entrance into accessing and understanding other disciplines' work.

4.3.2 Shut-Up-And-Write. The Shut-Up-And-Write format which was initiated by the PhD students aimed at enabling them to experiment with transparency of writing procedures as an additional mode of interdisciplinary encounter. The format was inspired by the advice platform The Thesis Whisperer [3]. Once a week a group of students met in a lounge room in the Faculty of Social Science to work individually on their writing projects (papers, dissertations, data analysis, etc.). The Shut-Up-And-Write sessions started with a brief round of everyone explaining what they would be writing that day. This was documented on a whiteboard or flipchart to generate a visual map of the group's (i.e., not purely individual) work. The writing periods were designed in rhythms of silent writing and time for breaks and chats. The weekly Shut-Up-And-Write meetings offered a different engagement with each other's work by uttering and listening to concerns and challenges related to writing.

4.3.3 Discussion of Network Graph. This format was less of a routine activity. Towards the end of the third year of the programme, the authors of this article organised a one-day workshop on interdisciplinarity. We report here from this Participatory Workshop that took place after an introductory keynote on interdisciplinarity by Andrew Barry. The workshop started out with the authors of this article presenting a semantic network graph of in total 16 English language publications on cybersecurity written by the programme's members (although some co-authors had other affiliations). The semantic-analysis tool CorText Manager was applied to create an image of the interconnection of the 100 semantic units that across the articles were most frequently used (filtered for non-semantic terms). CorTexT Manager does not only identify terms but automatically identifies and differentiates between semantic units. Instead of just identifying the term "algorithm", for instance, it looks for semantic units such as "problem solving algorithm". Instead of identifying "security" it differentiates between "security system", "security paradigm", "usable security", etc. Subsequently, the programme analyses co-occurring semantic units, which are understood as two semantic units that appear in the same paper. Whenever two of the 100 most frequently used semantic units are found in one and the same paper, they are represented as points (a knot) in the semantic web connected by a line (an edge). The distance between two connected knots represents the frequency of the co-occurrence of the two semantic units in one paper relative to the co-occurring of other semantic units (closer is more frequent co-occurrence, father away is less frequent co-occurrence). The analysis furthermore divides the clusters of co-occurring semantic units into 'communities', which are a collection of co-occurring semantic units that relate more often to each other than to other collections of co-occurring semantic units [19]. Figure 1 reveals

Figure 1: Network Graph of Publications



[3] https://thesiswhisperer.com/

Table 4: Agonistic-Antagonistic Mode of Interdisciplinarity

Format	Mode of Interdisciplinarity	Mode of Disciplinarity	Logic of Accountability	Logic of Innovation	Logic of Ontology
Shut-Up-And-Write, Lab Visits, Network Graph Discussion, Scenario Exercise	Agonistic-Antagonistic	Situational Transdisciplinarity	Situational Accountable to Shared Commitments	Desire for Collective Engagement	Commitment to View Own Disciplinary Ontology from the Others

seven communities in the publications analysed, each presented in a different colour.

The visualisation suggests seven discoursive areas, five of which have very limited connections. At first, this result seemed disappointing, as the whole idea of the programme was to collaborate across disciplines. However, the graph facilitated a discussion among the group whether it was even desireable to develop a shared vocabulary, thereby commensurating the displayed differences in the field. It could be equally valuable, they contended, to maintain some differences in order to actively question and develop one's own disciplinary commitments. The visualisation therefore aided in honing reflexive abilities in the scholarly group. More than representing the group in a concluding way, the graph gave rise to new and different conversations among the interdisciplinary partners about their own work. One professor of engineering, for instance, had always seen the social sciences and humanities as peripheral to cybersecurity, which is also the case if one counts the number of publications on this topic. However, the visualisation shows cryptography as rather unrelated to the other fields (upper left community). The discussion provided a new perspective on the disciplines' relations in the fields. Not only due to the results did the visualisation become a means for interdisciplinary exchange.

The graph, furthermore, reveals an important condition of academic work: Our primary results are peer-reviewed articles published in highly specialised journals. Specialisation of academic fields develops through a process of differentiation of discourse [25], and thus of semantic units. This makes it more difficult to shape cybersecurity as an interdisciplinary field, since outlets for interdisciplinary and thus less specialised publications are rare. The display of relations between semantic units rendered the effects of the publication landscape visible and debatable in the group. The visual language was new to the disciplines present, which required the programme's members to leave their individual disciplinary vocabularies behind, and engage collectively in a discussion of the interdisciplinary character of cybersecurity research.

4.3.4 Scenario Exercise. The second section of the workshop was a Scenario Exercise. The scenario presented to participants described a fictive situation in which all research data in SecHuman should be shared. Participants of the workshop should now map the process of establishing a collaborative platform for shared data. It was not determined whether this platform should be digital or analogue, neither what research data encompassed nor how access control should be managed. It was up to the participants to discuss their data and their concern about sharing and about storage, how data could be shared, what sharing mechanism they could imagine, etc. The interdisciplinary groups were asked to map the process of how they would decide on a system, as well as mapping the system themselves. The organizers hoped that this Scenario Exercise would transpire both disciplinary data practices, multiple security definitions, and discussions of how to combine them.

A0 paper sheets and coloured markers were handed out to the participants. The mappings were made in four groups of five to six members from different disciplines and across status groups. Each solved the task in very different and fascinating ways that we cannot do justice to in this paper. For this paper, the most interesting insight from the scenario exercise was the ways it worked as a format for interdisciplinary exchange: In one group, participants first discussed what kind of data they would need to store in the data base and who should have access to those data. This opened a conversation through which the participants revealed for each other what for them counted as data. For some, data was spreadsheets with numerical measurements from an experiment. Another explained that her data mainly consisted of large numbers of published texts – either scientific or journalistic – with her added notations, excerpts and memos. Yet others would not even consider their research to involve data, as all they dealt with were calculations. Of this conversation, a discussion started over what could be made accessible to Tandem partners, to the whole PhD programme and to which additional external publics. Depending on the notion of data, the data publics varied, which made the question of how to structure a data base rather challenging. Luckily, the building of databases was not the actual aim of the Scenario Exercises; the generation of interdisciplinary conversations was. Scholars who had worked next to each other for three years suddenly came to understand details about the others' approaches, such as what counted as data and what consequences these definitions had. They came to view their own data from the perspectives of the others.

Another group tried to implement data protection laws into their scenario, and encountered a dilemma between centralising access – which was required from a legal perspective – and allowing free flows of data between the scientists, which would be the preferred solution of cryptographers. The group ended up laughing about their idea to give the head of the PhD programme the only key to a safe room for the PhD programme's shared database in the basement of the university campus. The laughing alluded to the fact that it was impractical to implement data protection laws in this way when trying to facilitate access. A negotiation was needed of security in the sense of the law scholars, and security in the sense of safe access.

Several aspects of the Lab Visits, the Shut-Up-And-Write sessions, the Discussion of the Network Graph and the Scenario Exercise resonate with Barry and Born's agonistic-antagonistic mode of

interdisciplinary work. First, they engendered a confrontation of different paradigmatic commitments in cybersecurity and were characterised by a probing and experimental attitude towards the object of inquiry that should be explored in cybersecurity. They were all exploratory formats, which may have added to their agonistic character, and none of them aimed towards overcoming the exploratory character. Secondly, the formats presented in this section all unfolded a collective ethics. Different from the choice mode, which left it to the individual scholars to choose among logics of cybersecurity ontology, and different from the Tandems that were either based on a clear division of labour or a trading zone that did not interfere with the disciplinary commitments, the driving force of these formats was a shared concern about cybersecurity research as a collective endeavour. That cybersecurity was conducted as a collective endeavour resonates with an additional, third aspect of Barry and Born's agonistic-antagonistic mode of interdisciplinary work, which is its transdisciplinary character. In a transdiscipline different disciplines do not come together to exchange while retaining their disciplinary identity and commitments. Instead, they establish new engagements that differ from commitments of each of the original disciplines, or, put differently, they become antagonistic towards own disciplinary convictions. However, the three formats discussed did not aim to establish a new transdiscipline in Barry and Born's sense. Rather, the formats generated a *situational transdisciplinary sensitivity* by attending in singular but repeated situations to aspects of each discipline, whose relevance was so obvious to members of the disciplines themselves that they mostly went unnoticed by them, suggesting there would be "not much to see". The external view of members from the other disciplines came to invite scholars to notice and reflect their own approaches, which made their logic of ontology accessible for discussion and revision in the interdisciplinary community.

Contrary to the formats of interdisciplinarity discussed in the previous sections, the transdisciplinary character of the Lab Visit, Shut-Up-And-Write, Network Graph Discussion and Scenario Exercise intervened into the logic of ontology of cybersecurity, i.e. into the disciplines' articulation of their object of inquiry. Yet, the formats were all modest interventions and none of them had the thrust to turn participants away from their disciplines, nor did they aim at this. But they did accomplish to generate situations of *critical proximity* [21]. Birkbak et al. [5] suggest this term to describe engagements that interrupt and disturb commitments — a virtue of interdisciplinarity in Stubbe's [34] terms. Different from a point of critique towards other disciplines that is distant and non-accountable, these interdisciplinary gatherings create co-ownership of a new and emerging logic of ontology, of the object of inquiry and of relevant problems thus evoked. Moments were created in which new shared questions about how to deal with and relate through cybersecurity research could be imagined or maybe even initiated. The formats discussed in this section generated a *situational accountability* that was directed towards the formats rather than towards the individual disciplines. The success of the Lab Visit, the Shut-Up-And-Write sessions, Network Graph Discussion and Scenario Exercise depended upon the participants being accountable to each other by opening up [24] their own disciplinary commitment to new perspectives. The Shut-Up-And-Write sessions were more of a shared moment of work; it was also about sharing perspectives on cybersecurity.

Even more than the other formats the formats discussed in this section suggested an ethics of care, which Mol [27] in opposition to the ethics of choice understands as generating relations and shared situational accountability rather than individual responsibility. In the third mode of interdisciplinarity we observed – the antagonistic-agonistic mode – desires were cultivated that imagined cybersecurity as a joint endeavour and communal ongoing challenge. Table 4 summarizes this mode of interdisciplinarity.

5 DISCUSSION

We have applied Barry and Born's [3] typology of modes and logics of interdisciplinarity to analyse eight formats for interdisciplinary collaboration in the PhD programme. In this section, we discuss the extension of this typology for cybersecurity.

5.1 A Typology for Modes of Interdisciplinarity in Cybersecurity

Much of existing literature on interdisciplinarity as practice stems from collaborations in the area of sustainability and environmental sciences (including Barry and Born's vocabulary). An analysis of the collaborations currently present in cybersecurity research, therefore, requires an adaptation of this literature. We have analysed the following modes of interdisciplinarity in cybersecurity: trading mode, choice mode and agonistic-antagonistic mode. Aspects of the subordinate-service mode and the synthetic-integrative mode were also observed, and accordingly, we find it necessary to include them in a typology for modes of interdisciplinarity in cybersecurity. Table 5 summarizes the five modes of interdisciplinarity in cybersecurity we observed in our case. It allows comparing the modes according to how much scholars' disciplinary logics of accountability, innovation, and ontology become entangled with the logics of other disciplines. The logics are less entangled at the top of the table, and more entangled towards the bottom. This scale of interdisciplinary entanglements is multi-dimensional, meaning that a mode at the top of the table does not just have "less of the same" interdisciplinarity than those at the bottom. As accounted for above, the modes are qualitatively different. Although in different ways, it is possible to identify some modes as entangling different disciplines more than others. As discussed in the ethnographic analysis, different modes of interdisciplinarity are combined and co-exist. The typology emphasises that a commitment to one's own discipline is combinable with engaging in modes of interdisciplinarity. The Tandem format proved to be flexible, realising different modes of interdisciplinarity, while the more traditional formats of interdisciplinary revealed less interdisciplinary entanglement. It is worthwhile noting that the agonistic-antagonistic mode of interdisciplinarity, which we have observed the most to entangle different disciplines, purchases interdisciplinarity only in bounded situations. As interdisciplinarity becomes more common in cybersecurity, we expect it to be possible in the coming years to extend this typology to add modes of interdisciplinarity that are more permanent. The typology offered here can serve as a orientation for which parameter to consider when developing new formats for interdisciplinarity in cybersecurity.

Table 5: Typology of Interdisciplinarity in Cybersecurity

Mode of Interdisciplinarity	Mode of Disciplinarity	Logic of Accountability	Logic of Innovation	Logic of Ontology	Interdisciplinary Format
Choice	Self-sufficient, Integrating External Components upon Choice	Accountable to Own Discipline	Distant Judging of Other Disciplines	Stabilise Own Discipline	Colloquium, Dummy Lectures, Summer Schools
Synthetic-Integrative	Well-defined own Area, Co-operable with Others	Accountable to Own Discipline	Exchange with Other Disciplines	Stabilise own Discipline	(Tandems)
Subordinate-serving	Independent, Complementing Other Disciplines	Accountable to Own and Serviced Discipline	Expand or Curtail Object of Desire	Stabilise Own Discipline	(Tandems)
Trading	Territory with Permeable Boundaries	Accountability to Own and Trading Discipline	Desires for New Empirical Objects/Tools	Disciplinary Positioned Exchange with Other Disciplines	Tandems
Agonistic-Antagonistic	Situational Transdisciplinarity	Situational Accountable to Shared Commitments	Desire for Collective Engagement	Commitment to View Own Disciplinary Ontology from the Others	Shut-Up-And-Write, Lab Visits, Network Graph Discussion, Scenario Exercise

5.2 Informality of Interdisciplinarity in Cybersecurity

It is important to emphasise that none of the formats were through and through, purely nor homogeneously corresponding to one specific mode and one specific logic of interdisciplinarity. While all the modes and logics we described above were observed and fitting to the formats, the modes are more dynamic in practice than a typology tends to suggest. The analyses showed how the Weekly Colloquia, the Summer Schools and the Dummy Lectures were occasions for very low degrees of interdisciplinarity in the choice mode. However, the frequency and repetition of these formats meant that the scholars got together very often, they came to know each other well and cared for each other and the group. The effect of such frequent encounters need to be documented in a longer-term study. Given the very specialised character of academia, scholars mostly encounter people from their own and related areas of studies and also privately tend mainly to come together with people from this rather homogeneous community. In this light, it is worth pointing to how often cryptographers, legal scholars, social anthropologists, mathematicians, media studies scholars, etc. were joined together in conversations in the PhD programme. In the current state of cybersecurity, which is characterised by many different disciplines being involved, but each remaining primarily accountable to their own disciplines, the plain existence of formats for encounters may be crucial for other logics of accountability, innovation, and ontology to emerge in cybersecurity. It may well be the situational accountability and commitment to other disciplines that were observed in the agonistic-antagonistic mode of interdisciplinarity that serve as fertile ground for more durable interdisciplinarity to develop.

5.3 Language and Interdisciplinarity

In the current situation of extreme heterogeneity of different disciplines in cybersecurity and the thus variety of disciplinary vocabularies, it is interesting to notice that scholars of cybersecurity interdisciplinarity (e.g. [29, 30]) often emphasise the need for a shared language. Our analysis suggests that this proposal ignores the logic of scientific specialisation. A shared vocabulary would imply a shared way of thinking about cybersecurity, and thus a lack of specialisation. This would not promote new ideas in cybersecurity research; it more likely would reduce innovation. Particularly our discussions of the agonistic-antagonistic formats pointed to the value of differences in interdisciplinary cybersecurity. During the Lab Visits, in the Discussion of Network Graphs as well as in the Scenario Exercise it was the encounter between different ontological logics that made scholars notice the specificities of practices and perspectives in their own disciplines, which they had not prior paid attention to. While all the other modes of interdisciplinarity focussed on how individual disciplines could engage with the *other* disciplines either through trade or through choice, the antagonistic-agonistic mode attends to how disciplines come to notice their own disciplinary logics. While we cannot determine whether these discoveries had durable effects on disciplinary commitments, we can maintain that it was the differences in logics that enabled the disciplines to recognise their own work in new and potential innovative ways through the views of the others. Based on this, our suggestion is not to attempt to develop a shared vocabulary for cybersecurity but rather to develop formats that provoke disciplines to notice the specificities of their own commitments and thus make it available for potential reflection, discussion and innovation.

Galison notes with reference to interdisciplinary work in physics, that "cultures in interaction frequently establish contact languages, systems of discourse that can vary from the most function-specific jargons, through semi-specific pidgins, to full-fledged creoles rich enough to support activities as complex as poetry and metalinguistic reflection" [14, p. 783]. The notion of "Dummy Lectures" is one example of a functional-specific jargon developed in the PhD programme, which different from the originally disciplinary titles of the lectures pointed to a shared and genuine transdisciplinary experience. For cybersecurity to develop in a more inter- and transdisciplinary direction, it may be helpful to cherish the pidgins and

creoles that are developed and support their stabilisation, and not aim for a purified shared language.

6 CONCLUSION

Interdisciplinarity in cybersecurity, as in other fields, is highly demanded by funding agencies and political actors. However, so far, exchange on the practical formats through which different modes of interdisciplinarity are accomplished is scarce. And, possibly more severely, it is unclear what is meant when evaluating whether interdisciplinarity was "accomplished". This paper has offered a vocabulary, in the form of a typology of interdisciplinary modes, that can be utilized when attempting to define *what mode of interdisciplinary encounter* is desired in a project, and, as we argued, subsequently *what mode of cybersecurity* is studied.

We opened this paper with the aim to understand how interdisciplinary practices shape cybersecurity. Searching the literature, we found only few titles that deal with the interdisciplinary character of cybersecurity research. The existing works state the heterogeneity and breath of research into cybersecurity, including computer science, mathematics, engineering, psychology, law and political and social science. Both Ramirez [29, 30] and Choras [8] develop models for interdisciplinary cybersecurity. These models, however, are not based on empirical studies of how interdisciplinary work in cybersecurity unfolds in practice. A step to fill this research gap has been taken with this article, and the beginning of a typology for modes of interdisciplinary cybersecurity has been developed, which points to how logics of interdisciplinarity are shaped and combined in different ways through different practical interdisciplinary collaboration formats.

Our analysis above and the typology suggested reveal cybersecurity as a heterogeneous field in which many different disciplines come together. Most often, the disciplines are committed to the logics of their own discipline, be it cryptography, social anthropology, psychology, linguistic, or other. Our discussion pointed to the informality and the situated and temporary character of the transdisciplinary commitments in cybersecurity. The heterogeneity of the results points to the scholars in the cybersecurity case study having many different interdisciplinary commitments. It suggests interdisciplinary modes in cybersecurity to be less of long-term marriages to a single other discipline, and more of a promiscuous and temporary sharing across many disciplines. Our study of interdisciplinary practices in cybersecurity shows that scholars engage both in parallel and at different points in time in many different formats and different kinds of exchanges. This may be the beginning of new shared logics in cybersecurity. But it may also be a stable condition of multiple logics and commitments to home disciplines, to "master" or "subordinate" disciplines, to disciplines with which trading unfolds, disciplines to choose between, transdisciplinary situations, etc. Time will show, whether cybersecurity develops into a single transdisciplinary paradigm, or indeed into a dynamic post-disciplinary field of exchange.

In this exciting stage of development of interdisciplinary cybersecurity, we can maintain on the basis of our analysis that formats for developing local pidgin or creole languages and practices for translation and trading between disciplines can come to take the shape of either the problem-solving Tandems or of the agonistic-antagonistic interdisciplinary formats. The accountability and commitment of the choice mode formats are too strongly bound to the individual disciplines and too strongly generating distant observing subjectivities to provide opportunity for developing local languages.

There is no doubt that cybersecurity research is an interdisciplinary endeavour, and the question of how to collaborate interdisciplinarily will remain a challenge the years to come. This is the case for scholars learning to engage in different formats and different modes of interdisciplinarity. But it is also a challenge for universities to introduce interdisciplinary degrees, and for funding associations and publication venues that often assess application and publications according to one discipline, thus giving interdisciplinary research less chances. Alongside other interdisciplinary cybersecurity research groups, SecHuman has offered an important step towards establishing different modes of interdisciplinarity in the field. It has not only experimented with different formats of interdisciplinary work, it has also allowed a case analysis such as the one presented in this articles on the practices of how to do interdisciplinarity. Interdisciplinary cybersecurity work is strongly needed and accordingly, we need more empirically based insights into the practices of how to conduct interdisciplinary work.

ACKNOWLEDGMENTS

This work was supported by the federal state of North Rhine-Westphalia, Germany. We thank our colleagues and friends in SecHuman for engaging in lengthy discussions about interdisciplinarity, and for allowing us to observe and analyse their practices. We are indebted to the diligent work of our reviewers and shepherds, as well as all to all participants of NSPW'23. We acknowledge that the preparation and writing of academic articles consume earthly resources.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Andrew S. Balmer, Jane Calvert, Claire Marris, Susan Molyneux- Hodgson, Emma Frow, Matthew Kearnes, Kate Bulpin, Pablo Schyfter, Adrian Mackenzie, and Paul Martin. 2015. Taking Roles in Interdisciplinary Collaborations: Reflections on working in Post-ELSI Spaces in the UK Synthetic Biology Community. *Science and Technology Studies* 28, 3 (1 Dec. 2015), 3–25.

[3] Andrew Barry and Georgina Born. 2013. *Interdisciplinarity: Reconfigurations of the Social and Natural Sciences.* New York, NY: Routledge.

[4] Mathieu Bastian, Sebastien Heymann, and Mathieu Jacomy. 2009. Gephi: An Open Source Software for Exploring and Manipulating Networks. *Proceedings of the International AAAI Conference on Web and Social Media* 3, 1 (Mar. 2009), 361–362. https://doi.org/10.1609/icwsm.v3i1.13937

[5] Andreas Birkbak, Morten Petersen, and Torben Elgaard Jensen. 2015. Critical Proximity as a Methodological Move in Techno-Anthropology. *Techné: Research in Philosophy and Technology* 19 (04 2015), 266–290. https://doi.org/10.5840/techne201591138

[6] Philippe Breucker, Jean-Philippe Cointet, Alexandre Hannud Abdo, Guillaume Orsal, Constance de Quatrebarbes, Tam-Kien Duong, Cristian Martinez, Juan Pablo Ospina Delgado, Luis Daniel Medina Zuluaga, Diego Fernando Gómez Peña, Tatiana Andrea Sánchez Castaño, Joenio Marques da Costa, Hajar Laglil, Lionel Villard, and Marc Barbier. 2016. *CorTexT Manager.* https://docs.cortext.net

[7] Johannes Busse, Bernhard Humm, Christoph Lubbert, Frank Moelter, Anatol Reibold, Matthias Rewald, Veronika Schlüter, Bernhard Seiler, Erwin Tegtmeier, and Thomas Zeh. 2015. Actually, What Does "Ontology" Mean? A Term Coined by Philosophy in the Light of Different Scientific Disciplines. *Journal of Computing and Information Technology* 23 (01 2015), 29. https://doi.org/10.2498/cit.1002508

[8] Michal Choraś, Rafal Kozik, Andrew Churchill, and Artsiom Yautsiukhin. 2016. *Are We Doing All the Right Things to Counter Cybercrime?* Springer International Publishing, Cham, 279–294. https://doi.org/10.1007/978-3-319-38930-1_15

[9] Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, and National Academies of Sciences Engineering and

Medicine. 2017. *Foundational Cybersecurity Research.* National Academies Press, Washington, D.C., DC.
[10] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Emploring Privacy and Security as Social and Cultural Phenomena. 21, 3 (sep 2006), 319–342. https://doi.org/10.1207/s15327051hci2103_2
[11] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Pers. Ubiquitous Comput.* 8, 6 (2004), 391–401. https://doi.org/10.1007/s00779-004-0308-5
[12] Andrew C Dwyer, Clare Stevens, Lilly Pijnenburg Muller, Myriam Dunn Cavelty, Lizzie Coles-Kemp, and Pip Thornton. 2022. What Can a Critical Cybersecurity Do? *International Political Sociology* 16, 3 (07 2022). https://doi.org/10.1093/ips/olac013 arXiv:https://academic.oup.com/ips/article-pdf/16/3/olac013/45054045/olac013.pdf olac013.
[13] Ulrike Felt. 2017. *Responsible Research and Innovation.*
[14] Peter Galison. 1997. *Image and Logic: a material culture of microphysics.* University of Chicago Press, Chicago, IL, USA.
[15] Daniel E. Geer, Kevin Soo Hoo, and Andrew Jaquith. 2003. Information Security: Why the Future Belongs to the Quants. *IEEE Secur. Priv.* 1 (2003), 24–32.
[16] Charles Goodwin. 1994. Professional Vision. *American Anthropologist* 96, 3 (1994), 606–633. https://doi.org/10.1525/aa.1994.96.3.02a00100
[17] A. Grunwald. 2011. Responsible innovation: bringing together technology assessment, applied ethics, and STS research. *Enterprise and work innovation studies* 7 (2011), S.9–31. 48.02.01; LK 01.
[18] Martyn Hammersley and Paul Atkinson. 1983. *Ethnography: Principles in practice.* Taylor & Francis, London, England.
[19] Torben Jensen, Anne Katrine Hansen, Stanley Ulijaszek, Anders Munk, Anders Madsen, Line Hillersdal, and Astrid Jespersen. 2018. Identifying notions of environment in obesity research using a mixed-methods approach. *Obesity Reviews* 20 (12 2018). https://doi.org/10.1111/obr.12807
[20] Karin Knorr-Cetina. 1981. *The manufacture of knowledge.* Pergamon, Amsterdam, Netherlands.
[21] Bruno Latour. 2004. Why Has Critique Run Out of Steam? From Matters of Fact to Matters of Concern. *Critical Inquiry* 30 (12 2004), 225–248. https://doi.org/10.1086/421123
[22] Bruno Latour and Steve Woolgar. 1986. *Laboratory life.* Princeton University Press, Princeton, NJ.
[23] John Law. 2004. *After method.* Routledge, London, England.
[24] Tobias Liebetrau and Kristoffer Kjærgaard Christensen. 2021. The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security* 6, 1 (2021), 25–43. https://doi.org/10.1017/eis.2020.10
[25] Niklas Luhmann. 2009. *Die Wissenschaft der Gesellschaft.* Suhrkamp Verlag, Frankfurt am Main, Germany.
[26] Leigh Metcalf and Jonathan Spring. 2021. *Using Science in Cybersecurity.* World Scientifc Publishing Co. Pte. Ltd.
[27] Annemarie Mol. 2008. *The Logic of Care: Health and The Problem of Patient Choice.* https://doi.org/10.4324/9780203927076
[28] Thomas Nagel. 1986. *The View From Nowhere.* Oxford University Press.
[29] Robert Ramirez. 2017. *Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization.* Ph. D. Dissertation. https://doi.org/10.13140/RG.2.2.27123.02081
[30] Robert Ramirez and Nazli Choucri. 2016. Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access* 4 (2016), 2216–2243.
[31] J.M. Spring and P. Illari. 2019. Building General Knowledge of Mechanisms in Information Security. *Philosophy & Technology* 32 (2019), 627–659. https://doi.org/10.1007/s13347-018-0329-z
[32] Jonathan M. Spring, Tyler Moore, and David Pym. 2017. Practicing a Science of Security: A Philosophy of Science Perspective. In *Proceedings of the 2017 New Security Paradigms Workshop* (Santa Cruz, CA, USA) *(NSPW 2017)*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3171533.3171540
[33] Susan Leigh Star and James R. Griesemer. 1989. Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science* 19, 3 (1989), 387–420. http://www.jstor.org/stable/285080
[34] Julian E. Stubbe. 2018. Innovationsimpuls „Integrierte Forschung".
[35] Estrid Sørensen. 2009. *The materiality of learning: Technology and knowledge in educational practice.* Cambridge University Press, Cambridge, England.
[36] Lucy Tsado. 2019. Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. 2019 (07 2019).
[37] John Urry. 1990. *The tourist gaze* (1 ed.). SAGE Publications, London, England.
[38] Helen Verran and Michael Christie. 2013. The generative role of narrative in ethnographies of disconcertment: Social scientists participating in the public problems of North Australia. *Learning Communities: International Journal of Learning in Social contexts* 12, April 2013 (2013), 51–57.
[39] Stefan Beck (verst.), Jörg Niewöhner, and Estrid Sörensen. 2012. *Science and Technology Studies.* transcript Verlag, Bielefeld. https://doi.org/doi:10.1515/transcript.9783839421062
[40] Rossouw von Solms and Johan F. Van Niekerk. 2013. From information security to cyber security. *Comput. Secur.* 38 (2013), 97–102.
[41] Daniel W Woods and Aaron Ceross. 2022. Blessed Are The Lawyers, For They Shall Inherit Cybersecurity. In *New Security Paradigms Workshop* (Virtual Event, USA) *(NSPW '21)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3498891.3501257