In search of new directions for cyber security advice



Mark Quinlan

Linacre College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity Term 2022

Abstract

Security researchers have expended significant effort on both creating cyber security advice, and how to best persuade users to follow it. But what exactly is this advice? What does it look like to these users? And why is it that once seen, some still require more persuasion to use it than others? But rather than focus on the user's mindset through qualitative studies, as many of our progenitors have done, this dissertation takes a different approach; we consider not merely the advice itself, but attempt to expand the environment around it, to see where and how such advice is seen, and where it is (or is not) applied. Our primary aim is to see how an investigation of these factors may lead to an improvement of security advice efficacy, and provide the first steps towards an alternative viewpoint for usable-security researchers. Therefore, we consider the following overarching research question:

> *How might cyber security advice be improved upon whilst keeping in mind the user's perspective(s) upon cyberspace?*

This dissertation presents three distinct major contributions, with each contribution informing the direction of the next. We believe this approach allows us to understand the *environmental* level, and drill down, first into the *epistemological*, then into the *phenomenological* area of security advice. In the first contribution we articulate the environment in which security advice is meant to be applied. To do so, we build a conceptual framework that describes 'cyberspace', through the use of metaphors from other fields with similar gaps between advice and practice. Subsequently, we report upon an agent-based experiment to ascertain the potential efficacy of these metaphors in a usable-security context. The second and third contributions both seek to gain a better perspective on how security advice disseminated through this environment is seen and consumed. In the second contribution, we assess one of the largest cyber security advice dissemination channels, the news media, for efficacy, using quantitative metrics to determine the efficacy of advice contained within them. For the third contribution we undertake a novel assessment of the non-verbal aspects of cyber security advice dissemination, with emphasis placed on how these aesthetics may aid or hinder the successful dissemination of cyber security advice to users.

Acknowledgments

Many people have contributed to this thesis. First and foremost, my deepest thanks go to my supervisor, Andrew Simpson, who has been a steadying hand throughout my DPhil journey. He provided not only invaluable guidance on the research itself, but also believed in my work when I needed it most, offering priceless support and wisdom on navigating life as a doctoral student. Without him, you would not be reading this thesis today, and for that I am eternally grateful.

I extend heartfelt thanks to my examiners. Prof Karen Renaud, whose seminal work in the field is heavily referenced throughout this thesis, graciously served as my examiner and continued to support my research thereafter. Prof Andrew Martin, the visionary leader of the CDT Cyber Security program, stood by me whenever my DPhil journey took unexpected turns. I'm also grateful to Ivan Fleshais, who examined me during my internal stages, and to Jun Zhao, who mentored me into becoming a researcher and co-authored my very first academic paper.

To my friends and colleagues, who have shared countless ups and downs with me over the years, I hope I have proven worthy of your friendship. Aaron Ceross, my co-conspirator throughout this DPhil, with whom I explored so many ideas yet never had enough time to pursue them all. Rebecca Buening, a kindred spirit who patiently transformed my spelling-riddled ramblings into eloquent prose with her masterful editing. Dennis Malliouris, who showed me the path to timely graduation. Tom Walsche, my office-mate who endured my ramblings and the only one with the patience to become my squash instructor. Nihil Shah, who became family during post-lockdown times, master-chef and whiskey connoisseur.

The optimistic spirits of Ursula Hicks House: Tommaso De Zan and Pink Kulthanan. Guanze and Qian He, who encouraged me to persevere. Prof Samar Khatiwala, who engaged me in stimulating debates across the UK and Japan while introducing me to the richness of Oxford college life. Frankie Wilson, my methodological mentor and the master-librarian. David Hobbs, the ultimate organiser during those first years who somehow managed to organise even me.

My gratitude extends to Graham Curtis, Olu Fasan, and José-Rodrigo Córdoba-Pachón, who encouraged me to begin this journey and provided vital early support. Lonie Sabagh, who consistently offered to review my work. Damon Williams, one of my longest-standing supporter, going back decades. Oscar Darwin, an office-mate who introduced me to some of Oxford's musical treasures. Ayumi Takenaka, the anthropologist who brought new perspectives. Tingting Zhu, who kept both Aaron and me in line while supporting us throughout. Adam Zibak, bop-specialist extraordinaire who introduced me to Oxford's finest party scene. Prof Charles Roehr, because we all have a SAAB-story. Klaudia Krawiecka, bop-specialist, Takuya Maede, who opened my eyes to new perspectives on ethics.

Jack Kenny, master of cyberspatial law, and Kevin Cheng, a fellow philosopher of automotive culture and life wisdom.

To my parents, to everyone at Linacre College, and to all my peers in CDT17—truly the best cohort one could ask for.

Finally, to my sister Gabriella Quinlan, who has traveled to be with me wherever I am, welcomed me home whenever I needed refuge, and supported me. And to Mariko Nakahara, my everything.

Contents

Bibliography **ix**

List of Figures **xi**

1 Introduction **1**
1.1 The research problem 2
1.2 Works arising from this research 7
1.3 Dissertation outline 8

2 Background and motivation **11**
2.1 Cyberspace: our virtual environment 11
2.2 Cyberspace safety & security 13
2.3 Usable security 14
2.4 Interacting in cyberspace 15
2.4.1 Individual users of cyberspace 15
2.4.2 Non-corporeal users of cyberspace 18
2.5 Cyber security advice 21
2.5.1 Who provides guidance into cyberspace? 21
2.5.2 How the user may learn this advice 22
2.5.3 Causal-efficacy 24
2.5.4 The expert 25
2.5.5 The efficacy potential of advice 27
2.5.6 Epistemic innocence and naïve advice 29
2.5.7 Incorporating risk when undertaking cognitive processes . . 30
2.6 The link between the learning of cyber security and cyber security aesthetics 31
2.6.1 Learning informally through media 31
2.6.2 Why aesthetics form an important field of study when analysing cyber security advice efficacy-potential 33
2.6.3 How aesthetics relate to the our specific study of news-based cyber security advice 34
2.7 Summary 35

3 Methodology **39**
3.1 The conceptual model 40
3.2 Empirical data collection and classification 42
3.2.1 Generating online-sourced news data 43
3.2.2 Classifying online-sourced news data 45
3.2.3 Generating online-sourced image data 47
3.2.4 Classifying online-sourced image-data 47
3.3 Summary 49

4 Cyberspace through the eyes of the user **51**
4.1 Building a conceptual model: Background 51
4.2 Cyberspace ecology 53
4.2.1 Epidemiological metaphors in cyber security 54
4.2.2 More-than-metaphorical commonalities 55
4.3 How individuals learn about cyber security in comparison with epidemiological threats 55
4.3.1 Similar failings in both advice types 56
4.4 A conceptual model for cyberspace 57
4.5 Providing evidence for our model through an experiment 62
4.5.1 Modelling the user actor 64
4.6 Interpreting our results 67
4.7 Discussion 71
4.7.1 Is cyberspace homogeneous? 72
4.7.2 Who has the agency to mitigate risk in cyberspace? 72
4.7.3 The impacts of self-efficacy when navigating cyberspace . . . 76

5 News-disseminated cyberspace advice **79**
5.1 The cyber security advice corpus 81
5.2 Results 82
5.2.1 CIS-vector occurrences 83
5.2.2 Articles containing no CIS-vectors 85
5.2.3 Sentence length and vocabulary size 86
5.2.4 Readability scores 87
5.2.5 Sentiment analysis 89
5.3 Discussion 90
5.3.1 What kind of informally learnt and actionable security advice most often appears in news articles? 90
5.3.2 What is the efficacy potential of this security advice as consumed by an individual user? 92
5.4 The phenomenological aspects of cyber security advice dissemination 94

6 The aesthetics of cyberspace security **97**
6.1 Cyber security aesthetics: additional background 99
6.1.1 Aesthetics and meaning 99
6.1.2 Aesthetics and learning 100
6.1.3 Aesthetics and self-efficacy 101
6.1.4 Our expectations for this exploration 102
6.2 The image-set: results 103
6.2.1 Colour 106
6.2.2 Objects 108
6.2.3 People 108
6.2.4 Places 109
6.2.5 Other 110
6.3 Discussion 112
6.3.1 The visual vocabulary of cyber security 112
6.3.2 Physical traditional security semiotics 114
6.3.3 Hackers: anatomy, gender, and race 115
6.3.4 Digital-Physical spheres 117
6.4 Trends and Recommendations 118
6.5 Summary 120

7 Reflections and conclusions **123**
7.1 Chapter 4: On the blending of metaphors as a basis for cyberspace exploration 124
7.1.1 Reflections on the experiment 125
7.1.2 The limitations of metaphor 125
7.1.3 Future directions 127
7.1.4 Improving security advice through agent-based simulation . 128
7.2 Chapter 5: Gauging the difficulty of learning security advice 129
7.2.1 The limits of assessing news-mediated cyber security advice 130
7.2.2 Future directions 131
7.3 Chapter 6: On the benefits of cyber security aesthetics 132
7.3.1 Cyber-security Aesthetics: A lack of suitable analysis methods? 133
7.3.2 Future directions 134
7.4 Final thoughts 135

Bibliography **137**

List of Figures

1.1 The relationships between the research questions, contributions and the chapters of this dissertation. 8

2.1 The relationships between Information, ICT and cyber security (adopted from: [371]). 14

3.1 The four-spaces model as adapted from Fauconnier and Turner [114]. 43
3.2 An overview of the news-scraper tool. 44
3.3 An overview of the CIS-vectors ontological framework [10]. 50

4.1 Our blended concepts shown at the Macro-Level. The solid lines represent connections between input sources, and the dotted lines represent connections in spaces. At the top we find our generic space, labelled “Physical space’. On the left-hand side, we have the “online’, which is our first input space, on the right, “epidemiology’ is represented form our secondary input space. The two spaces come together in our blended space of “Cyberspace". 59
4.2 Our blended concepts shown at the Micro-Level. As before, the solid lines represent connections between input sources, and the dotted lines represent connections in spaces. At the top we find our generic space, labelled “Physical space’. On the left-hand side, we have the “online’, which is our first input space, on the right, “epidemiology’ is represented form our secondary input space. The two spaces come together in our blended space of “Cyberspace". 61
4.3 Two illustrative graphs of cyberspace. On the left, we have complexity/control as the defined axes. On the right, we have prevalence/complexity as the defined axes. 62
4.4 The overall infection rate broken down by week. Out of 100 user actors, 7 were infected. 68
4.5 The overall infection rate broken down by type. 69
4.6 Each compromised user actor was at a different stage in their journey when infection took hold. 70

4.7 Each compromised user actor was visiting either an e-commerce site or an adult genre site upon infection (genres taken from Alexa Top-1000 websites rankings). 70
4.8 A process diagram highlighting the actions each agent took while in cyberspace. 77

5.1 Articles published per day between January 2015 and December 2020. 82
5.2 The occurrence rate of CIS-vectors. Null values are excluded. 83
5.3 A correlation plot, highlighting in particular the strong correlation between CIS-4 and CIS-16. The larger and darker the circle, the stronger the correlation. Each CIS-vector is represented, with many have weak correlations. For a reference to what each CIS-Vector is, please refer to figure 3.3. 84
5.4 The distribution of sentences per article. 86
5.5 A visualisation of Heaps' law. 88
5.6 The distributions of our readability metrics. 89
5.7 A visualisation of changing sentiment, depicting a slight increase in negative sentiment along with a corresponding increase in article generation. 95

6.1 A random selection of images taken from classes 1-5. 104
6.2 A random selection of images taken from classes 6-10. 105
6.3 An example of the most commonly used colours within our top-two classes, simplified to 4-bit. 107
6.4 Heat-map highlighting the overall colour differences between images in Class 1 (Traditional physical-digital security semiotics). 108
6.5 Heat-map highlighting the overall colour differences between images in Class 10 (Non-security semiotics and skeuomorphism). 109
6.6 Heat-map highlighting the overall colour differences between images in Class 2 (Hackerman archetype). 109
6.7 Heat-map highlighting the overall colour differences between images in Class 3 (Non-malicious users of cyberspace). 110
6.8 Heat-map highlighting the overall colour differences between images in Class 9 (Disembodied anatomy interacting with a physical device or digital overlay). 110
6.9 Heat-map highlighting the overall colour differences between images in Class 4 (Digital superpositions over cityscapes or skylines). . . . 111
6.10 Heat-map highlighting the overall colour differences between images in Class 5 (Physical-digital hybrid workspaces). 111

6.11 Heat-map highlighting the overall colour differences between images in Class 6 (Abstract patterns). 112
6.12 Heat-map highlighting the overall colour differences between images in Class 7 (Textual content such as explicit warnings). 114
6.13 Heat-map highlighting the overall colour differences between images in Class 8 (Wall of code). 114

7.1 The way in which the research progressed. 124

1 Introduction

Before the advent of digital information transfer, and long before William Gibson [135] coined the term 'cyberspace' in 1982, humans looked for ways to secure their data. We can find the forebears of modern encryption in ancient Egypt, where deliberately disordered hieroglyphics were used to prevent text from being read by untrained eyes. Similarly, the Spartans utilised transposition ciphers, and Julius Caesar is commonly thought to have realised the military potential of data security by encrypting the messages he sent to his generals. These ancient solutions were intuitive and easy to deploy, and they were functional enough to address relevant threats [167]. Now, the objective of information security remains the same: to protect assets from various threats, including malicious actors who exploit vulnerabilities to reach their goals [371], by deploying security processes to partially or completely eliminate these vulnerabilities [113, 132].What has changed, however, is the complexity of security threats and attendant security processes.

In today's data-driven and highly interconnected world, cyber security risk is not exclusive to those who actively communicate private information in more-or-less public domains. Even individuals who do not own digital devices or participate online can be vulnerable to data breaches. For example, in Japan it is estimated that only 40% of individuals over 65 use the internet [21], yet pension data held on

them in a digital format was still lost by their government [1]. Further risks such as rapid evolution of cyber threats outpacing defensive knowledge, under-resourcing of cyber crime units, lack of government prioritization and oversight, and ineffective deterrence of attackers all compound the issues facing users today, and, given the scope of these contemporary threats, individual users have had to become active participants in ensuring the security of systems, despite the fact that they have little knowledge about or control over the systems themselves (also known as 'responsibilisation' [311]). As such, they must mediate experts' security advice—which, in the context of this dissertation, we define as explicit instructions intended to make recipients' devices more secure, once implemented [305, 293, 160] in order to learn and apply security solutions. But such advice must adhere to basic principles in order to be effective. For example, Saltzer and Shroder in 1975 created a set of design principles based on their idea of 'psychological acceptability'. In their work, they describe the essential nature of ensuring that human interfaces are designed for ease of access, so that users can apply their protection mechanisms where necessary. In addition to this ease-of-use, psychological acceptability means the solution should match up with the protection goals the user has in mind (for example, a four-digit security code for a debit or credit card is both easy to remember and matches with the idea of protecting one's financial resources whilst maintaining easy access)[342]. These concepts also apply to cyber security advice, where however, guidance into overcoming these issues were not adequately actualised until the mid-1990s, when the field of usable-security was born out of works that championed 'user-centred security' [399] which identified the user as part of the solution rather than the problem [4, 398]. Even so, research in the field consistently finds that users have difficulties implementing security advice [305, 293, 381].

1.1 The research problem

Many influential studies have attempted to uncover the root causes of, and solutions to, the perceived psychological acceptability barriers users may have: Brandimarte

[1] https://www.reuters.com/article/us-japan-pensions-attacks-idUSKBN0OH1OP20150601

et al. [52], for example, argued that users' inattentiveness reflects their lack of knowledge for the possible consequences of losing control over their information, whereas Rader et al. [302] concluded that users resist security advice that they deem too difficult a barrier to implement. This latter point corresponds with an interesting facet of the principle of psychological acceptability: because the user maintains a 'mental image' of the data they want to protect, cyber security mechanisms must accord with this image (especially in terms of their complexity [385]) or be rejected as more taxing than beneficial [120]. Herley [160] made this point even more explicit, arguing that — of three possible reasons for users' disengagement with security advice ((1) users are simply unmotivated; (2) security advice is inaccessible; and (3) the rejection of security advice is rational from a purely economic standpoint) — users' behaviour could therefore be explained as a rational result of cost—benefit analysis.

Usable-security researchers continue to investigate such questions of users' motivation and deliberation, as well as how users learn about cyber security. The supposition is that, if this learning can be optimised, then users' apathy might be overcome. However, usable-security work often relies on qualitative methodologies to explore specific issues within cyber security. These works do not often proceed beyond high-level abstractions, and they do not clarify how to define 'efficacy' with regard to security tools and techniques. For example, it is difficult to define the concept of providing *advice*, partly because it pertains to almost every discipline involving human behaviour [284, 44]. *Security advice* is particularly complicated, as it derives from diverse disciplines, including Psychology [386, 105] and Medicine [394].

We began by describing the research problem above in this manner, not just to espouse the problems surrounding the efficacy of such research, but rather to additionally highlight a finding in such research: environmental (cyberspatial) risks. Our motivation behind this is the work of Quinlan et al. [300] (which is discussed in Section 1.2). In this paper, an exploratory study of the connected systems of a modern vehicle revealed not only a wealth of technical data pertaining to potential

privacy infractions, but additionally several large-scale sociological effects that cyber-physical systems exert on the environment, which may not be well-understood by the users of these systems. While data collected and sent by the car did not extend to PII (Personally Identifiable Information) data, there were still implications that could have long-term privacy, social and financial implications depending on the context in which they are used. For example, data pertaining to seat-belt usage, window usage and heating elements had insurance and licence implications that most users would not be aware of, yet may affect them in the longer-term. Based on these findings, we can take a phenomenological approach, and argue that while the subjective experience of the user within the real world may follow a set of top-down predictions based upon continual interaction with an external environment [127], in cyberspace an environmental layer is added that superimposes contextual constraints upon the user that they may or may not consciously engage with. Our overarching research question is therefore an exploratory question:

> *How might cyber security advice be improved upon whilst keeping in mind the user's perspective(s) upon cyberspace?*

This question allows us to cover a secondary motivation: this dissertation takes the view that in some cases user-behaviour observed in the above-mentioned studies isn't definable, instead referring to what is known as the "other-minds problem" [257]. In essence, the other-minds problem refers to the epistemological challenges in determining the state-of-mind of another entity [172]. With a greater understanding of the environmental risks, perhaps we can provide an alternative view of user-behaviour not as reliant on first-hand observations and qualitative framing, and enhance the efficacy potential of cyber security advice. (We discuss this in Section 2.5.4.)

We chose to start our investigation by covering the broadest possible scope, and narrowing down depending on the findings. The first research question derived from our overarching question therefore covers the *where* of the matter, in the sense that we must understand more about the environment in which the above-mentioned usable-security studies were conducted, and where the user requires cyber security:

> **RQ1:** Given that users have complex motivation and decision-making patterns when interacting with cyberspace, can we establish a more contextually appropriate environment in which security decisions are made by users?

RQ1 lays the foundation for the complete work through providing an exploratory qualitative environment of the major actors within cyberspace and the associated power relationships between them as they interact in cyberspace. We refer to this contribution as **C1**, and it describes a conceptual framework for 'cyberspace', the world in which cyber security and its associated advice is meant to be utilised. We add context to the security of these interactions by our focus on the cyber security elements of cyberspace. The model itself was derived from a mixture of secondary research and applied use of metaphor blending, where metaphors, often a source of great heuristic fecundity, aid us in the development of new ideas and testable hypotheses. The contribution also contained an experiment meant to highlight the potential potency of our new environment.

However, what might we gain in terms of understanding from answering our main question that might lead to a change in the way cyber security advice is created and disseminated? This is what the second and third contributions espouse. Their associated research questions are shown below, derived directly from research findings in the first contribution.

> **RQ2:** Considering that the dissemination of security advice about cyberspace takes place through a multitude of vectors, is it possible to measure the efficacy potential of such advice through one such dissemination vector?

RQ2 was derived from the design and development of the experiment for our model, and seeks to ascertain the status of the security advice as given to users of cyberspace. We refer to this contribution as **C2** and it describes an assessment of the way in which common cyber security advice is currently disseminated to users. We placed particular emphasis on how this advice may be learnt, as well as on the practical barriers to acquiring this advice.

In order to provide an appropriate answer, we scoped the work through a single large dissemination channel, chosen due to its strong public-facing elements and large body of cyber security advice. The resulting contribution discusses the effectiveness of one of the largest advice dissemination channels through the development and analysis of a corpus of cyber security advice generated from mainstream news articles.

The third research question was derived directly from the secondary research for C2, where we found that work by Thomson-Jones and Moser [360] as well as Shelley [334] espoused the clear and growing import of the need for philosophical research into digital art within cyberspace. These findings were further supported on a more practical usable-security level, where there has been clear secondary evidence of aesthetics informing user decisions with regards to cyber security decisions within the usable-security community. Throughout the development of usable-security as a paradigm, work such as Josephson and Holmes [183], Fogg [122], Alsudani and Casey [13], Flavian et al [119], Shires [335], and Carroll [70] have all made note of aesthetic judgement in the area of usable-security. RQ3, then, is as follows:

> **RQ3:** What do cyber security aesthetics look like to an individual user, and what are their efficacy potential?

We refer to this contribution as **C3**, and it describes an assessment of the aesthetics of cyber security, as presented to the user in conjunction with cyber security advice. Within this contribution emphasis is placed on how these aesthetics may aid or hinder the successful dissemination of cyber security advice to users. This study contributes new insight into the pedagogical effects that current cyber security design aesthetics may have on users, with the aim to answer the question in two parts: *What* are the aesthetics, and *why* these may be important to usable-security researchers? This piece represents cyber security advice at its most targeted, not at the environmental or epistemological levels, but at the phenomenological level. With these elements in place, this dissertation can take a holistic view towards answering our primary research question. Our contributions allow for insight into how much power a user has within cyberspace through the focus on at least one aspect of their informal learning activities and the aesthetics they

process throughout their interactions with cyberspace. To accomplish these goals, this dissertation leverages a mixed-methods approach. As we take a holistic view of cyberspace security interactions, we argue that through taking this approach towards usable-security, we may increase the efficacy of expert–user interactions. Furthermore, by utilising quantitative tools to obtain data for our research questions, we anticipate that we can bolster subsequent qualitative discussions of security data-sets, drawing more granular and targeted results.

In the next section, we specify the works arising from this dissertation.

1.2 Works arising from this research

1. Mark Quinlan, Jun Zhao and Andrew Simpson: "Connected Vehicles: A Privacy Analysis" In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. 2019.

2. (In review) - Mark Quinlan, Aaron Ceross and Andrew Simpson: "Towards the creation of a cyberspace model: A metaphorical approach". *In Technology in Society*. 2021

3. (Publication pending revisions) - Mark Quinlan, Aaron Ceross and Andrew Simpson: "The efficacy potential of cyber security advice as presented in news articles". In *Interacting With Computers*. 2021.

4. (in progress) - Mark Quinlan, Aaron Ceross and Andrew Simpson: "Cyber Security Aesthetics - An exploratory study".

In all of the above works I am the primary author. For (1), the paper was the culmination of two separate mini-projects, with Andrew Simpson by supervisor for the first mini-project, and Jun Zhao for the second mini-project. In both a standard work pattern was followed, where my initial idea was refined through discussion during regular meetings with both, allowing for a paper developed by myself but shaped by their experience. The data collection, analysis and all drafts

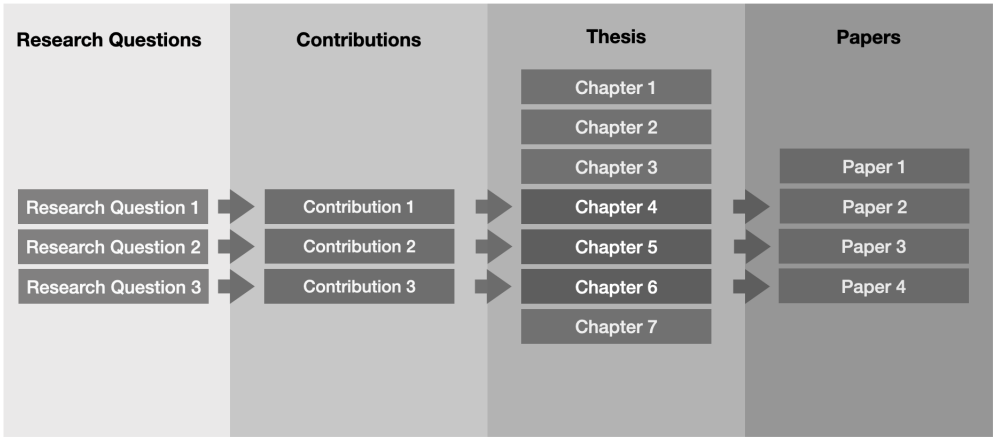


Figure 1.1: The relationships between the research questions, contributions and the chapters of this dissertation.

were completed by myself alone, with the final draft provided to Andy for pre-submission edits. For (2-4), the initial idea was developed for the conceptual model of cyberspace by me, and refined through periods of discussion with Aaron and Andy. In each of these cases, the design for the experiments, data collection and all written work were completed by me, with Andy providing feedback at each stage and the edits for the final draft. For (3) and (4), Aaron provided feedback and additionally assisted in the selection process of the analysis methodology, which was then decoded, finalised and executed by me. The breakdown of these papers into the dissertation is as follows. Chapter 2 contains a significant proportion of work from (1-4). Chapter 3 describes the methods for (2-4), Chapters 4, 5, and 6 contain the results and discussion from (2-4), with Chapter 7 consisting of research limitations and future work directions, and consiting of mainly new text.

1.3 Dissertation outline

The remainder of this dissertation is organised as follows:

> **Chapter 2: Background and motivation**, details the background of our research through the lens of usable-security and illustrates further the motivation for each of the aforementioned contributions. It introduces concepts that apply to all of the contributions and research objectives, and it provides a detailed discussion of the practical challenges facing the usable-security field.

Chapter 3: Methodology, describes the various (mixed) methods used to carry out each contribution (C1–C3), some of which are informed by a case study.

Chapter 4: Cyberspace through the eyes of the user presents our conceptual framework that describes 'cyberspace', the world in which cyber security and its associated advice is meant to be utilised. It answers **RQ1**.

Chapter 5: News-disseminated cyberspace advice utilises research findings from the model to provide an assessment of the way in which common cyber security advice is currently disseminated to users. It answers **RQ2**.

Chapter 6: The aesthetics of cyberspace security presents an assessment of the aesthetics of cyber security, as presented to the user in conjunction with cyber security advice from Chapter 5. It answers **RQ3**.

Chapter 7: Reflections retraces our steps across Chapters 4-6 to develop a unified set of reflections that respond to our overarching research question. It summarises the dissertation and explains how our contributions can be applied to current practice. It also highlights the weaknesses and limitations of each of our studies, alongside opportunities for future research that could extend the contributions of this dissertation.

2
Background and motivation

We set out with two aims for this chapter. The first aim is to provide definitions of terms that we will use throughout this dissertation, for example 'cyberspace' and 'users'. Some, such as 'informal learning' will be discussed in-depth to aid our understanding of the topic, and some such as 'security advice' will be made as explicit as possible using a singular definition. The second aim is to provide additional background for our motivation as to what we discussed in the preceding chapter. The rest of this Chapter is structured as follows. In Section 2.1 we introduce our concepts for cyberspace as an environment, before covering the security of this environment in Section 2.2, usable-security in Section 2.3, and the ways of interacting within it in Section 2.4. Section 2.5 covers the specifics relating to advice when interacting in cyberspace, and Section 2.6 covers elements pertaining specifically to chapters 5 and 6 respectively. An expansive summary of all the topics covered can be found in Section 2.7.

2.1 Cyberspace: our virtual environment

The term 'cyberspace', as coined by Gibson — a science-fiction writer — [135], has become synonymous with descriptions of global computer networks such as the Internet at every level. Cyberspace in this sense was seen as 'a new universe' —

parallel to the physical, but created by the digital [33]. As early as 1991, 'cyberspace' came to designate an abstract, conceptual, three-dimensional fifth domain alongside land, sea, air, and (extra-planetary) space [33, 51]. This term became pervasive within U.S. military documentation, and it helped to shape the military's approach to Internet security [228, 51] by means of conceptual comparison to the pre-extant domains. Today, the conceptualisation of the World Wide Web in terms of online 'spaces' is universal, from the social sciences to the media [38], rendering the web meaningful within our externally facing sensory experience [51]. Thus, the environmental metaphor of cyberspace is perhaps the first of most metaphors in the cyber field [38].

As many of the concepts of cyberspace are derived from humanity's experiences in the physical realm [359], cyberspace in this dissertation is visualized as a techno-spatial domain[1] developed by humanity within our vision and limitations.

As a fully-fledged domain, we furthermore assume that cyberspace is subject to *macro-environments*, which are a set of core conditions that define its global environment. A physical analogue to this might be the six defining macro-environments for global economics, such as Gross-Domestic Product [170]. These macro-environments are subject to forces, which are defined as ways which influence, pressure, and manage interactions between systems, agents and actors in cyberspace [266] and shape development of the domain overall, similar to the forces at work in the physical domain[286].

Based on these ideas we present the following explicit definition for cyberspace:

> Cyberspace represents a human-constructed techno-spatial domain with perceived similarities to the physical world we occupy, and manifest macro-environments that are subject to both physical and digital forces.

From the users' perspective, cyberspace, or at least, the subset of cyberspace they interact with, may be seen as being derived from the philosophical notion of a

[1] A techno-spatial domain is defined here as a mainly digital domain that assumes certain characteristics of the physical realm through the use of metaphor (for example a digital workspace), the use of literal re-imagining of physical environments (such as a Virtual Reality) and through the use of domain-straddling devices (cyber-physical systems such as an autonomous car).

'lebenswelt' or life-world [173]. In a lebenswelt, individuals encounter a pre-developed social world in which all subjects are united in a sense of community or togetherness. The social world consists of subjective social interactions with other users or *'second-order virtual agents'* (see Section 2.4.2), which over time leads to a shared-group perspective [236, 173], and is often seen in virtual reality contexts [257].

2.2 Cyberspace safety & security

All forms of security, regardless of domain type, revolve around the protection of assets from various threats and malicious actors that exploit vulnerabilities to reach their goals [371]. There are usually security processes in place that assist in mitigating these threats through the partial or complete elimination of vulnerabilities[2] [113, 132]. When one develops these ideas towards a human context, we arrive at what is called Information Communications Technology security (ICT security). In ICT security, the assets that require protection are often the informational infrastructure [371, 389]. Including not just the infrastructure, but also all aspects of the information itself is a further development and called Information security. Information security therefore encompasses not just ICT security but all of the processes and data not directly generated and/or stored by the infrastructure itself [322]. Cyber security moves that definition forward once more, incorporating assets ranging from an internet-connected washing machine through to the interests of human society at large [232]. Cyber security is described as being inclusive of any person or device that has an on or off-line communication capabilities [371, 378, 245]. The relationship between these different security definitions is visualised in Figure 2.1.

One must also make the distinction between safety and security when discussing cyberspace security. Work such as Burns et al. in 1992 looked at the emerging threat of cyberspace safety and security. In the paper, safety and security are distinguished by their stance towards accident versus intention, randomness versus agency, and hazard versus hostility in assessing and managing threats. This colors their differing

[2] `https://www.iso.org/standard/54533.html`

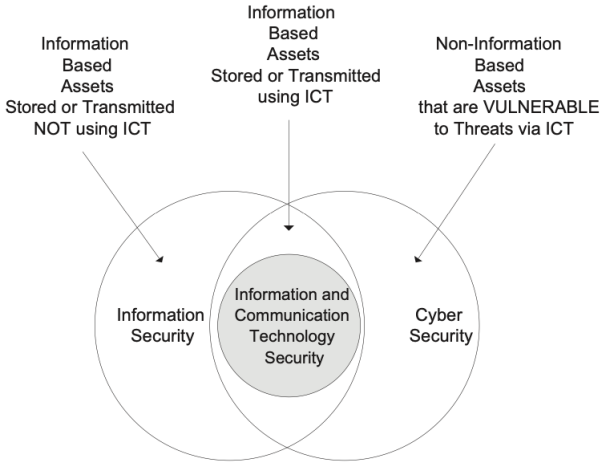


Figure 2.1: The relationships between Information, ICT and cyber security (adopted from: [371]).

ontologies, orientations, and ethics [59]. An example is provided through the work of Lisova et al, who conducted a thorough review of cyber security and safety. They state that within cyber-physical systems, safety deals with unintentional faults or failures that can lead to hazardous conditions, while security focuses on defending against intentional cyber attacks and threats from adversaries. Safety engineering aims to ensure system reliability and availability so that no unintended physical harm occurs. In contrast, security engineering protects confidentiality, integrity, and accessibility of systems and data from malicious actions like hacking, sabotage, or espionage. While safety and security were historically treated separately, their tight coupling in modern connected systems requires integrated analysis to build robust cyber-physical systems that are both safe to use and secure against threats [234]. Therefore, whilst this dissertation will focus on the security of cyberspace, minor overlap is bound to occur.

2.3 Usable security

Cyber security requires that the user follows a particular process, or utilises a function that is first learnt and then utilised [371, 113]. The field of usable-security was developed to aid in the understanding of cyber security processes,

and aid with accessibility. However, in many cases dual aspects of usability and security are at odds with each other [186]. In some cases, this can be attributed to the fact many system designers treat both usability as well as its security as somewhat of an afterthought [392].

Ideas and tools which aid the process of allowing usable cyber security have come from sources such as Flechais et al[120], who argued that undesirable actions (such as acting insecurely) could be made more difficult, and contrasted with aiming desirable actions easier to implement and comply with, even if specific proof was not offered at the time of writing. In such a case there would be a clear correlation between improving both action types. In the case making desirable actions easier to perform, the advice that is given to a user about their security in cyberspace will play a strong role in the efficacy of any potential system designed to enable such security.

2.4 Interacting in cyberspace

At the time of writing, aside from edge-cases and emerging technologies all content within cyberspace is processed by single machines before being presented to individual users on a single device [257]. Hence we utilise the term 'user' for any given individual that interacts within cyberspace. The sub-sections below aim to provide more background to these users.

2.4.1 Individual users of cyberspace

It would be prudent to define our user further to align more sufficiently with our cyber security context. Therefore, for our purposes the 'user' in usable-security relates to an individual that is making security decisions within cyberspace. Based on existing literature [261, 168, 276], we define these users as 'individual users' who own systems, devices and/or services that maintain internet connectivity. An individual user is someone who makes use of connected digital technology and can be of any gender, age group, and professional background. We include corporate users in this definition because their learning habits extend beyond their formal

corporate learning environments — that is, they may engage in informal learning outside of work environments [131].

Users may also represents corporate or other third-party interests [239]. In such cases, whilst they represent such interests the user falls outside of our scoped definition as they are presenting an interest that although may have a direct causal ancestor with their corporation [126] we can not ascertain to match with their own interests and needs [57]. Furthermore, the assumption can be made that the agency of such users can be significantly higher [3] or lower [4] than those of our definition due to the nature of the interest represented. For these purposes corporate users are excluded.

To further aid with our development of a definition, we look towards work such as that of Thibodeau et al. [368], who conceptualised the human to household technological relationship inside the home, and Nthala and Flechais [276], who proposed a spatial divide that contextualised individual users inside their homes: involving social, activity and technological aspects.

The social aspect was explored according to the household (a group of individuals occupying a single building), alongside the household's neighbourhood, friends and other social acquaintances. In usable-security terms, at least one study [271] supports this view due to the nature in which cyber security influences can be derived from this group.

The social is heavily linked to the activities in which these users engage. Typically our individual user engages in digitally-based tasks such as activity planning, online shopping, interpersonal communication and transmission of sensitive information (such as medical data [62, 276]).

The internet is the central element that enables the above aspects. It is important to consider the environment in which individual users find themselves, which are incredibly complex and vary from individual to individual. For example, office environments practising a BYOD (Bring-Your-Own-Device) policy, third-party

[3] Such as someone gaining an unfair advantage through internal access privilege, the insider threat [39].

[4] Such as employer network monitoring or outright bans [64].

spaces, such as social and activity spaces, among others [276] can be included and therefore serve to further complicate any kind of technology-mapping practices of individual users. With a mixture of traditional computers, smaller devices such as smartphones, as well as a myriad of IoT (Internet-of-Things) within their personal purview [205], their technology set-up can therefore be unique, akin to a fingerprint, making it difficult to assess the risks and vulnerabilities relevant to a particular space [62, 276]. All these developments leave us with the same question; who are the users of cyberspace? For the purposes of this dissertation we see the user as:

> A cyberspace user is an individual who must own or operate an internet-connected device with which it pursues certain goals within cyberspace, is of an age where they can independently interact with cyberspace on said device, and is not directly representing the interests of a third party when online.

This corresponds closely to Fleshais et al's definition of a home user [120], but we believe that these definitions can in fact extend beyond the home and into most realms of HCI in which users interact with cyberspace based on motivations that are not explicitly linked to third-party interests. Furthermore, we can now exclude extreme examples of cyberspace use for personal goals, such as a newborn linked to an internet-connected heart-rate monitor. Armed with the above we are in a position to provide further context to our individual user, through utilising several proto-personae.

Personae have been used in Human-Computing Interaction (HCI) research since at least the mid 1990s, and have helped to allow researchers and developers to make more informed decisions about their potential user [75]. Using personae through the development stages of hardware and software organisations can ensure that the needs of their personae are included throughout [176].

There are multiple ways one can use to develop personae, the main two being *research personae* and *proto-personae* [176]. For research personae, the vast majority are developed through conducting user research. For example, research personae may be developed through the use of interviews, observational studies and surveys [176]. Developing personae in this manner allows for the deepest possible insight into

the lives of their users, research subjects or similar [103]. Proto-personae are instead developed through indirect interaction methods, such as secondary research. Most proto-personae are therefore heavily assumption-based, which although a drawback as to their potential truthfulness, they also require far less resources to create, and can serve as a valid starting point for research. We have developed proto-personae to personify our users based on prior research where personae were developed for specific cyberspatial purposes. To construct these, we adapted work from sources such as Lee et al, who in 2017 developed personae for the dominant kinds of social media users [222], Arora, whose work profiled 'the next billion', which are users that do not necessarily have Western internet habits, nor do they necessarily purchase the same kinds of devices [19]. Another example would be Gizeck et al, who developed scales to which certain individuals performed in certain ways (e.g. in their scale on risk-estimation, individuals classed as students scored higher on risky behavior and exposure to offenses compared to academics and admin staff) [279]. We also used miscellaneous sources such as news media concerning internet usage[5], device usage statistics [6] and research on user behaviour in cyberspace mentioned in earlier chapters. From these we assembled attributes like sample demographics, personality traits, contexts of media usage, devices used, and interests/motivations, which are reflected in the table below. These individual should only be seen as a non-exhaustive, representative sample of cyberspace users, and are not used explicitly in the dissertation. Rather, they aid the reader in understanding the breadth and depth of individuals that interact with cyberspace.

2.4.2 Non-corporeal users of cyberspace

Consideration to users that interact with cyberspace but fall outside of our scoped definition are highlighted in this subsection.

[5]Such as the use of motorcycle taxi services in Indonesia: `https://www.eastasiaforum.org/2022/02/03/indonesias-gig-economy-falling-short-on-decent-work-standards/`.

[6]For example, https://iot-analytics.com/number-connected-iot-devices/.

1.	A single female, from a developing country who primarily speaks English. This individual works as a taxi driver, and their primary connection to cyberspace is through a single 4G connected smartphone. This user has no other connected technology in their home, and utilises public and neighbourhood wireless access when available in order to save on roaming charges. This individual is mainly concerned with utilising her device to keep in touch with family, and conduct financial micro-transactions.
2.	A single male, from a developed country in North America. This male is the parent of two children, and manages their household's access to cyberspace through a router-connected desktop. Each has their own smartphones, connected to the latest generation wireless networks and self-maintained Wi-Fi. This individual is mainly concerned with utilising her device to keep in touch with family and friends, conduct financial transactions and online shopping. He is also concerned with ensuring his children can access schoolwork online, and maintain their safety against potentially malicious actors online.
3.	A married female, living with her husband in a household of multiple occupation (for example, a *House of Multiple Occupancy* in the UK) in a major European city. This individual has taken responsibility for maintaining the couple's two connected computers, but only has access to her own smartphone. Both utilise a local wireless network to work from home, and this network is communally managed, meaning no single user has overall control. Her partner engages in online activities this individual deems risky, such as online gambling, downloading pirated content and so on. Her partner explicitly refuses to engage in what she deems secure behaviour, and she is therefore continually researching new ways to keep the couple secure in their daily online activities. She has no agency over what the other household users do during their interactions with cyberspace.
4.	A single male, from a developed east-Asian country whose technology fingerprint is complicated through his aggressive purchasing of new devices, use of cyber-physical systems such as connected vehicles, and frequently shares user data such as location, purchasing habits and financial information through use of multiple social media networks. He straddles the digital divide, using Virtual-Private-Network to access Western applications and services.
5.	A single female, from a developed North-American country, who uses a customized computer containing only open-source software and as much open-sourced hardware as possible [7]. This user shuns large sections of cyberspace (such as social media), and has publically campaigned on data-privacy issues in the past.

Table 2.1: A set of proto-personae that fit with our definition of an 'individual user'

Corporates and nation states

During an earlier period in the history of cyberspace, work such as that of Johnson [180], who asserted that cyberspace was a new beginning and would require brand-new definitions, and Barlow [27], who emphatically proclaimed "a declaration of independence" for cyberspace, the domain must have seemed a new frontier [49]. The current state of the domain is rather different, with nation states imposing their politics and territoriality, either through technology[8] or indirectly through the restructuring of networks[9] or emerging spaces such as social networks [216].

Corporations similarly wield significant control throughout cyberspace, being capable of giving orders [202], projecting force[10] and defending against other corporations and individuals at the network level and above. In this manner, the users' agency within cyberspace is curtailed, and harkens back to Foucault's notion of agency permanently being diminished through "the omnipresence of the controlling eye"[124].

Autonomous agents

In the case of cyberspace, where elements are networked and as mundane in the foreground (for example, a networked smart phone) as they are in the background (for example, a traffic management system [396]), users are largely unaware of the interactions between their inputs and the underlying processes (such as the data and analytic algorithms [108]) that constitute user-facing software systems [229, 153]. These are the autonomous agents of cyberspace.

[8]For example, within China their Great Firewall is a censorship system that prevents the vast majority of the country's 600 million users from accessing content deemed inappropriate by the state. It accomplishes this through monitoring and filtering several layers of the TCP/IP model including IP addresses, TCP ports, DNS requests, HTTP requests and more [109]).

[9]For example within the United States, term Net-Neutrality, is loosely defined as a discussion on the policy of the role of network infrastructure owners as the gatekeeper position on the internet [209].

[10]Such as the Cloudflare de-platforming of right-wing application, Parler(`https://krebsonsecurity.com/2021/01/ddos-guard-to-forfeit-internet-space-occupied-by-parler/`)

Second-order virtual agent

Virtual agents differ from autonomous agents in that they contain an internal model of itself in relation to its social relations. It does not imply sentience, however, when users are confronted with such an agent they share an inter-subjective presence while interacting [257]. An example of such an agent is an avatar within a virtual reality environment that is system-controlled [339].

2.5 Cyber security advice

This section briefly discusses some of the issues surrounding our understanding of how users interact with cyberspace and cyber security advice in relation to how they encounter, react and deal with said advice.

2.5.1 Who provides guidance into cyberspace?

The concept of guidance, in terms of *advice*, is difficult to define, partly because it pertains to almost every discipline involving human behaviour [284, 44]. *Security advice* adds further complication by introducing the concept of 'what security means' to any form of advice generated around it, with similar paralells in other disciplines [386, 105, 394][11] Each of these disciplines has its own approaches to security advice, so it would be foolish to attempt a comprehensive review of this topic covering all of these fields.

In this dissertation, rather than taking a broad view of security advice within cyberspace, we limit our concerns to what we term *professional security advice*. Çelen et al [73] describe the term *professional advice* as "advice rendered by experts", which is then disseminated to individual users (see Section 2.5.4). Professional security advice is designed to alleviate security challenges, but, because this must often occur through the mediation of individual users, these instructions are characteristically *persuasive* and typically *explicit*, rather than *implicit*.

[11] Given that cyber security is the discipline of concern in this dissertation, we shall refer to it simply as 'security'.

Explicit advice often takes the form of a verbal or written appeal, such as *Keep your browser up to date at all times*. There are even different varieties of appeals, as with *Keep your browser up to date at all times ... or else your browser will get infected*, which constitutes a *fear appeal* [220, 22]. Implicit advice often takes the form of a threat message [309], such as *Downloading a file from an untrusted source is risky* [111].

Based on this distinction and the definitions prevalent in the literature [307, 305, 293, 174, 302, 97, 160], we define *security advice* thus:

> A written instruction, provided by a source trusted by the receiving individual and of professional origin, which has the explicit goal of enabling the recipient to be more secure once they execute the instruction.

We exclude verbal advice simply as it is too difficult to manage within the scope of this dissertation[12] and attempt to remain device-agnostic.

2.5.2 How the user may learn this advice

There are many ways in which individual users can encounter new security advice, but most involve some degree of *formal* and *informal learning* [150, 310, 347, 302].

Formal learning occurs through structured courses in an online or in-person classroom environment, usually followed by an assessment [162, 63]. For example, the delivery of security awareness programmes such as SETA (Security Education, Training and Awareness) [13] occurs within organisations, and they include classes that train employees to recognise threats [393]. These training programmes tend to focus on compliance with corporate policy [221], and they evoke generic situational awareness [221], rather than providing specific contexts and situations from which an individual user can learn.

Informal learning is unstructured, occurring outside of formal education contexts and without direct targeted interaction with security experts [347]. Nevertheless, it is the primary way in which adults learn about the world around them [242, 281].

[12] For example, Pfeiffer et al. conducted studies in medical contexts, tracking verbal and verbal plus written advice, which illustrates some of these difficulties in measuring efficacy and more [291].

[13] `https://media.defense.gov/2017/Mar/24/2001721513/-1/-1/0/CIM_5528_1A.PDF`

As such, it is the main mode of learning considered in this dissertation. Informal learning is usually triggered by some internal or external impetus [242], and it occurs primarily when individuals choose to actively seek out new ideas and advice.

Thus, for the purposes of this dissertation, we distinguish *informal learning* from *incidental learning* [242, 58] on the basis of their differing intentionality: *informal learning* requires some kind of prior impetus and concerted effort, whereas *incidental learning* is often a by-product of carrying out another task, where the new information is learnt almost by accident [242]. Despite being a conscious decision, informal learning is often conducted haphazardly and is influenced either by randomised chance [242] or by the learning behaviours of others [58].

Many of the studies concerned with individual users' security intentions frame users' situational awareness and knowledge as necessary conditions for appropriate security decisions [123, 310]. Essentially, researchers assume that individuals must know about the issue at hand before they can make a reasonable decision. Thus, when an individual is faced with a security message about a potential threat, their decision process could proceed in one of two ways.

1. First, if they already possess prior knowledge about the threat (and, more importantly, about how to prevent it), they are significantly more likely to take appropriate action. This is a *danger control process* [309]. Danger control involves thoughtfully processing threat information and coping recommendations, which facilitates experiential learning about risk management and how to mitigate said risks [375].

2. Second, if they do not possess prior awareness or knowledge, and therefore do not know how, or are unable, to neutralise the stated threat, the security message may be rejected. The individual user may instead act to control the psychological fear generated by the message (rather than the practical threat implied by its contents). This is called a *fear control process* [309, 123, 310]. Fear control can involve avoiding engagement with threat details and coping mechanisms, which can impede learning [375].

Therefore, individual users may accept security advice, but subsequently reject it if they lack relevant coping strategies or actionable means to counteract the threat, choosing to deal with the issue in ways perhaps not easily foreseen [168, 305, 174]. Or they may reject the threat message altogether[14]. Arguably, then, the efficacy of security advice depends on how well suited it is to a given individual's existing frame of reference and practices. This poses interesting problems for security advice that is disseminated to a broad audience, as is the case with media-acquired advice.

2.5.3 Causal-efficacy

In the early 1960s, anisotropy (the property of a material or entity which allows it to change or assume different properties) was researched as a part of a case study into the ways in which space as a domain plays a part in the development of behaviours and explanations offered by scientific theories [332]. It was found that the exploration of these domains led to significant anisotropy in the scientific community, characterised by increased heavy reliance on specific mathematical techniques and the development of domain-specific language [332] without explicit necessity being highlighted. This is an example of *causal-efficacy*, and in our case, we would examine how our individual user is changed through their interactions with cyberspace, and by extension, cyber security advice. Furthermore, Dack et al. [96], undertook an experiment to aid understanding of how causal-efficacy from informally-learnt information informs self-efficacy (for example, how an individual may develop a phobia for a certain food by reading about its supposed flavour, rather than through first-hand experience). They began with an indirect stimuli (words on a computer screen), and then presented a basic task to complete related to the words. They found that evaluations of self-efficacy on the task were somewhat dependent on the valence of the stimuli, but highly dependent on the reinforcement schedule. Their findings further showed that evaluations of self-efficacy are dependent on other stimuli (such as colour, sounds) that may be present when making the evaluation, or when carrying out a task. They make comparison of how certain stimuli in

[14]A commonly rejected threat message is those that appear in smoking advice literature, both on the cigarette packaging and elsewhere [388].

an environment can trigger feelings of hopelessness in clinical patients prone to depression. In our case, indirect stimuli and events in cyberspace could be said to have an impact on efficacy potential of individual users' security behaviour. The nature and extent of that impact is currently not understood.

2.5.4 The expert

In our case, it is of importance to provide an explicit definition of an expert. Expertise as a concept can be divided into two distinct categories: expertise as a function of *what someone knows*, and expertise as a function of *what someone does*. In the former, we are interested primarily in the expert's epistemic knowledge over a particular domain, in this case, their capacity to provide justifications for any given range of ideas and knowledge [382]. Assessing the risks of security threats to a specific set of systems and people (as defined in Section 2.1) involves risk management using an uncertain informational background [363, 178]. For instance, assessing accurately the cost of a cyber attack [363, 72, 178, 373], whether it is successful in all of its goals or not [346], the likelihood of a rare attack and the range of tools available to malicious actors is a constantly evolving process [346]. Due to all of these difficult to assess (and define) problem-sets, significant expertise to carry out any kind of assessment and provide appropriate advice is required. Therefore, many organisations and public-facing institutions employ security experts that have the requisite knowledge to offer insight and compose security advice based on considerable expertise gained from education and/or industry experience [66], whilst also maintaining the ability to provide assessments of the viability of current security processes and tools available to end-users [260]. Therefore, the work many security experts may undertake can be compared on a high-level to that of an aggregation function within a software system, which considers a large number of complex and diffuse data-sets from often uncertain sources (such as users, qualitative academic and industry publications, other security experts and security solutions). The security expert then combines these sources in order to produce novel knowledge on

the topic [61]. It must be stated that not all security experts follow this approach [161, 305], nor do all manage effective communication [35].

Within almost any field in which professional advice is rendered, two forces of market are always at play. The first concerns reputation, in which professionals are interested in how their advice is seen to be well-informed by colleagues and recipients [6, 214, 292], and the second concerns competition, which our context relates to how competition between the advice providers can distort information before it reaches the intended recipient. For example, professional advice can often take the shape of a contest, in which the experts are evaluated on the basis of their opinions (a great example of this can be found within the financial markets, where the Wall Street Journal Forecasting survey pits analysts and experts against each other and provides rankings [243, 144]). Both of these kinds of influences have the potential to alter the contents of any advice rendered.

Shortages of security experts with the skill-sets mentioned above are often reported by industry and academia [290, 260, 345, 227], which has led to a requirement for additional tools and techniques that can be used to aid current security experts in their work [262, 227]. Of particular importance to many users is that verifying the authenticity of the security experts behind the advice is difficult [347], which needs to be taken into consideration when attempting to ascertain the legitimacy of advice and whether to follow it.

Given the above-mentioned indeterminacy, incompleteness, or sometimes faultiness of the data used to generate expert advice in both settings, alongside an unknown mixture of experts with a particular education and/or occupational background, we determine the security expert who renders our advice to be *an individual who creates cyber security knowledge out of a mixture of some epistemological, as well as performative expertise.* Their backgrounds and motivations are otherwise opaque to us, as they may be to the reader of the news articles, and this forms a limitation on how we may perceive expertise in this field. Thus, individuals may struggle to verify or make use of security advice, or they may simply reject the advice as unreliable or impractical to implement (as per Herley's cost-benefit

analysis [160]). Indeed, a proportion of typical users may not receive information from the professional sources described in this dissertation at all [305, 307, 302], preferring to simply request specific information from unverifiable sources [152].

The *'other-minds'* problem refers to the epistemological problem of the ability to gain knowledge of another human being's mental state [257]. By state in this case we refer to their mental processes when undertaking actions to safeguard their security when interacting in cyberspace. The other-minds problem originated with the philosophically similar *'mind/body'* problem, which itself dates back to Descartes and possibly beyond [12]. Where the mind/body problem related to reducing experience to a *physical* state, scholars who work on the other-minds problem attempt to decipher methods in which differing mental states can be proven mathematically [172]. An analogy for the other-minds problem within artificial intelligence is the Turing test [151]. The opacity in our understanding of the mental state of another is what this dissertation believes limits the efficacy of previous studies utilizing qualitative methods such as interviews and questionnaires , and the issues below highlight the scale of the other-minds problem.

2.5.5 The efficacy potential of advice

Efficacy is a word derived from the Latin *efficacia*, meaning "efficiency". In our case, we are concerned with efficacy potential, a term derived from epidemiological circles where it serves as a function of treatment regimen effectiveness[15]. In our case, we define efficacy potential merely as the 'potential effectiveness' of a particular piece of advice.

As mentioned in Chapter 1, many studies have concerned themselves with the efficacy potential of advice. In many studies, they relate to the individual user's ability to perceive *self-efficacy*. According to self-efficacy theory, individual users' pass judgement on their own ability to cope with a given situation, thus developing self-efficacy beliefs for a specific domain. Based on these beliefs, individual users are able to initiate and persevere with behavioural strategies that lead to successful

[15]A treatment regimen ranges from following health advice through to short or long-term medicine use [107]

Table 2.2: Some examples of self-efficacy measurements, as taken from survey questions.

Topic	Question/statement	Reference
Email	I am confident of recognizing a suspicious email.	[272]
Software protection	I am capable of utilising anti-spyware software.	[313, 182]
Software security	I feel confident updating security patches to the operating system.	[313]
Web browsers	I am capable of setting my web-browser to differing security and privacy levels.	[313]
File security	I am capable of managing files of differing sentitivity in my computer.	[313]
Passwords	I utilise strong and multiple passwords for different online accounts.	[182]
Cyberspace navigation	I am cautious when downloading files from the internet, and am capable of checking their authenticity.	[156]
Policy management	I can read and understand information security policies for my personal devices.	[42]
New skills	I feel confident learning advanced skills to protect my information and information system.	[42, 163]
Mobile security	I set up password on your phone; I install antivirus software in my smartphone.	[313]

outcomes [241, 25]. Self-efficacy, in these cases, tends to be a generative capability that allows individual users to organise their skillsets and beliefs, which allows for an efficacy potential for these users [25].

A significant proportion of academic literature on the subject of usable-security agree with the notion of self-efficacy playing an important part in determining the users' information security practices. Their impression was that the impact self efficacy has on variables such as the users' intentions, behaviour (both actual and self-reported) policy attitudes and actual use of security software, was significant. For example, Yoon et al, [393] performed a survey on students, and established that self-efficacy has a significant impact on their intention to practice information security. Similarly, Johnston & Warketin [182] showed how self-efficacy could have

a positive effect on users' intentions to combat spyware[16]. Ng et al. [272] provides an example of the upper limit to the importance of self-efficacy, espousing that if perceived severity reaches a crucial point, self-efficacy is replaced as the primary driver in intention. However, the ability to perceive the severity of a security situation remains within the purview of self-efficacy [272].

What this means for cyber security advice is this: to enhance the efficacy potential of advice, researchers must develop it in such a manner that the advice itself helps structure and direct the behaviour of individual users towards goal setting within cyber security, and afterwards measuring the progress towards this goal [323]. However, as we saw in Chapter 1, many usable-security studies have already looked into this (for example [305, 293, 381]). Furthermore, self-efficacy is closely linked to motivation, with the level of self-efficacy needing to be higher in order to correspond to the difficulty of the faced problem [25, 352]. We know from Chapter 1 that the problem of cyber security is seen as complex and important to users, and yet the motivation to enhance self-efficacy are in many cases still waning (as explained in [160], and explored through psychological and cultural means in [146]).

2.5.6 Epistemic innocence and naïve advice

The theory that imperfect cognitive processes such as delusions and confabulations which give rise to accidental or deliberate sharing of misinformation can have certain epistemic benefits in terms of knowledge acquisition is but one factor that has been of interest in fields ranging from psychology to computer science [46, 257]. Often, users may look beyond traditional guidance [73] (see Section 2.5.4), and instead rely on more informal information [73, 308, 301] sourced from their local environment. This form of advice is known as *naïve advice* [328] and — contrary to its label — it has certain efficiency-enhancing properties, for example, when used within negotiations [348], public-good experiments [78], and certain types of games [211]. In these instances, naïve advice has positively affected how often users actualise

16

security advice. Nonetheless, the provisional way in which naïve advice is put into practice makes it difficult for experts to account for user behaviour.

2.5.7 Incorporating risk when undertaking cognitive processes

In digital environments, risk is tied to the data security and privacy of an individual's information [80]. While not synonymous, the close link between privacy and security may have a biological basis for risk, which ties into the more general behaviours and concepts mentioned within the danger control process in Section 2.5.1. Klopfer and Rubenstein [203] examined the biological drivers of privacy and security utilising animal studies and found that their preservation encompasses a multiple, layered group of concepts related to (i) safety (including security against malicious actors) and (ii) economic activity. The biological explanation for security and privacy transforms as these concepts take on normative values in human society, which is further complicated by the use of information technologies. It has long been theorised that individuals now view their digital activities as extensions of themselves [255], identifying with their online activities on an intimate level [32]. Consequently, online activity is perceived as intrinsic to, rather than separate from, the identity of the individual, which distorts individuals' perception of safe boundaries.

Despite individuals' conceptual and philosophical notions of security and privacy, which may be rooted in an 'online/offline' division, their actual activity online in some cases may flout any concern with safety and security. Contrary to many cyber security experts' opinions, this may not be an individual failure, but a systemic one. Solove in his seminal work 'conceptualizing privacy' referred to the apparent contradiction where individuals express concerns about privacy yet readily relinquish personal data in exchange for benefits like convenience or customized services. However, this seemingly hypocritical behavior stems from conceptualizing privacy too narrowly as an absolute end in itself rather than as pluralistic practices enabling other valued ends. This 'privacy paradox' arises when failing to recognize the contextual nature of privacy across different dimensions and practices. Solove

argued that individuals view privacy not in binary terms but through situational judgments, willingly giving up privacy in discrete contexts to achieve desirable benefits while still valuing broader notions of privacy [344]. Barnes [28] popularised the concept of the 'privacy paradox' further, noting that mediated communications, such as social media, require the relinquishment of privacy despite the individual, private nature of social communications; thus, there is an underappreciated loss of control over one's information, which closely linked to the conceptualization Solove mentioned. Brandimarte et al [52] discovered that, though individuals want to exercise control over their information, this may not be feasible within online digital/information environments, as there are numerous unknowns that undermine the individual's ability to grasp their actual online security.

2.6 The link between the learning of cyber security and cyber security aesthetics

In this section we briefly highlight the background that aided the development of our second and third contributions as they took shape during the development of the first.

2.6.1 Learning informally through media

There are many possible sources of security advice available to individual users engaged in informal learning [301], including retailers and vendors of security software and services [301, 347], online sources with varying levels of expertise and credibility [347], governmental organisations such as NIST (in the United States)[17] and the National Cyber Security Centre (in the United Kingdom)[18], professional media services such as the BBC and the Associated Press, and online media organisations such as Arstechnica and Motherboard, which often create and distribute security content.

The media and communications field has the greatest reach of all of these sources. In 2017, Ruoti et al [320] reported that individual users primarily learnt about

[17] https://www.nist.gov/cyberframework
[18] https://www.ncsc.gov.uk

threats through four primary sources: advertisements, news reports, television dramas, and movies. Subsequently, in 2018, Das et al [97] documented that news reports about threats (including cyber threats) were among the most-shared stories between individuals.

Social resources such as news outlets are particularly important for older users, especially when assessing the severity of threats and the pertinence of advice [274]. Even fictional news can influence individual decisions about security [128].

Additionally, the media and communications field is uniquely capable of influencing public opinion *about* security advice [320]. News sources facilitate group-based consensus [219] and set the agenda for what is regarded as an important topic, be it a presidential election [252] or an event such as the 2017 Wannacry threat [327], which may be accompanied by security advice. Given this unique influence, we accord special importance to media-acquired advice in our research. Indeed, we would argue that researchers in the security advice field have a duty to understand current practices in national and international media communications.

Studies such as that reported by McCombs [251] argue that there are two main factors that affect an individual user's perception of media-acquired security advice. The first is the degree of alignment between the user's judgment and that of the source; the second is the overall urgency of the security issue, or the threat's perceived ability to personally affect the reader, which varies depending on the user's past and risk proclivity [261]. Thus, an individual user must have both a sense of certainty about the content and a personal interest in the topic in order to feel sufficiently compelled to act on the information.

Media sources are adept at controlling both of these factors, using various strategies to prime the individual user and make them feel invested in the given topic — regardless of whether it truly pertains to them [251]. This 'taste-making' function complements their primary advice-creation function. As such, media sources act as 'knowledge brokers' within informal learning contexts, facilitating the one-way delivery of information, concepts, and ideas from professional sources

to individual users [384, 259] and ultimately influencing the opinions, actions, and personal development of the recipients of security advice [85].

2.6.2 Why aesthetics form an important field of study when analysing cyber security advice efficacy-potential

Content such as online news or blogs are often accompanied by aesthetics such as visual media [136]. There is a large body of work which makes the link between these aesthetics and news articles, usually to highlight a specific research concern. As we are concerned with efficacy potential, we present some examples with this in mind. For example, work such as [136, 54] highlight how these aesthetics (in this case the images accompanying news articles) have specific effects on the audience. For example, the work of [54] finds that accompanying aesthetics can guide future communication over the events the individual user read about. If we narrow our scope slightly towards crime (such as cyber crime), work such as [331] looked at images of factual crime across different media, and found the images are affected by potential biases and work such as [143], which found that images may frame the text in such a way as to potentially distort the realities of crime. Although not specific to cyber security, work such as the above highlights a clear connection between aesthetics and news articles, situated within our context.

The field of cyber security has similarly made use of visual media, often through the use of aesthetics to aid learning. Examples in this area range from user interface design, such as the usage (and later general abandonment) of skeuomorphism[19] as objects of association within interface design [285, 93], through to the usage of colours within e-learning platforms that may be used to teach cyber security concepts and practices in personal and corporate settings [355, 312].

When combined with informal learning processes (such as those we focus on for cyber security advice), aesthetics therefore have a large role to play within informal learning for usable-security, where the aesthetics allow for instinctive analysis of meaning and truth that users undertake when consuming visual media, whether

[19]Skeuomorphism is a design concept where digital interfaces mimic the appearance or textures of physical objects [285].

as stand-alone objects, as part of a user interface or as an accompaniment to text, thus aiding their capacity to learn informally [119, 184, 335, 70].

There is a body of literature that looks at user perceptions of aesthetics within technology. For example, work by Fogg et al. [122] found that almost half of all users of a given website made judgements regarding the aesthetics of the site that directly aided their decision about the credibility of its content. These results are further compounded by work that investigates the time taken to make these decisions based upon aesthetics; work such as Robinson et al. [315] as well as Alsudani and Matthew [13], find that work is often judged most quickly based upon its aesthetics, and in a time-frame of 3.5 seconds, respectively.

2.6.3 How aesthetics relate to the our specific study of news-based cyber security advice

Where making a link becomes more difficult is when we attempt to make a *direct* connection between *cyber security* based aesthetics within news articles. Potential justification can be found from research such as that of Ma [237], who investigated visualisation techniques for cyber security, and if we cast our net wider, work such as Shires [335], who looked at the adaptation of neo-noir aesthetics for use in cyber security visual media. There is also work by Bernal within the field of digital exhibits [36] and the transferal of security aesthetics into cyber security [133]. In particular we highlight the digital exhibits, which present a clear aesthetic link. In this work, Bernal described three recent U.S. museum exhibits on cyber security, showing how each uses different aesthetics to make the opaque digital visible. The first promotes faith in government cyber security through a futuristic aesthetic, which was designed to condition audience members to fear potential future cyber attacks as the digital parallel of nuclear warfare. The second used analogue skeuomorphism to teach individuals cyber security practices, for example utilizing low-tech wooden keys as passwords and rotating dials to simulate cryptography—to portray the internet as a mechanical system that individual citizens could and should secure through routine practice. The third featured artists questioning surveillance overreach through a

dystopian aesthetic, in which a pedagogical tone intended to shock viewers into questioning the overreach of surveillance technology was used [36].

The image-based aesthetics mentioned above can be analysed from a variety of different perspectives, ranging from content analysis through to semiology and discourse analysis [304]. For example, Rose states that image analysis "explores how images construct views of the social world" by analysing the visual elements of the images and their contextual meanings [316].

Accordingly, it should follow that an analysis of the aesthetics which accompany news articles about cyber security may also deliver insights into their effect on the individual user. Such an analysis can also aid in the hypothesising as to how and why these images were constructed and chosen for their respective articles. In Chapter 6, we explore the symbolic link between aesthetics and cyber security advice, and highlight how aesthetics can present potential challenges to individual users.

2.7 Summary

In this section we review how what we learnt in this chapter relates to our understanding of the research questions. We discussed:

- In order to form an epistemological basis for our research question RQ1 (*Given that users have complex motivation and decision-making patterns when interacting with cyberspace, can we establish a more contextually appropriate environment in which security decisions are made by users?*), we introduced the concept of cyberspace, a human-constructed techno-spatial domain with perceived similarities to the physical world we occupy, and include macro-environments that are subject to both physical and digital forces. We then introduced cyberspace security, its origins within physical security and how these have translated into cyberspace. We followed this with an overview of usable security, which is the study of how abstract concepts in security are turned into processes that a user can execute in order to remain secure, as well as their method of study. Usable-security is paramount to our context,

for if cyberspace is the environment we consider to be *where* the user needs to remain secure, then usable-security is the core concept of *how* the user can remain secure in cyberspace, as it provides a way of studying the processes and efficacy potential of doing so.

We clarify the *what* of a user, which we term the 'individual user', that we take forward in our scope (in Section 2.4.1). In our case, the individual user is someone who owns a system or device which maintain a connection to cyberspace. When we say 'owning a system' we are referring to a wide variety of potential examples. One such individual user may be someone whose primary connection to cyberspace comes in the form of a single smartphone connection to a mobile network (for example, in third world nations, where many own a single connected device), or someone with a sophisticated home-network set-up consisting of multiple devices which may have multiple users. In this case, the individual user we refer to are those who maintain domain over this network (for example, single-parent household with 3 users total, only the parent is counted within our scope).

Unless appropriate in the context, we avoid mention of the individual user's age-group or other demographics other than to assume basic literacy and a high-school education. Not all of cyberspace is populated by our individual users. Other entities within cyberspace exist, and these were explored in Section 2.4.2. Nation states, corporations and others all maintain motivations in cyberspace, and help to shape it.

- We provided a definition for the experts who provide security advice through our dissemination vector (see Section 2.6), and discussed the benefits and drawbacks to both this definition and the to the experts' behaviour and epistemological/performative backgrounds.

- We also discussed two main areas that this dissertation views as potential issues within assessing the efficacy potential (see Section 2.5.5), of our individual users: epistemic innocence and the manner in which user calculates risk

potential. Both of these ideas, one from the world of philosophy, the other from risk analysis, allow an insight into the opaqueness of the individual users' potential motivations. Chapter 4 contains a more in-depth discussion on these topics.

- Moving on to RQ2: *Considering that the dissemination of security advice about cyberspace takes place through a multitude of vectors, is it possible to measure the efficacy potential of such advice through one such dissemination vector?*. We built upon our initial definitions of cyberspace and the individual user to to refine terminology such as what we explicitly mean by security advice. We began these deliberations by learning how our individual user may learn about cyberspace, and security advice relating to cyberspace (in Section 2.5, who our advice disseminators are (in Section 2.5.4), and established what we mean by efficacy potential (in Section 2.5.5). In particular, we looked at informally learnt advice, how it is created, and disseminated through at least one dissemination vector (media generated cyber security news and advice, in Section 2.6). We found that there are epistemological issues with our individual users' self-efficacy and efficacy potential that receive exploration in Chapter 5.

- For our final research question, *What do cyber security aesthetics look like to an individual user, and what are its efficacy potential?*, we discussed both the causal efficacy potential (in Section 2.5.5) that could be influenced by viewing media bundled with cyber security content, as well as the effects of aesthetics. These are most pertinent to Chapter 6.

The next chapter will provide a detailed overview of the methods used in this dissertation.

3
Methodology

In this chapter, we introduce the methods used to underpin the research described in this dissertation. We highlight how they are combined and used to drive and validate our contributions.

Gathering empirical evidence about the efficacy potential of users' security decision-making process is difficult. Observing decisions in the real world, as highlighted by several security studies mentioned in the previous chapter, is problematic because of selection and observation effects and the "other-minds problem". Utilising the workings of the other-minds problem, we assume that although users who choose to follow cyber security advice may differ from those who do not, due to their differences in risk approaches, self-efficacy and other attributes that influence behaviour, these differences can not be effectively measured.

Hence, with these elements in doubt, under 'normal' circumstances a model may be constructed which encompasses all possible behavioural outcomes, and which an independent variable is selected to be randomly varied in order to define a causal relationship. However, a complete model of cyberspace and its behavioural outcomes would be far beyond the scope of this dissertation (if not infeasible). Instead, in order to arrive at a set of conclusions which retain external validity (in the sense that the results may generalise beyond the confines of our studies), and to reconcile our previously mentioned difficulties, this dissertation utilised both a

form of conceptual modelling, and empirical observations. The conceptual model aimed to create a detailed account of cyberspace's structure and actors, and the empirical work describes the state of what we defined as cyber security advice situated within the context of our model. In particular we combine these methods in order to reflect on the concurrences and discrepancies between the assumptions made when creating the model and the associated empirical observations, modelling assumptions and empirical observations.

The remainder of the chapter is as follows. Section 3.1 describes the Blended Theory, the specific methodology behind our conceptual model. Section 3.2 describes the methods used to collect and clean empirical data. We conclude with a short summary in Section 3.3.

3.1 The conceptual model

Reminding ourselves of one of the ideas surrounding the dissertation in Chapter 1, where, with a greater understanding of the environmental risks, we may be able to provide an alternative view of user-behaviour. This leads us first to the methods chosen for C1.

Empirical data collected either through surveys or experiments form the primary way in which usable-security researchers attempt to answer issues highlighted in the research problem (see Section 1.1). Therefore, it may at first appear to be counterproductive to begin our set of contributions with a conceptual model, derived utilising a methodology that does in itself directly incorporate the empirical findings of others. So, why begin with such a model? We refer the reader to work such as that of Hausmann [155], whose work into the relevance of economic theoretic models suggested their usefulness extends primarily into the exploratory, as a guide towards the possibilities of a given hypothesis. They could further be seen as representation which could isolate the major forces and processes of a system. Once isolated, these forces can then be empirically tested in order to assess the model's predictive success and adapt its parameters [149].

Our model is designed utilising a qualitative methodology derived from concept blending. Concept blending is a cognitive process that allows us to combine elements from otherwise separate conceptual spaces, and use these to develop a new unified domain (or environment, as in the case of cyberspace). We use this environment to derive axioms of cyberspace [115]. Taken separately from mathematical (such as [48]) or economics-based blending of theories (such as [247]), which are primarily algorithmic in nature and therefore unambiguous, concept-blending allows us to present descriptive results which can take a certain perspective (in our case, that of the user), and allows us to inhabit their conceptual space or 'lebenswelt'[43, 48].

When taking concepts from separate domains, we can create similarities between the separate inputs through abstraction and generalisation between them. According to Aristotle's comparison theory [18], metaphors establish a relationship between two or more distinct concepts, thereby enabling implicit comparison [2]. Furthermore, by relying on standard pragmatic and semantic terms, metaphors can make previously unknown concepts instantly familiar. Thus, metaphors can serve as associative tools that disrupt standard ways of thinking about a given topic. Indeed, in fields like anthropology and psychology, metaphors have been used to centre human experience [175], promote associative and holistic thinking [358], and render cognitive associations and 'mental models' legible for systematic analysis [117].

As per the 'interactive' view of metaphors described by Tourangeau and Sternberg [361], metaphors present neither inert nor novel information; they are not a restatement of the original subject, but they are also not statements in and of themselves. Instead, they provide a new vantage point on established concepts — a kind of 'framing' effect [267] that allows us to derive new meanings from existing circumstances.[1] Thus, in the context of cyber security, metaphors can provide a new space in which to consider cyber security advice, free from the constrained ethical reasoning about responsibilities that, it might be argued, can sometimes characterise traditional usable-security research. As such, they can provide a helpful first step towards considering security advice from the user's perspective.

[1]We refer the interested reader to work by Davidson [99] and Tourangeau and Sternberg [361].

To account for the environment that is cyberspace (an axiom the reader will have to take on-faith until explained in Chapter 4), we adapt Fauconnier and Turner's [115] blended theory to partially integrate and systematically map the operative metaphors within the larger epidemiological metaphor. This approach was derived from Conceptual Metaphor Theory (CMT) [215], which is the traditional methodology for metaphor-based work. In this framework, metaphors are analysed as a set of stable and systematic relationships between two otherwise competing domains. For example, consider the following expression: "The governing body has kept us in the *dark* about this important matter". In it, language from the domain of human vision has assumed a new meaning, conveying a lack of knowledge or understanding about a given topic. According to CMT, this 'mapping' between domains is reflected in the neural connections that preserve this association within someone's long-term memory [134].

Blended theory also involves the use of mental spaces and four-spaces mapping models. Rather than having two domains serve as an input and output, instead we will utilise a four-space model with two input domains, a generic space that represents the structure shared by the inputs, and a further space where we can blend the metaphors into a new structure. This allows us to transcend the unidirectionality of traditional metaphor mapping by creating a structure where both domains serve as useful inputs for our model [115]. The visualisation of this model in Figure 3.1 reveals a structural similarity with models from blended-space applications, such as augmented reality, where physical and digital spaces are meant to mix with one another [34]. We elaborate on the way in which this model builds our conceptual model in Chapter 4.

3.2 Empirical data collection and classification

This section primarily covers the methods utilised to gather, store and analyse data for what we see in Chapters 5 and 6. We use two primary data sources, the first of which was a data-set of news articles we refer to as a 'corpus'. The corpus consisted of 15,422 (English language) news and online magazine articles from

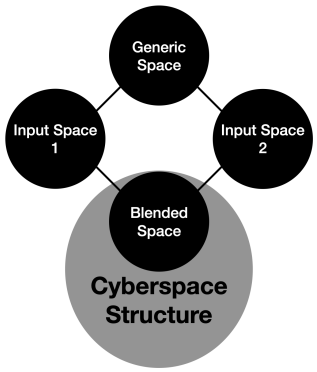


Figure 3.1: The four-spaces model as adapted from Fauconnier and Turner [114].

North American (US and Canada) and UK-based sources, as well as some historical data stretching back to 2000. We ascribed broad classifications to specific advice, ascertained the dominant methods of advice construction and dissemination, and analysed their potential efficacy potential over time. The second data source was an data-set consisting of images, which we refer to as an 'image-set', which consisted of an original 3,757 usable images taken from the public domain before processing. Both data-sets were generated by utilising web-scraping methods that allowed us to generate a sample of sufficient size and scope from we could answer the questions we had set ourselves. Web-scraping is a popular digital research technique that allows researchers to automatically capture freely available online data — that is, data that does not require privileged access [246] — via the use of scrapers. Both tools were developed in Python and made use of a search methodology discussed in Section 3.2.4. Rather than incorporate additional system logic to ensure that all gathered data were viable candidates for analysis, we chose to refine each data-set through subsequent data cleaning. In the rest of this section we give consideration to the data-collection tools and the analysis processes before discussing the search methodology to inform their usage.

3.2.1 Generating online-sourced news data

We designed a software tool in Python which would enable the automatic collection of news articles that would fulfill our needs, which we term the 'news-scraper'. We

Table 3.1: Basic functional requirements for the news-scraper.

Requirement	Detail
1	The ability to systematically search for news articles within a set time frame utilising pre-set search queries.
2	The ability to extract the full content from news articles.
3	The ability to extract metadata, including publication date, author(s), titles, source names, and country of origin, for further analysis.

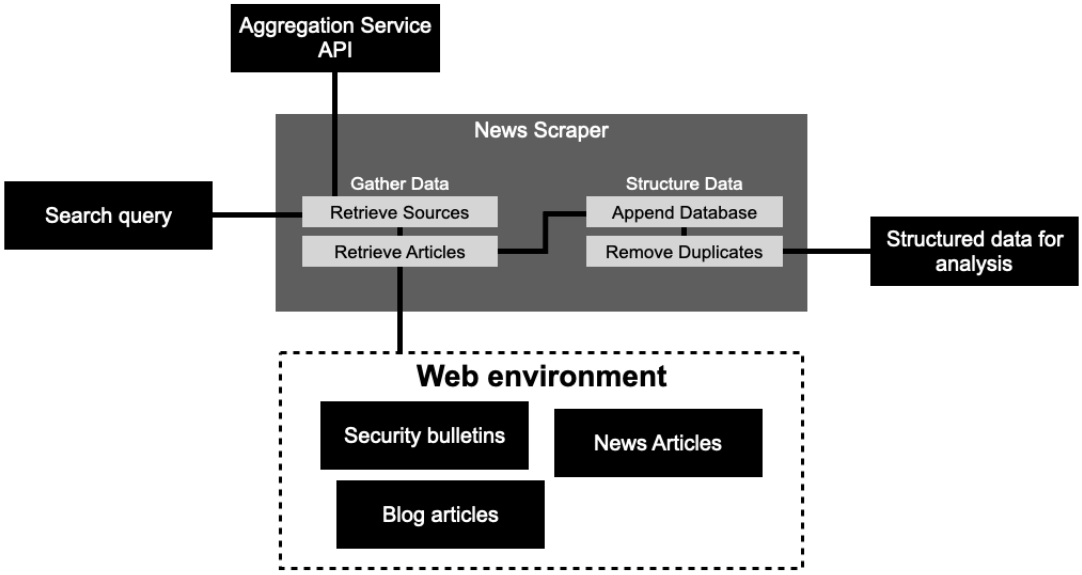


Figure 3.2: An overview of the news-scraper tool.

highlight its basic functional requirements, which are shown in Table 3.1; these gave rise to the abstract architecture depicted in Figure 3.2.

We utilised a news-aggregation API[2] to filter content from a variety of unstructured and structured news sources were consistent with our definition, and we added functions to enable the complete capture of content, in accordance with Requirements 2 and 3. The captured data was then fed into a data-storage pipeline before being converted into a flat-file database storage solution. Incoming data was merged with existing records when required to avoid duplicate data.

[2]A paid solution sourced from NewsAPI (`https://newsapi.org`).

3.2.2 Classifying online-sourced news data

As we saw in Section 2.5, individuals require actionable elements within their security advice. We therefore utilised an ontological framework to help us classify and integrate the data collected from the sources queried by our news-scraper. We chose our ontology according to our idea of efficacy potential. We therefore required an ontology which, while evaluative in nature, could demonstrate effectively that a particular level of security has been achieved. Hence, we conducted a non-exhaustive search for an ontology through work such as ENISA's *IoT Security Standards Gap Analysis*[3] and a report by the UK's Department for Digital, Culture, Media and Sport, mapping security recommendations for various audiences[4]. We additionally looked at including only those ontologies that have received frequent updates to include concepts recent to our individual user such as edge computing, e.g. [295]. We found that many ontologies were aimed at a technical or policy audience and often included several layers of abstraction within the work, used vaguely defined terminology or simply did not include our original requirement of actionable security advice.[5]

An ontology by the Center for Internet Security (CIS)[6] was chosen, as we found it provided us with actionable security advice that can aid towards self-efficacy. Although it was not intended for individual users, this ontology does prioritise risk-based security and focuses on the practical mitigation of these risks, which it accomplishes by identifying and utilising 20 domain-specific CIS-vectors that represent practical and actionable remedies for security threats. Furthermore, the CIS ontology has been aligned with other ontological frameworks such as that of NIST to allow for easier adoption by organisations and projects.[7] A high-level

[3] `https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis`

[4] `https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards`

[5] For example, high-level policies for IT professionals and business executives were considered to be out of scope.

[6] `https://learn.cisecurity.org/cis-controls-download`

[7] `https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-CIS-vectors/`

Table 3.2: Basic functional requirements for the image-scraper.

Requirement	Detail
1	The image must be derived from a news or blog article that directly addresses at least one aspect of cyber security and / or explicitly contains our search terminology. Blog articles were limited to tutorials, editorials, tool demonstrations, and discussions of technical reports. Due to the nature of the assessment and the search methodology, we only retrieved images from English-language sources.
2	The image cannot be a corporate logo or advertisement (like the lead slide of a corporate presentation).
3	The image must be accessible and not hidden behind a paywall or other kind of lockout mechanism, as these obstacles restrict the amount of text that can be retrieved, making it difficult to explain why some images were included in a given article or blog post (that is, the role that the images serve in relation to the text).
4	The image must be at least 360x640 pixels for ease of processing.
5	The image must be in either .jpg or .png format.

version of the framework can be seen in Figure 3.3. The individual CIS-vectors are discussed in detail in Chapter 5.

The CIS ontological framework provides us with the requisite entity types and properties which are ascribed to individual news articles within the corpus as additional metadata. Thus, we are able to use the ontology to define the entities, relations, and other factors that can be extracted from the corpus. The ontology also serves to focus the corpus and to restrict our vision to the research objectives, as the language utilised within security can range from extremely specific to extremely ambiguous [319]. In many cases, this range can make it difficult to apply an ontology to specific news articles within the corpus.

3.2.3 Generating online-sourced image data

Applying these functional requirements onto a Python-developed image-scraper and applying the search methodology shown in Section 3.2.4 yielded an initial image-set of 4,784 images. We then counted and removed all duplicates[8] and then down-sampled our images to a standard pixel resolution. This yielded a final image-set of 1,027 individual images, which we used for analysis.

3.2.4 Classifying online-sourced image-data

In order to classify the images in our image-set, we utilised feature extraction — a form of quantitative image classification wherein categorising labels are assigned to images based on specific extracted features. For our image-set, we chose to begin with object recognition to identify any potential semiotic objects (or signs) before moving onto semantic categorisation (categorising emotion or other subjective features).

The Bag-of-Words Model

We utilised a variation of the Bag-of-Words (BoW) model to provide human-assigned classifications for our image-set. The BoW model is often used in situations where images require text categorisation but word order is not particularly important. We based our model on work by [91], selecting three knowledgeable cyber security researchers to manually locate dominant interest points in individual images (recreating feature extraction) and derive labels that represent these interest points. This solution presented several advantages over an automated set-up, as the expert knowledge allowed for more concise labelling, the ability to label occluded objects that would have been missed by automated methods, and the ability to construct a clearly defined codebook for our classification labels based on prior expertise. However, the contextual awareness these experts brought to the labelling exercise may have introduced some biases. This limitation could be mitigated in future studies by recruiting a wider range of annotators.

[8]We counted the number of duplicates to assess the extent of duplication within cyber security aesthetics.

Measuring image similarity through colour

To confirm the internal consistency of each image class derived from our classification process, we utilised Weller and Weastneat's [383] quantitative, colour-based method for measuring image similarity. This involved transforming each image's pixels into 3D coordinates to produce a multidimensional color histogram for each image, then using the earth mover's distance measure [317] to compute the pairwise distances between histograms. We opted for this method over contour-recognition for object classification (as used by [145, 374]) because we had already classified our images according to their dominant features. Colour similarity measures also allow us to more confidently make qualitative assessments relevant to our research questions. Colour similarity heat-maps for each class will be shown in Chapter 6.

Establishing search parameters for sample generation

To establish the list of search terms needed to guide the generation of data-sets from the above tools, we followed the precedent of Schatz et al [326], who used Google Trends to automatically collect real search terms employed by the target audience. [9] This focus on user-centred definitions excluded the possibility of replicating the work of Humayun et al [169], who looked at primary studies undertaken within academia. Instead, we followed the *Systematic Mapping Study* protocol presented by Kosar et al [207].

We defined a set of base search terms (for example, 'cybersecurity' `OR` 'cyber' `AND` 'security') and then added search terms derived from Google Trends (online OR advice OR protection OR protect OR prevent OR preventative OR tips OR email OR social network OR password OR hack OR hacked OR hacking). All search terms were technology-agnostic — they did not include explicit references to specific products or services. The image-scraper then returned all images that corresponded with content that included these terms within the title or body text. Though not

[9] Schatz et al [326] sought to derive a more precise definition of security, and so they collected the terms that individuals used to search for security content.

exhaustive, this strategy yielded an image-set that adequately represents operative definitions of cyber security, as actualised by users.

3.3 Summary

This chapter justifies the use of mixed methods in this dissertation. A metaphorical model of cyberspace is used to explore forces and actors and to inform our research direction, and empirical data is collected to understand the concurrences and discrepancies in the assumptions made when creating the model. Our model provides a richer picture of the environmental level of cyberspace, and our empirical results on news-generated cyber security advice covers the epistemological level. The sample generated for our image data-set provides for a representation of cyberspace the phenomenological level. Insights from both levels will be interpreted in the context of empirical evidence and sociological critiques of cyber security that aims to ascertain and enhance the efficacy of cyber security advice.

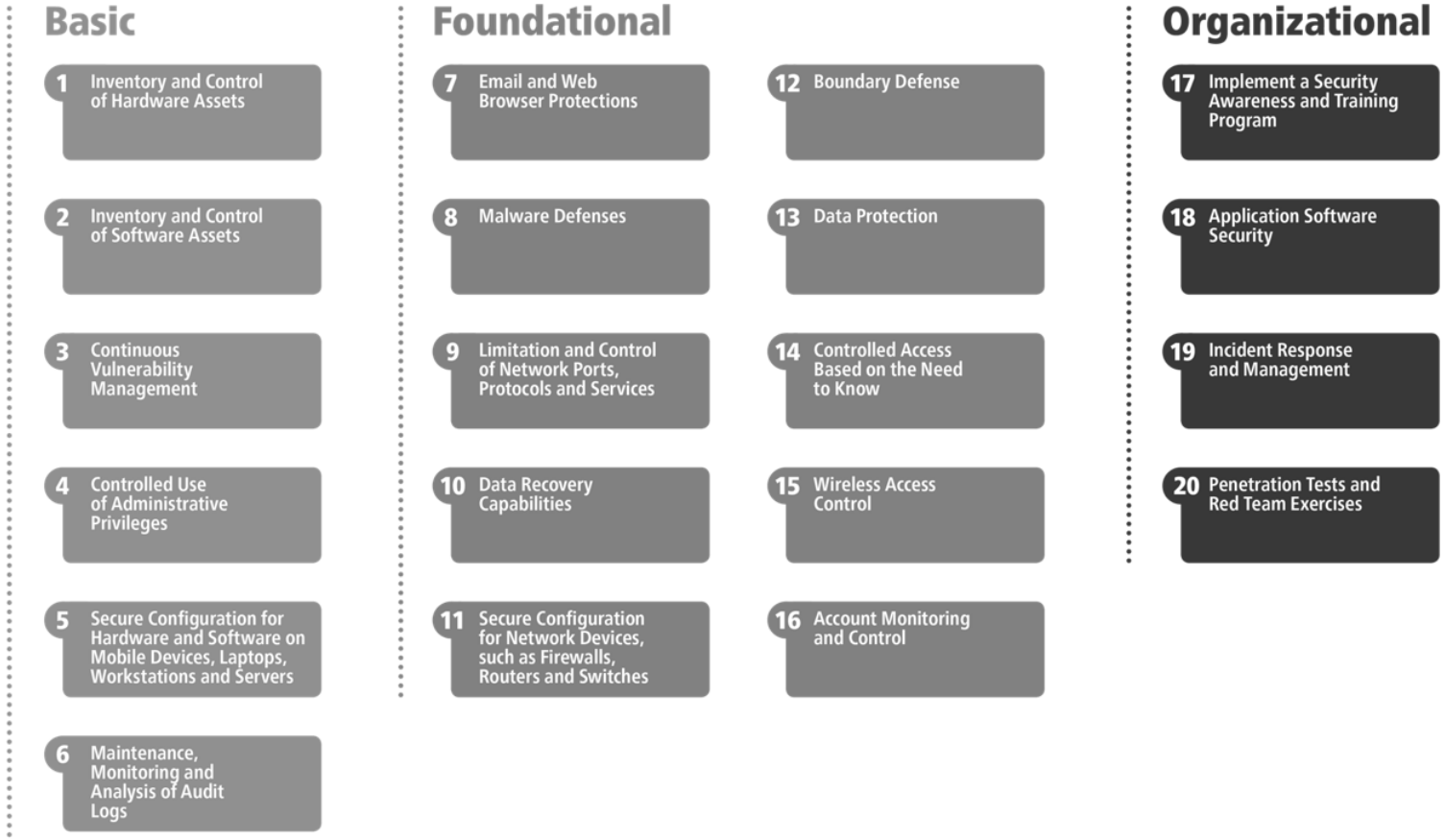


Figure 3.3: An overview of the CIS-vectors ontological framework [10].

4

Cyberspace through the eyes of the user

In this chapter, we use metaphor to build an exploratory conceptual model of 'cyberspace' espoused in Section 1.1. We then use the ideas from the model to build and execute an experiment meant to provide further understanding into user behaviour inside this framework. The chapter is laid out as follows. Section 4.1 presents additional background into how our conceptual model was derived from metaphors in adjacent fields and how these fields were chosen. Section 4.4 introduces the model. Section 4.5 presents an experiment to test the model in an empirical context. Lastly, section 4.6 discusses the results individually and then how they relate to wider context of our research question.

4.1 Building a conceptual model: Background

In Chapters 1 and 2 we learnt about one of the core concepts troubling usable-security researchers today, namely that of the user's disengagement with security advice. Herley [160] provided three possible reasons for this: (1) users are simply unmotivated; (2) security advice is inaccessible; and (3) the rejection of security advice is rational from a purely economic standpoint. Herley proceeded to argue for the third interpretation using economic rationality as a metaphor to describe users' engagement with security advice. We took inspiration from this metaphorical

strategy in the research described in this chapter, as it makes sense of individual behaviour within a specified context [191]. Accounting for this context may be necessary to demystify users' ostensibly careless behaviour, especially insofar as users' risk-assessment contexts (and, thus, perspectives) differs from that which experts prescribe. Instead of the purely economic reason which Herley describes, we expand this to include risk-based choices (see Section 2.5.7) made in a complex environment, such as that described in Section 2.1. From our research problem stated in Section 1.1, we take the initial axiom that users indeed have complex decision-making habits, especially when interacting with cyberspace, and ask whether we may establish a more contextually appropriate environment in which security decisions are made by users.

Therefore, in cyberspace, do users perceive risk as discrete — a property of individual online events that can be avoided with education and due diligence — or as an innate quality of online spaces that can only be managed by wholly avoiding these spaces? This is where we begin to refer to cyberspatial risk. We hypothesise that, where cyber security experts conceptualise security according to discrete risks, users conceptualise security according to environmental (cyberspatial) risks. As such, when analysing the cause of an infection, cyber security experts are more likely to emphasise users' agency (in our case, users' ability to influence or control their environment), hence the links to self-efficacy (discussed in Section 2.4.2). These discrete risks, in the view of experts, can be overcome through formal or informal education, informal or otherwise. Instead, in the hypothesis we argue that users may be more likely to emphasise surrounding circumstances. If this is true, then the rationality of users' risk-taking behaviour must be determined with regard to their environment. In order to establish this hypothesis we develop a three-part response:

1. First, we provide a sufficiently detailed account of the metaphorical environment itself, including the entities that exist within it. To this end, we explore the cyber security environment using metaphors that have lent themselves to cyber security-related descriptions. In particular, we look to the field of healthcare, where the reasoning behind risk-taking behaviour is often

examined with regard to the transmission of disease, and where risk-based activity affects the likelihood of harmful or even fatal encounters.

2. Second, we specify the structure of cyberspace to clarify how different entities interact with each other and with the environment itself. Thus, after introducing our metaphors, we organise the environmental elements into micro- and macro-level actors and clarify their relative agency. In so doing, we can provide context for high-risk behaviours.

3. Third, we simulate a user's navigation through this environment to understand what they are likely to experience and, by extension, to clarify the reasons why someone might perceive risk as environmental rather than discrete. If risk is discrete, we expect that these risks will manifest as opportunistic entities that thrive on risky behaviour; thus, high-risk behaviour would yield a higher-than-average infection rate. If risk is environmental, we expect that viruses will operate as predators that, while not necessarily looking for a victim, will grievously harm the victim if an attack is initiated; thus, high-risk behaviour would not necessarily affect the infection rate.

4.2 Cyberspace ecology

For an introduction to the metaphoric methods utilised here, see Section 3.1. We begin by reminding ourselves of the definition of cyberspace provided in Section 2.1: *Cyberspace represents a human-constructed techno-spatial domain with perceived similarities to the physical world we occupy, and includes macro-environments that are subject to both physical and digital forces.*

We need to take this spatial metaphor further, before it becomes possible to depict cyberspace as an environment or ecology. Indeed, as even hardware networks bear a certain resemblance to artificially created biological environments, insofar as they contain both macro- and micro-systems that link together to produce navigable spaces for humans [125, 38]. Furthermore, many existing models of cyberspace utilise another metaphor borrowed from biology and biodomes: that

of evolution. For example, Dorogovtsev [104] specifically highlights similarities between the evolution of protein structures, metabolic reaction networks, and various other biological systems, on the one hand, and the ever-developing nature of hardware infrastructures, on the other. In both cases, networks must be discovered, catalogued, and navigated to improve human health and well-being.

This overlap between the technological and biological is not entirely surprising, as technological developments respond to and inspire deeply biological needs, co-existing with other elements in the larger physical environment. Similarly, technological developments engage, to some degree, with biological risks. Though we conventionally distinguish between biological risks and technological risks — the former in relation to the physical well-being of the human organism, the latter in relation to the security and privacy of an individual's information [80] — Klopfer and Rubenstein [203] found that the need for privacy and security may have a biological basis in the need for safety and economic security. Furthermore, it has long been theorised that individuals now view their digital activities as extensions of themselves [255], identifying with their online activities on an intimate level [32]. Consequently, online activity is perceived as intrinsic to, rather than separate from, the identity of the individual, which distorts individuals' perceptions of safe boundaries [255].

4.2.1 Epidemiological metaphors in cyber security

Given the prevalence of the bio-technological cyberspace metaphor, it is unsurprising that efforts to defend individuals from risks in the online environment borrow language from similar efforts in the offline environment. Indeed, of the two main metaphors used to describe cyberspatial threats (conflict metaphors[1] and 'computer viruses'), the computer virus metaphor has become ubiquitous, despite the fact that it does not enjoy universal praise within academic circles (see, for example, the

[1]Conflict metaphors are characterised as metaphors that present harmful online events as 'attacks' [51], and they have proven useful in international relations and military doctrine. They have also been used sporadically in scientific literature [228, 351].

contribution of Theng and Thimbleby [357]). This is largely due to the metaphor's ability to describe certain activities and behaviours within the domain.

Kraus [210] determined that the idea of a computer program behaving like a virus dates back to Von Neumann's work on self-replicating programs in the late 1940s [370], finding that biological and technological viruses shared many characteristics, such as their self-replicating nature and their dependence on a host to execute code and obtain outside energy [210]. As per their biological counterparts, computer viruses can mutate [56], so there may be regional variations in their occurrence [278]. Given this overlap, computer virus metaphors are often derived directly from the medical field of epidemiology [38, 138, 76].

4.2.2 More-than-metaphorical commonalities

The commonalities between cyber security and epidemiology extend beyond metaphor [264]. Both fields exhibit the problem that individuals respond in counter-intuitive ways to real threats (as mentioned by Mgrath et al. within epidemiology [249], and by Redmiles in cyber security [306]). Despite individuals' professed concern for their physical well-being, their increasing personal investment in the security and privacy of their online information, and the fact that risk of viral transmission can be mitigated both off- and online, humans often seem to flout any concern with security in both settings. Below, we outline common reasons for, and outcomes of, this discrepancy.

4.3 How individuals learn about cyber security in comparison with epidemiological threats

It is worth remembering what we saw in Chapter 2, that most users do not receive the kind of formal security training obtained by cyber security experts. This can be extended to the medical domain, where formal training is most likely absent. Instead, they learn to navigate both online and offline environments through *informal learning* [242, 281]. Informal learning occurs primarily when individuals actively choose to seek out new ideas, typically in response to an internal or external

impetus [242].[2] Therefore, it is usually unstructured, occurring outside of classroom settings and without direct interaction with security experts [347].

Thus, research in both epidemiological and cyber security settings suggests that individuals do not wield enough knowledge to meaningfully control their environment or what happens to them within this environment (the privacy paradox of of cyber security [28].

4.3.1 Similar failings in both advice types

Experts in epidemiology and cyber security try to intervene in order to help users interpret their environment, and to equip users with the information needed to identify and alleviate threats. However, assessing the prevalence of real threats is difficult even for experts (an epidemiological example would be conflicting guidance for the wearing of personal protective equipment during a pandemic [218]). Many previous studies in cyber security have attempted to crawl the web in order to determine the prevalence and type of malicious software [350, 16, 204]. Moshchuk et al. [268], for example, conducted a longitudinal study wherein they crawled the web for malicious executables. They found that, of the 18 million URLs sampled, spyware made up 13.4% of executables, whereas scripted 'drive-by-downloads' comprised 5.9%. The study found that the density of these executables decreased over time, suggesting an increasingly secure web. Provos et al. [298] conducted a similar study, finding that, of the 4.5 million webpages sampled, nearly 10% contained identified viruses. *Security Week* [362] reported that, of 1.94 billion webpages, 18.5 million contain viruses at any given time, yielding a 9.54% virus prevalence rate. Overall, these and other studies indicate that a virus is present in approximately 10% of websites. Unfortunately, there is no information about how this rate varies in different contexts, nor about infection patterns, making it difficult to ascertain real

[2]Based on this intentionality, we distinguish between informal learning and its subcategory of *incidental learning* [242, 58], wherein individuals unintentionally learn something as a by-product of carrying out other tasks [242]. This is common in technological environments, where processes unfold without significant conscious thought on the part of the user. Incidental learning may occur when one's attention is directed towards a potential fault, which allows for increased awareness of technological processes that may otherwise have remained hidden [158].

risk levels. Indeed, Ugarte-Pedrero et al. [366] utilised data from several sources to ascertain whether common biases about virus creation levels were justified. They found that, out of a sample size of 172,000 forms of viruses, the vast majority belonged to only a few virus families. Additionally, they found that many of these viruses were either unable to cause harm or relied on user interaction to inflict harm.

Similar incongruities arise in studies of sexually transmitted infections (STIs), where researchers examine the behaviour of people who engage in frequent high-risk sexual activities[3] and compare transmission rates with the general population to ascertain whether high-risk sexual behaviours do in fact lead to higher rates of STIs. Counter-intuitively, Coughlan et al. [89] found that clients of sex workers reported lower incidences of STIs than controls (despite having a greater number of sexual partners). Seib et al. [329] reported that sexual disease transmission among sex workers and clients is lower than expected and largely context dependent. McLaughlin et al. [254] conducted a meta-study and systematic review of STI rates across China, finding that rates were not uniform and that certain 'high-risk' groups reported lower rates of STIs than those deemed 'less risky'. They concluded that better methodologies are required to reliably understand infection vectors and risk factors and to deploy effective risk prevention strategies. McGrath-Lone et al. [249] performed a few studies that compared sex workers and clients to their non sex-work counterparts. Only some STIs were more prevalent in sex workers than in control populations. Overall, results are heterogeneous, even within single studies, ensuring that passing a verdict on the efficacy potential of advice in these areas remains very difficult.

4.4 A conceptual model for cyberspace

In Fauconnier and Turner's method [115] described in Section 3.1, we saw the four-spaces mapping model for metaphor blending. We define these spaces in Table 4.1.

[3]For the purposes of this chapter, 'high-risk sexual activity' is defined as sexual activity with a higher likelihood of negative outcomes, such as becoming infected with an STI. Thus, a lower number of sexual partners and use of protection decrease the risk of contracting STIs.

Table 4.1: Our input spaces, adapted from Fauconnier and Turner [114].

No.	Input type	Space name
1	Input space	Cyber security
2	Input space	Epidemiology
3	Generic space	We simply term it as a physical space and includes only those elements with high-level commonalities between the two input spaces.
4	Blended space	Our 'cyberspace structure'.

We further elaborate on this model in order to arrange the blended metaphors from our cyberspace structure into a hierarchy, yielding a metaphorical environment with clearly defined levels. The reason for this is due to the way we defined cyberspace, which already utilises metaphor[4]. As with natural ecosystems, cyberspace is composed of various hierarchical systems. We conceptualise two categories within cyberspace: the *macro-level*, the mapping of which can be seen in Figure 4.1 and the *micro-level*, which are further divided into *actors* and mapped according to the metaphor level. The mapping of the micro-level can be seen in Figure 4.2. As an interpretative example, we take a look at the macro-level, where from the online space (our first input space, taken from cyber security) we have the ready-to-hand example of the *Expert*, which we can project very easily into the generic space as a *human-being*, which in-turn translates directly into the *epidemiologist* from the Ecosystem mental space. The point of the expert's representation out of these spaces in our blended space is to serve as a springboard for appreciating the tensions and similarities between the input spaces, where we can use the literature to support the legitimacy of our blend[5].

We designate those processes or systems that (1) operate automatically or autonomously and (2) have indirect influence over the quality of the user's experiences in cyberspace as micro-level actors. These actors can help or harm the

[4]As a reminder, a *techno-spatial* domain, which we take to mean a generic ecosystem that continually evolves into more complex and interconnected forms (see Section 2.1).

[5]Work such as Dulleck and Kerschbamer [106], who in their work on the economics of credence highlighted the similarities of the fields both relying on relies on expert opinion and heuristics to build legitimacy, or that of Cains et al. [65], who used a multidisciplinary context to elicit definitions for cyber security.

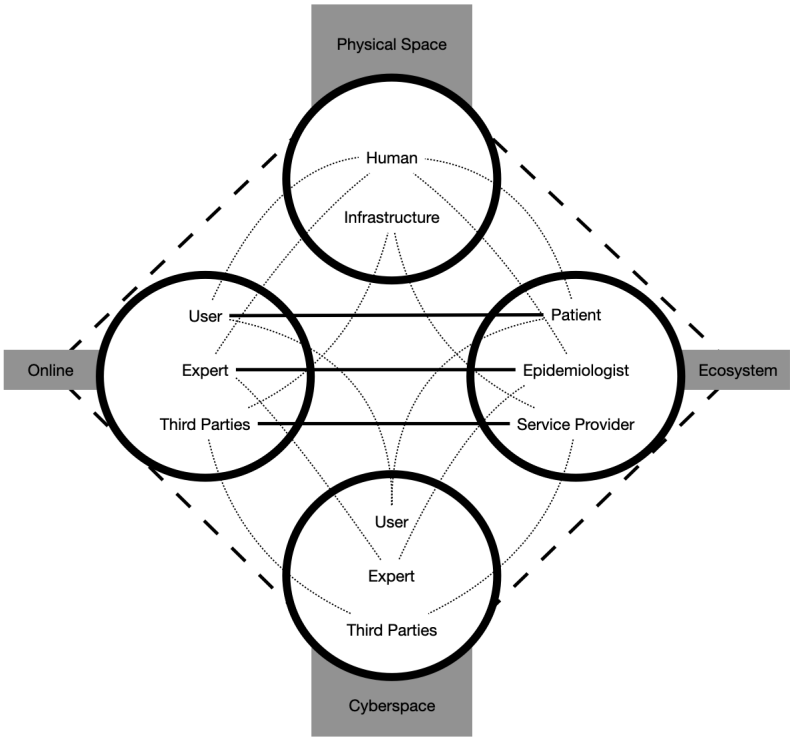


Figure 4.1: Our blended concepts shown at the Macro-Level. The solid lines represent connections between input sources, and the dotted lines represent connections in spaces. At the top we find our generic space, labelled "Physical space'. On the left-hand side, we have the "online', which is our first input space, on the right, "epidemiology' is represented form our secondary input space. The two spaces come together in our blended space of "Cyberspace".

user, and we specifically consider only those micro-level actors that are relevant to our metaphors. These include:

1. *Users*, the principal macro-level actors who interact with cyberspace by utilising a hardware–software network (over which they may or may not have control). The user is subject to interference from other macro and micro-level actors. In an epidemiological sense, the user may be either a patient,someone who receives medial advice or simply someone operating within an ecosystem in which viruses are present.

2. *Experts*, macro-level actors who perform a function similar to that of health professionals in healthcare contexts (see Section 2.5.4). They develop security

advice out of a need or want rooted within observational data [1], threat-related data [363, 72, 341, 178, 373], and data arising out of the continuous development of tools and services, including those available to malicious actors [79, 379, 71].

3. *Third parties*, who play an incredibly important role in cyber security, both physically and metaphorically. Because spatial environments — whether biological or technological — can be rather opaque to humans who do not have significant prior knowledge to astutely navigate them, third parties act as guides or brokers who mediate user-generated data. An epidemiological equivalent to third parties would be organisations maintaining health infrastructure, or providing health related services.

1. *Cyber security processes*,[6] which encompass myriad systems that are intended to protect users from online harms.

2. *Sub-processes*, which are more neutral micro-level actors that aid in the successful navigation of cyberspace. These range from navigation algorithms that aid users in either digital [353] or physical navigation [55] through to queuing or prioritisation systems or bots that may aid or compete with users, depending on their design. The vast majority of these tools are typically under the direct or indirect control of a third-party macro-level actor and cannot be directly accessed by users.

[6]While ICT (Information and Communications Technology) security [371, 389] is concerned with protecting informational infrastructures and information security is concerned with protecting all aspects of information — including processes and data not directly generated and/or stored by the infrastructure [322] — cyber security In a technological context, the systems that protect informational infrastructures are called information and communications technology security (ICT security) [371, 389]; the systems that protect all aspects of the information itself — not just ICT security, but all of the processes and data not directly generated and/or stored by the infrastructure [322] — are called information security. Cyber security goes even further, protecting everything from internet-connected washing machines to human social interests at large. Cyber security must therefore encompass any person or device that has on- or offline communication capabilities [371, 378, 245].

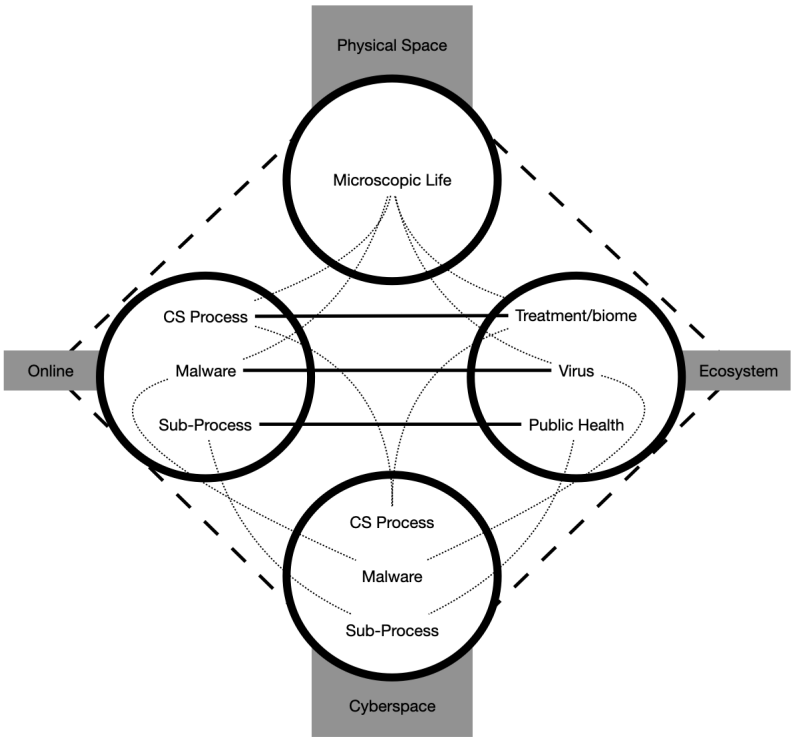


Figure 4.2: Our blended concepts shown at the Micro-Level. As before, the solid lines represent connections between input sources, and the dotted lines represent connections in spaces. At the top we find our generic space, labelled "Physical space'. On the left-hand side, we have the "online', which is our first input space, on the right, "epidemiology' is represented form our secondary input space. The two spaces come together in our blended space of "Cyberspace".

3. *Computer viruses*, which are representative examples of harmful micro-level actors in our system. We define these as a form of autonomous or semi-autonomous malicious software.

It is difficult to determine the actual prevalence of our various actor types; thus, we have attempted instead to graphically represent their qualitative prevalence in cyberspace — that is, the relative influence that we believe each actor wields in this domain (Figure 4.3). Our micro-level actors are grouped under 'machine organisms'. Figure 4.3 illustrates the assumptions we make about cyberspace and the hierarchical structure of its constituent entities, in terms of the agency they may hold. In this case, we ascribe agency to power based on our hierarchical structure, and complexity broadly based on what we saw in Section 2.4. The

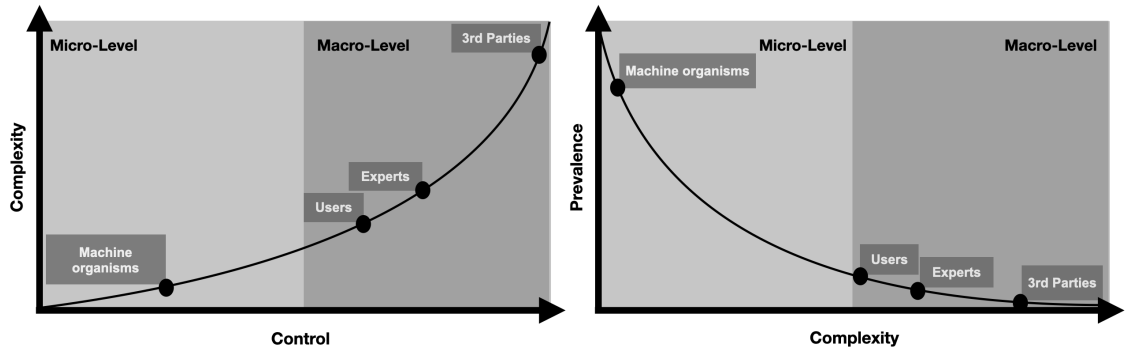


Figure 4.3: Two illustrative graphs of cyberspace. On the left, we have complexity/control as the defined axes. On the right, we have prevalence/complexity as the defined axes.

left graph within Figure 4.3 highlights the first assumption; that as the level of complexity exhibited by the actor increases, their level of control within cyberspace also increases proportionally. Similarly, the graph on the right-hand side of Figure 4.3 highlights how the prevalence of these actors in cyberspace drops proportionally to their complexity. This is our second assumption.

4.5 Providing evidence for our model through an experiment

Although the model provides us with a set of fundamental concepts from which to derive insight from cyberspace, its validity requires testing. However, providing direct evidence of a qualitative model such as the one described above can be difficult, in particular with regards to such concepts as control within complex environments such as cyberspace. To address this, we return to our discrete or innate risk hypothesis from Section 4.1, and ask ourselves how, with our conceptual environment in which these risks exist in place, we may begin to prove it.

As we assume experts look primarily towards the minimisation of discrete risks, we can make the direct comparison with epidemiologists' attempts aiming to quantify the effectiveness of different public health intervention strategies. We chose an agent-based simulation of the environment, which we believe to be the most prudent way to assess the hypothesis in our conceptual environment. The reasons for this are many,

First, we based this assessment on research such as Wang et al. [380], who described the two main ways in which virus ecologies are tested. These methods, equation-based and agent-based, have two alternative approaches. In the equation-based method, the concept was proven in a theoretical sense. In our case, that would need a top-down approach in which many of the variables described in the model would be quantitatively known. For example, the rate of virus reproduction[7], or the extent to which users engage in risky behaviour, are in our case not known, and cannot easily be inferred from outside data (for example, work by Fleming et al. [121] highlighted the point of behaviour not being easily incorporated into a top-down deterministic or stochastic model of malware propagation). Furthermore we are unable to adjust coefficients to optimise its workings, which rules this model out.

In the second, the agent-based model, we are able to employ a 'bottom-up' structural style, as we are able to start with metaphors that represent our actors, that we then build up into data structures that can interact with the wider environment [110, 83, 165]. Our model allows us to systematically model a hypothetical user's subjective orientation to cyberspace, and then to non-subjectively test the rationality of this model in the face of real threats. Thus, our methodology can serve as a useful supplement to qualitative research, 'transposing' users' mental models into shared metaphorical environments.

As we have specified our parameters (namely, the macro- and micro-level actors) and configured our simulated environment, which will serve as an interpretative lens through which to evaluate our experimental outcomes, we will model a typical user's navigational routes through cyberspace — the generic tasks and interactions they undertake — to test the consequences of high-risk behaviour within it through non-conformance to informally learnt security advice.

We make the following assumptions about the potential threats from our micro-level actors. If risk is discrete, we expect that viruses will manifest as opportunistic entities that thrive on risky behaviour; if risk is environmental, we expect that

[7] In epidemiology, the basic rate of reproduction is denoted as R0 and interpreted as the number of cases spawning from a directly confirmed single case. The formula is $vR0 = \tau\beta$, where β is the number of infection-producing contacts per unit time, and τ is the mean infectious period [165].

viruses will operate as predators that, while not necessarily looking for a victim, will grievously harm the victim if an attack is initiated. Thus, in our experiment, if the modelled high-risk behaviour yields an infection rate that is higher than a pre-defined average, we may conclude that risk in cyberspace is a discrete property of interactions that users can reasonably avoid with due diligence. However, if the modelled high-risk behaviour yields an infection rate that is comparable to, or lower than, our pre-defined average, we may conclude that risk is an innate quality of cyberspace that users cannot necessarily predict or avoid of their own accord. We chose the 7% infection rate listed in the Microsoft Security Intelligence Report [5] as our pre-defined average, as it embodies the security outcomes of a large subset of users running the basic Windows Defender package at optimal security settings.

Because the user macro-level actor is the only actor we can control, our exercise takes the form of 100 virtual machines scripted to mimic our user's behaviour in cyberspace.The other macro- and micro-level actors need not be modelled as they already exist in the online environment shown in this chapter.

4.5.1 Modelling the user actor

To navigate cyberspace, our user actors would need a degree of contextual awareness. Thus, we designed our user actors around a set of basic metrics corresponding to user behaviour. In January 2019, the average time spent online by a typical user reached 6.5 hours per day on average, or around 98.85 days per year [195]. For our purposes, it was sufficient to model a third of a user's given year, meaning that our actors spent 32.95 whole days in cyberspace. We used browser information from [11] and [336] to determine the interactions our user actors would undertake. Furthermore, we investigated how users typically spend time in cyberspace and modelled specific behaviour based on average time spent on a website (5 minutes 52 seconds), eye movement tracking [287, 94, 275], and reading speed [213, 226]. We also took care to overcome obstacles that prevent automated Web visitors[8] and performed deep web analysis [299]. These metrics enabled us to design a user actor

[8]Specifically, we implemented the Death By Captcha automatic captcha solving service found at `https://www.deathbycaptcha.com/user/login`.

Table 4.2: Areas of vulnerability we have deliberately opened, based on highly common security advice that appears to have the most exhaustive dissemination across sources. All are client-side security, which means the user would have control over them.

Label	Chosen parameter
SA1	*Keep your operating system up to date.* Regularly updating your operating system is crucial for protecting your device, as updates often include security patches that address vulnerabilities and loopholes, making it harder for malicious actors to exploit your system and gain unauthorized access (for example, from `https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date`) [112, 224, 60].
SA2	*Keep your web browser up to date.* This refers to maintaining security defenses against threats that are specific to browsing activity, and to ensure compatibility with the latest web technologies for a safer and smoother browsing experience (for example where a Building Society (Credit Union) is providing customer advice for all browsers: `https://www.familybuildingsociety.co.uk/about-us/keep-your-browser-up-to-date`) [253].
SA3	*Install a form of virus protection.* An additional line of defense, aiding in detecting, preventing, and removing malicious software, reducing the risk of infections, data breaches, and unauthorized access by malicious actors (Although this appears to have lost some popularity over time, an example of 2022 still highlights its importance: `https://www.security.org/antivirus/do-you-need-antivirus/`).
SA4	Deploy content blocker plug-ins [297, 298, 140]. This security advice has to do with accessing potentially compromised web servers. In order to avoid common attacks such as drive-by-downloads, users are advised to install content blockers, including active content blocker plugins like NoScript [297, 298, 140]. More than 90% of websites depend to differing extents on third-party content [212], making this a common piece of security advice.
SA5	*Monitor your ports.* Refers to managing potential security vulnerabilities in your network. Regular port monitoring allows you to detect and respond to unauthorized access attempts, helping to prevent data breaches and maintain the integrity of your system's communication channels (Examples can be found here: `https://www.networkworld.com/article/3191513/securing-risky-network-ports.html` and here: `https://securitytrails.com/blog/top-scanned-ports`).

with the right level of breadth and depth to convincingly replicate real user actions as it cycles through the globally most popular web-pages executing basic functions.

We needed to enable our user actors to engage in high-risk behaviour to test the validity of our hypothesis. As such, we selected five common security advice

Table 4.3: The hardware/software combination our user utilises for cyberspace access.

System	Chosen parameter
Hardware architecture	X86
Operating system	Microsoft Windows 7
Internet browser	Google Chrome v18

elements that could reasonably have been learnt by our simulated user in their online environment (see Table 4.2). To do so, we conducted a brief and non-exhaustive mapping study to ascertain popularity based upon keyword searches, followed by the ability to test using our experiment methodology. Therefore, while not exhaustive, the list in Table 4.2 represents security advice as accurately as possible, within the constraints of the setup of the experiment. We chose five to test as this number was found to be the maximum amount to efficiently monitor given our sample size, data collection and classification methods.

We then selected a hardware set-up that specifically undermined these security elements. Specifically, we chose an OS and hardware combination that was at least five years past its original release date because this is the average point at which software manufacturers cease supporting their products. This figure was derived from an assessment of every closed-source OS since 1995 that has had more than 3% market share at some point since its introduction, as defined by the statistics in W3Counter [372]. Based on the average screen resolution from the same period — 1366 x 786 — we assumed that the average user uses a desktop computer; thus, we chose hardware with the specifications listed in Table 4.3[9][10][11]. Furthermore, we programmed the user actors to take additional actions that would increase their risk potential, such as clicking on all pop-up boxes. Overall, it took our user actors 3 days

[9] https://gs.statcounter.com/chart.php?bar=1&device=Mobile%20%26%20Desktop&device_hidden=mobile%2Bdesktop&multi-device=true&statType_hidden=comparison&region_hidden=ww&granularity=monthly&statType=Platform%20Comparison&region=Worldwide&fromInt=201501&toInt=201501&fromMonthYear=2015-01&toMonthYear=2015-01&csv=1

[10] http://www.w3counter.com/globalstats.php?year=2015&month=1

[11] https://gs.statcounter.com/#desktop-browser-ww-monthly-201501-201501-bar

and 23 hours to complete a full navigation cycle in cyberspace. We closely monitored each cycle for any potentially malicious interaction or other abnormality by means of a remote monitoring and management tool similar to that used by Matias et al [248].

The detection method builds upon work by Matias et al [248] who looked at overall Operating System reliability at kernel level. We then expand on it by using a Remote Monitoring and Management (RMM) tool in conjunction with the above-mentioned methods, to collect more metrics that are not necessarily directly associated with an event, but will help to inform the current state of the machine. The RMM tool also assisted with any ad-hoc error reporting that may not necessarily have been a part of the experiment. We utilised reference data set from our control group to help prevent false-positives. The events the agent engaged in, alongside the error handling process can be seen in Figure 4.8. The boxes represent processes, with the diamonds representing binary choices.

Every event logged the agent User ID, event type, creation/execution/closure timestamps, and recorded the user-names and passwords used in some of the scripted events. These user names and passwords were created manually beforehand as to ensure the unique nature of each event and agent usage pattern.

4.6 Interpreting our results

The user actors ran for their scheduled duration, with a small pause to push an update that addressed how these actors dealt with data protection regulation prompts. By the end, our user actors experienced an overall incidence rate of 7% (see Figure 4.4). Of this 7%, 28% (or two user actors) experienced a specific infection that required no further user interaction, which can be seen in Figure 4.5. Both infections were caused by a form of crypto-jacking tool, which we identified through our logs based on out-of-the-ordinary processor loads and specific network traffic, the evidence of which points towards an outside command-and-control server [356]. Referring to Table 4.2, it seems that both of these infections could have been avoided by following common security advice (such as SA1, SA2, and SA3 in Table

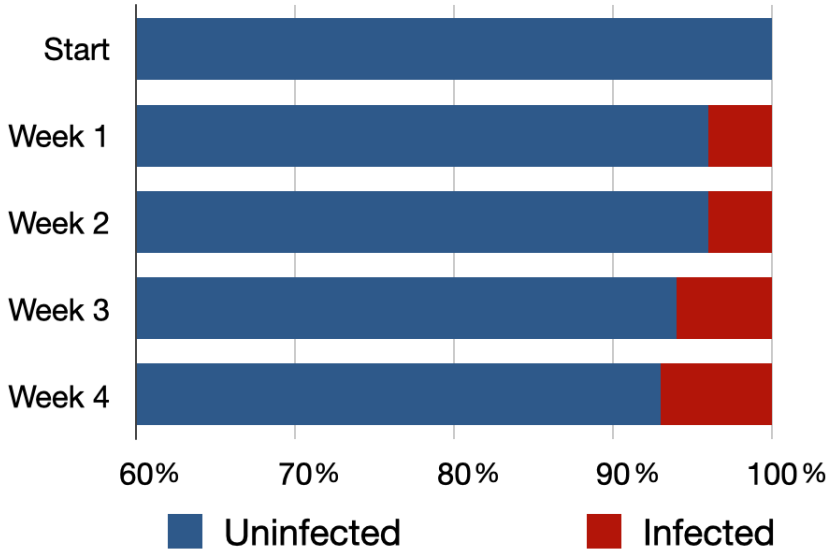


Figure 4.4: The overall infection rate broken down by week. Out of 100 user actors, 7 were infected.

4.2), although — barring increased use of resources and network traffic — neither infection caused direct, measurable harm to the system itself.

All remaining viruses were not executed after infecting our actors, as they likely required user interaction, had missing dependencies, or were otherwise corrupted in some fashion. Overall, four out of five agents had downloaded an illicit Adobe Flash Player® installer executable, and one other had downloaded a file disguised as a Microsoft Word® file. Our agents were not scripted to open these files, and no further identification attempt was made.

We detected temporary out-of-the-ordinary network traffic from more than 25% of user actors throughout the duration of the experiment. We concluded that this may have been a result of drive-by mining, wherein a script is embedded into a page in order to utilise a visitor's CPU power to mine cryptocurrency [206]. As this left no other trace of infection, there was no need to count it as an infection. It is, however, included here because it speaks to the power relationships between different macro-level actors and the compromise of user agency in cyberspace (expounded in Section 4.7.2).

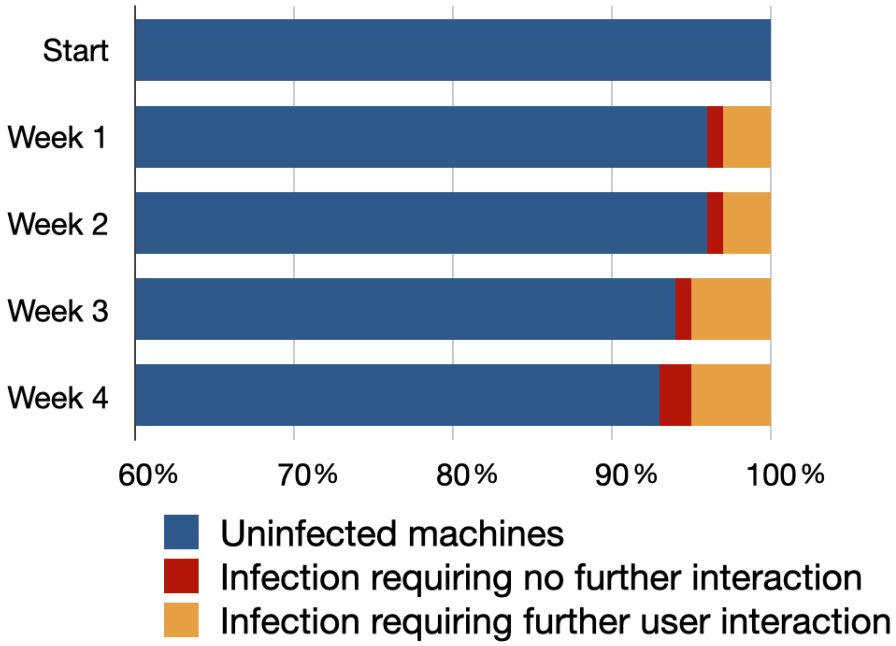


Figure 4.5: The overall infection rate broken down by type.

We would suggest that these results highlight that risk is more an innate property of cyberspace than it is a discrete property of potential interactions and transactions within it. This is because our infection rate of 7% closely matched standard exposure rates reported in the industry, despite the fact that we programmed our actors to deliberately engage in high-risk behaviours. Notably, though, our experiment reported *actual* infection rates (including infections that require further user interaction to take hold) versus *encountered* rates, as in the case of our benchmarked average [5]. Measuring actual infection is more analogous to how STD studies are conducted within epidemiology, and it could provide a more suitable template for future reference studies.

Figure 4.6 highlights how much of cyberspace user actors needed to navigate whilst engaging in potentially high-risk behaviour before infection took hold. Excluding non-infected user actors, the mean number of websites navigated before infection was 2,497, and the median was 3,819. This figure covers entire websites; it does not include sub-domains within that website (e.g. `login.facebook.com`). Given the accelerated schedule of the user actors compared to normal human

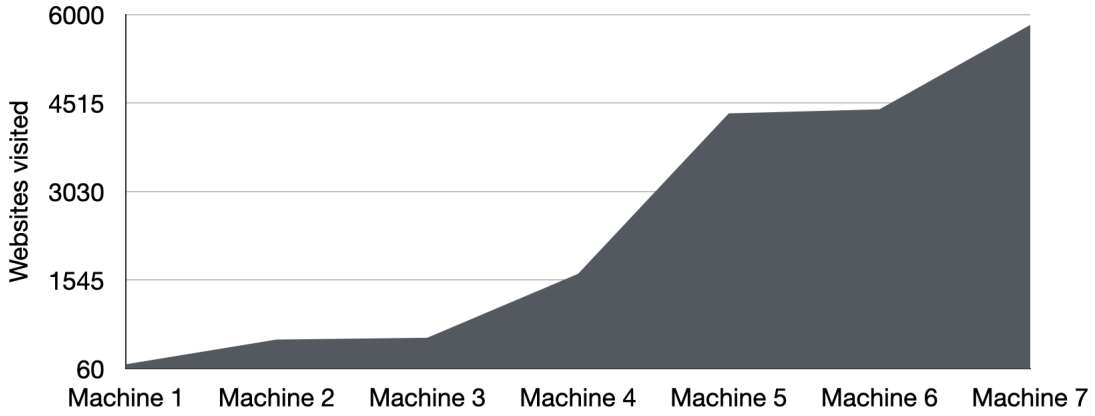


Figure 4.6: Each compromised user actor was at a different stage in their journey when infection took hold.

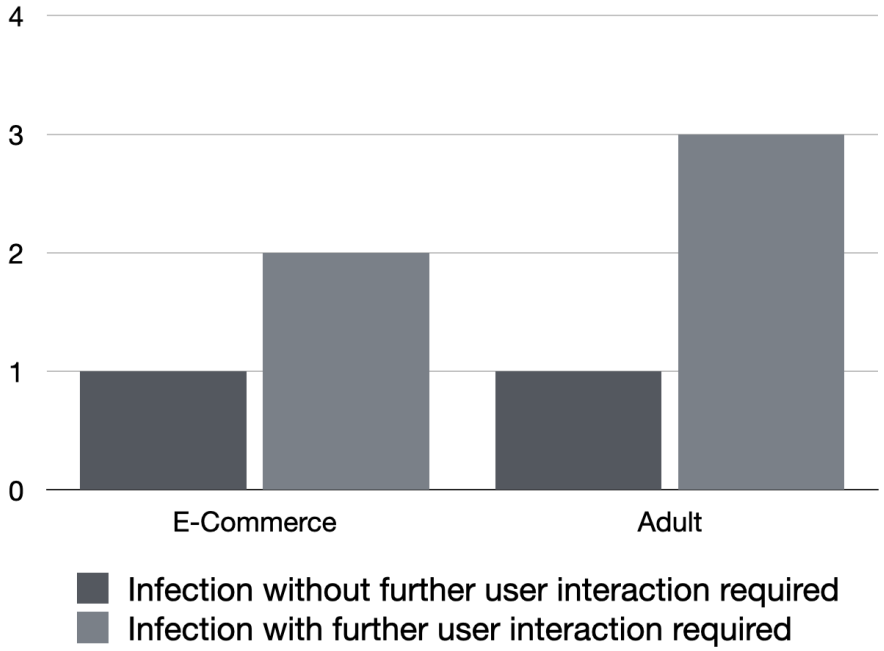


Figure 4.7: Each compromised user actor was visiting either an e-commerce site or an adult genre site upon infection (genres taken from Alexa Top-1000 websites rankings).

behaviour, we did not perform a time analysis to discern how *long* the user actors spent online before infection, as this would likely lead to over-reporting of individual website visits [17]. This may suggest that our user actors encountered a wider breadth and depth of cyberspace than a real user may have done before contracting an infection.

Figure 4.7 show us that all of the infections were derived from e-commerce and adult sites. In the case of adult category sites, our actors were most at risk when engaging in a pop-up click activity. This is unsurprising, as pop-ups — and adult sites overall — are widely known to present certain risks. Referring to our epidemiological metaphor, this may correspond with expected STI transmission rates at a brothel or other high-risk site (see Section 4.3.1). In the case of e-commerce category web-pages, infection most often resulted from 'malvertising', wherein virus delivery mechanisms operate within an environment that may be trusted by the user [390].

These findings collectively indicate that system-compromising computer viruses are somewhat rare, and they are concentrated in predictable cyberspace environments. Consequently, users who navigate these environments likely know about their associated risks, but choose to engage in risky behaviour anyway. In addition to the reasons specified in Section 2.5.7, and based on the nature of the risky sites in this chapter, such risk-taking may occur because users enjoy/anticipate more benefit than harm from certain risky activities [45]. Overall, we were able to implement high-risk behaviour sufficiently well to confirm the validity of our hypothesis, thus implicitly modelling the findings of Seib et al. [329] within epidemiology.

4.7 Discussion

Our metaphorical environment and experiment has highlighted broader themes regarding the nature of risk within cyberspace. In particular, our model highlighted the existential dimension of online risk, given the biological basis for the relationship between security and privacy, the increasing tendency for users to identify themselves with their online information, and the imperative of self-preservation in any environment. Because risk is an attribute of cyberspace more so than an attribute of user interactions within cyberspace, security experts need to take both environment and agency into account when determining how to help other actors to mitigate risk. We present three points that follow from our findings. We start from the existential and move towards the practical, including methodological considerations at the end.

4.7.1 Is cyberspace homogeneous?

We have an understanding that the laws of physics govern our physical world. However, within it, there are numerous systems that conform to different standards, leading to naturally occurring variations such as localised ecosystems and evolutionary divergence (see, for example, the work of Cleland [82]). If we look at the results of our experiment, we can see that our infection rate roughly corresponds to exposure rates in other studies.

However, virus occurrence rates vary depending on country of origin. The Microsoft Security intelligence report [5] affirms that many users in developed nations do not encounter viruses as often as those in developing nations. In particular, the rates of ransomware infection differ dramatically, with one example citing a ransomware occurrence rate of 0.07% for U.K. users and of 0.77% for Bangladeshi users. Based on our design, our infection rates for viruses (and, by extension, ransomware) should have mirrored a more global average; however, there were zero confirmed infections of the ransomware type by the end of our experiment. This could be because some of our infections were unrealised examples of ransomware, although it could also be a consequence of a design flaw in our experimental model (it was not designed to carry out instructions pertaining to executing ransomware code such as compromised files, for which no human-equivalent data of how many of these files are opened could be obtained within the confines of this work). It remains to be explained why our rate was lower than even the U.K. rate of 0.07%, although this may serve as a point of evidence to support the work of Moschuck et al [268], whose work with malware pointed towards an increasingly safer cyberspace. As viruses become more targeted, developing and maintaining a universal model for malware detection may become a more significant challenge.

4.7.2 Who has the agency to mitigate risk in cyberspace?

On the agency of users

When formulating our model, we argued that users have limited agency over their interactions within cyberspace (see Section 4.3.1). The results support this notion

and even suggest that agency may be more limited than suspected in previous research. In our experiment, all of the macro- and micro-level actors other than the user were unknown to us; we had no insight about the systems our user actors accessed, although — unlike real users — we kept detailed system and network logs for assessment purposes. This approximates an individual wandering around in the physical environment without knowledge of the natural sciences, the properties of matter and energy, or the laws that govern them.

This naïve mode of navigation on the individual level embodies what Parisier calls a 'filter bubble' [289]. In our model, the filter bubble relates to how sub-processes affect users' navigation and interactions within cyberspace. Because cyberspace is opaque, many users may not be aware of this subtle guidance of their navigation and interactions in cyberspace, which only arises in certain contexts. One example of this which has received attention from media and researchers involves recent changes to the *Google Maps* navigational algorithm: it no longer automatically provides the fastest route, but, rather, the most carbon neutral or congestion-free route [12]. Whether this is innocuous or insidious depends on the viewpoint of the user (if they are even aware of this). Furthermore, users will have few means to infer the safety of their data — more often than not, they infer safety based on their experience with infections, as seen in Nam's work [269], where experience in security breaches increased users' awareness (but not direct knowledge) of perceived threats, or in accounts of cyber attacks from media sources. We may consider our unrealized infections as an example where experience can be built through an execution of agency, as in these cases, the user would be required to interact with the malware in order to activate it. This could be construed as a form of agency through the offering of an opaque choice.

This begs the question: is cyberspace enfranchising or disenfranchising for those who use it? Given cyberspace's influence on contemporary society (affecting users and non-users alike), the power relationships between actors within this domain are non-trivial. With regard to our user actor, much research highlights

[12] `https://support.google.com/maps/answer/11470237?hl=en`

the enfranchising and equalising features of cyberspace, such as its perceived ability to aid social justice [87] or provide education to those who might otherwise not receive the chance[40], though other sources foreground its alienating and controlling attributes [321]. For example, Goldberg, as early as 1996 highlighted the potential of the addictive nature of cyberspace. Another later example comes from Rushkoff, who correlated declining narrative use in mass media with the emergence of post-narrative meta-shows, product placement, and online games, highlighting viewers' need to comprehend media and cyberspace as self-referential universes, where significnant knowledge is required in order to do so successfully. Rushkoff additionally address the pervasive connectivity of technology, which he argues leads users to the constant pressure for connection eclipses the previous desire for a longer temporal perspective, replaced by a focus on the present, where cyberspace assumes a position of great import to the user [321].

On the agency of third-parties

It is our third-party actors who issue cyberspace's sub-processes and shape the aforementioned filter bubbles. Third parties wield disproportionate power in cyberspace, as they control most of the back-end infrastructure that users are not aware of [101, 296] and act as brokers for the data generated by users, ensuring a downward economic trajectory for informational value [217, 20] and continuous development. Arguably then, third parties should take more responsibility for the parts of cyberspace over which they have sovereignty, placing less emphasis on user-side security efforts. If third parties shouldered additional responsibility for the security of those users, through the protection of their devises and systems, the risk landscape of cyberspace could be improved more reliably, although this would further limit users' agency.

On the agency of experts

On a biological level, this power relationship even influences users' reasons for ignoring or actualising security advice. Thus, the continuous evolution of the interaction between users and third parties influences the creation and dissemination

of novel security advice. How then can researchers mobilise their position within these power relationships to exploit this evolutionary loop in ways that enhance the efficacy of security advice? Furthermore, how can they deploy security features and disseminate security advice that adequately account for the complexities of cyberspace's rapidly developing ecosystem, the properties of which are often opaque?

Within the biological world, many solutions designed to alleviate existing concerns have simply created new ones. As such, the medical and biological sciences have supplemented direct interventions with education and legislation to achieve greater regularity and security in these fields[13]. In cyberspace, though experts and third parties have achieved a degree of self-regulation sufficient to provide a minimum product (such as ISO standards for cyber security [159], and development of ethics within academic circles [240]), there is little oversight or coordination between these actors and other regulators [338, 240]. This can have unfortunate effects for research applications. For example, one significant study by Stock et al. [349], which utilised decades-worth of data to plot the course of server-side security, found that many technologies developed to make users safer were not implemented until years after their original development and release, at which point they may have no longer been useful.

As cyberspace continues to develop, the first challenge for cyber security researchers, as experts in the field and progenitors of cyber security advice, may be to provide context to cyberspace — that is, to treat it as a techno-spatial environment with systems and dynamics comparable to those in biological environments, epidemiology, and other organic fields. This content may fit more closely with users' existing experiences of cyberspace or otherwise enable them to 'inhabit' online spaces more securely. Researchers might also take into account that cyberspace both provides and removes power and liberty, and the ratio between these movements depends largely on where actors find themselves on the complexity/power curve. Taking an example from our healthcare metaphor, where there is an ethical requirement

[13]For example, legislation has been used in the area of air pollution, where long term positive effects can now be seen in California, one of the first to pass these laws [92]. Education has likewise had single-issue based positive impacts, for example in the area of student smoking [15].

to ensure users' continual safety and autonomy within medical institutions, this may involve protecting users from both viruses and undue third-party manipulation. We believe that the metaphorical model presented here may provide a suitable starting point for critique and development.

4.7.3 The impacts of self-efficacy when navigating cyberspace

If we develop an improved idea as to the agency actors have within cyberspace, we can turn our attention towards the link between their agency and self-efficacy. Aside from what was discussed in Section 2.5.5, this symbolic link is highlighted by work such as that of Bandura [25], who investigated whether the overall agency an individual had over their environment had additional effects on their perceived self-efficacy in that environment. In that case, the results showed a clear correlation between agency and self-efficacy. However, there appears to remain a dearth of empirical evidence linking self-efficacy with agency in online environments.

A significant area of note was that in order to arrive at our chosen security advice to test in Section 4.5.1 (the chosen advice can be seen in Table 4.2), we needed to conduct our search in a manner more rigorous than what a user may enact when performing a similar function, yet, due to restrictions in time and scope within the work it was non-exhaustive. A significant element to consider therefore would be to return to idea that self-efficacy is derived from the ability to enact decisions based on prior cyber security knowledge. In this environment, where agency is limited, how does an informal learner gain access to this advice, and how is this advice structured? This is explored in Chapter 5.

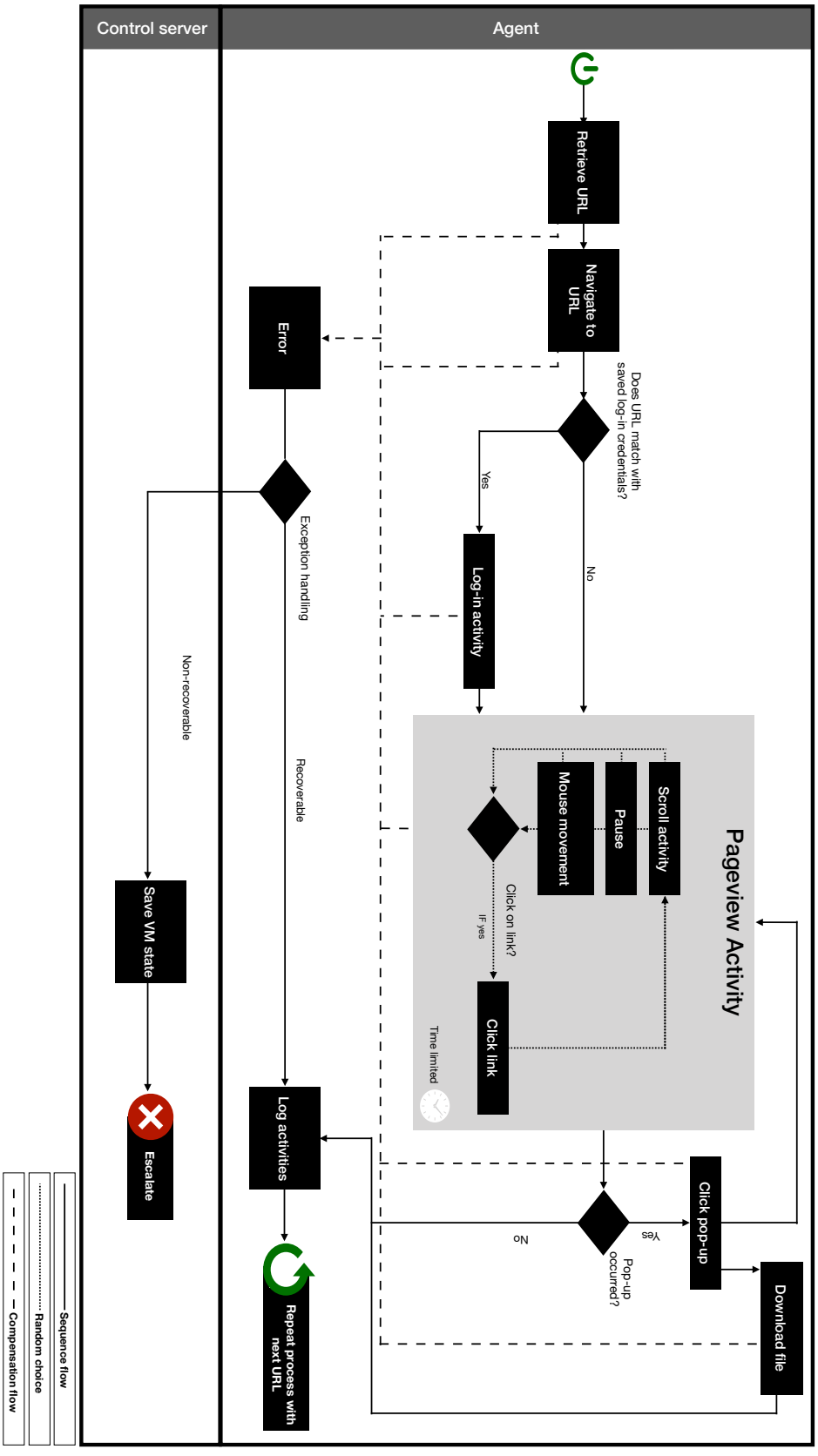


Figure 4.8: A process diagram highlighting the actions each agent took while in cyberspace.

5

News-disseminated cyberspace advice

In Section 1.1, our research problem espoused the idea that cyber security advice, whether followed or not, is seen as a vital security process, provided it can reach 'psychological acceptability' and avoid the user encountering difficulties in its use, such as the processes described within section 2.5.2.

The preceding chapter presented a conceptual model and insights about the environmental level of cyberspace which showed a tendency to highlight risks taken within this environment as innate rather than discrete. This provided a description of the environment but no insights into the mechanisms and processes driving factual, textual content of cyber security advice (defined in Section 2.5), discrete or otherwise. Furthermore one discussion point highlighted that we have no information on prior self-efficacy may affect navigation through cyberspace and risk appetite, as defined in Section 2.5.7. We are also aware of common cyber security advice dissemination practices (Section 2.6.1), a significant proportion of which can be found in cyberspace.

In this chapter we move from the environmental level into the epistemological, and investigate the nature of informally learnt cyber security advice through a corpus of cyber security advice generated from mainstream news articles. We know that users in cyberspace face a wide range of innate cyber security threats — including viruses [8], bot-nets [37], port-scanners [369], spyware [346, 161], malware [346],

stalkerware [198], and rootkits [346, 377]. Furthermore, due to the opaqueness of the environment and the lack of agency it may be difficult for them to develop sufficient 'knowledge' of the 'rules' even when advice is presented clearly and thoroughly. We attempt to provide insight into the discrete advice available to users, and look not to specifically catalogue it, but rather keep the self-efficacy potential of this advice in mind, as per our second research question of Section 1.1; *Considering that the dissemination of security advice about cyberspace takes place through a multitude of vectors, is it possible to measure the efficacy potential of such advice through one such dissemination vector?* In order to answer our question, a two-part response was developed:

1. To ascertain what kind of actionable advice is being disseminated through online media as the chosen dissemination vector. An explicit definition of cyber security advice used in aid of this can be found in Section 2.5.

2. To explore ways of determining the efficacy potential of news-mediated security advice through quantitative means.

As there have been relatively few quantitative studies analysing the security advice literature available to what we might term 'everyday' users, this chapter endeavors to bridge earlier contributions by providing additional context about the current security advice environment[1].

The remainder of this chapter is organised as follows. In Section 5.2 we present our results and perform an initial analysis, before, in Section 5.3, discussing the results in relation to our research objectives. Section 5.4 links the work into our follow-up work in Chapter 6 and offers conclusions.

[1]Notable examples of such studies include that of Redmiles and colleagues [305], which explores how individual users actualise and perceive their own cyber security capabilities (which often derive from informally learnt advice), and that of Renaud and Dupuis [310], which identifies large sub-concepts and classifications in the security advice field.

5.1 The cyber security advice corpus

The corpus spans a 24-month period and was assembled from a data-set containing 15,422 (English language) news and online magazine articles from North American (US and Canada) and UK-based sources, as well as some historical data stretching back to 2000. We described the process used to create the data-set, and our data cleansing process that develops the data-set into the corpus in Section 3.2. In the following we utilise a term called 'CIS-Vectors', which relates to our chosen ontological framework in aid of classifications. Further information can be found in Section 3.2.2.

We utilised an ontology from the Centre of Internet Security, which can be seen in Figure 3.3 (for a primer on the CIS ontology and its vectors, see Section 3.2.2). Within the corpus, we observed that only 6,134 of the 15,422 articles (representing 36.3% of the total corpus) contained references to any of our CIS-vectors. We performed a second pass on the corpus, introducing additional syntactic variants of the terminology utilised within the CIS-vectors. For example, we separated 'malware defenses' into 'malware AND defences', 'malware defence', and 'malware defense' to correct for localisation issues.

The results of the second pass result in an occurrence rate of 7,988 articles, or 51.7% of the corpus. Each of these articles contained references to one or more CIS-vectors. For the remaining 48.3% of the corpus, we performed a Latent Dirichlet Allocation (LDA) analysis of these articles in order to generate further details, the results of which are outlined in Section 5.2.2. LDA is a generative probabilistic topic model that allows for the discovery of otherwise abstract topics within text files [41]. The underlying idea behind LDA is that documents contain multiple topics within them, where the topic is a polynomial distribution over an otherwise fixed vocabulary. In essence, it considers documents to be a blend of topics, with the topics then blends of words [41, 67]. The goal of using this method is to discover topic-per-word and topic-per-document data automatically.

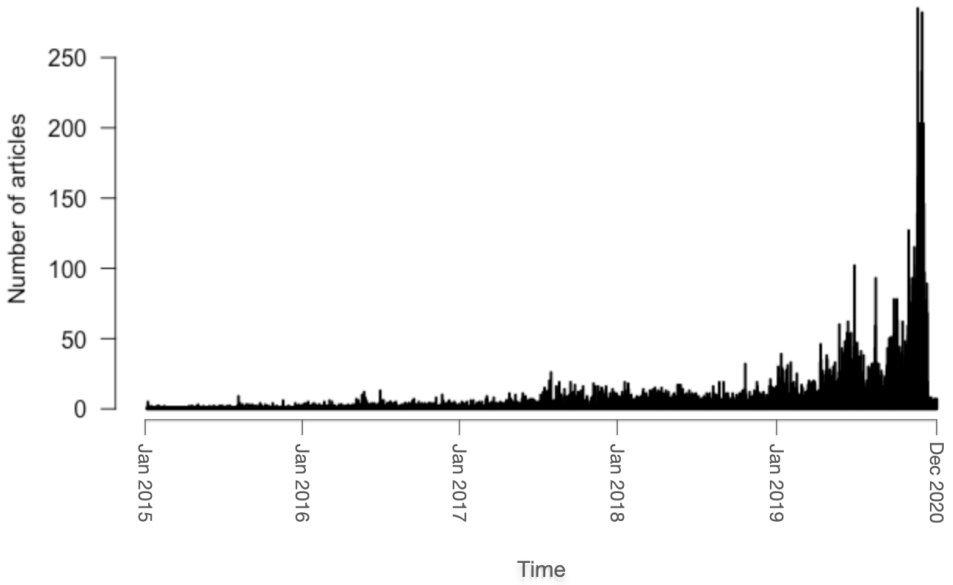


Figure 5.1: Articles published per day between January 2015 and December 2020.

5.2 Results

In this section we give consideration to our results. First, we corroborated the findings of Alagheband et al. [9], which indicated that coverage of security topics in the New York Times has steadily increased over the last decade. Figure 5.1 highlights this increase over time: the "vast terra incognita of print" [354]. The data also exposed the sheer diversity of publishers, ranging from traditional outlets such as the BBC news and CNN through to specialty security blogs, and government advice pages. Even so, we must acknowledge that this list is inevitably incomplete, as our search methodology, while extensive, was non-exhaustive, and it was limited to English-language media.

Next, we identify the prevalence and features of 'ideal' news articles in our corpus and use this information to develop our response. An ideal news article must contain a summary of the information that an individual user requires (in this case, regarding security advice), eliminating irrelevant and redundant information wherever possible [139]. To determine the prevalence of such articles in our corpus, we first utilised our CIS-vectors to ascertain how many of the articles contain content-specific vocabulary that users may expect to find within these articles, and

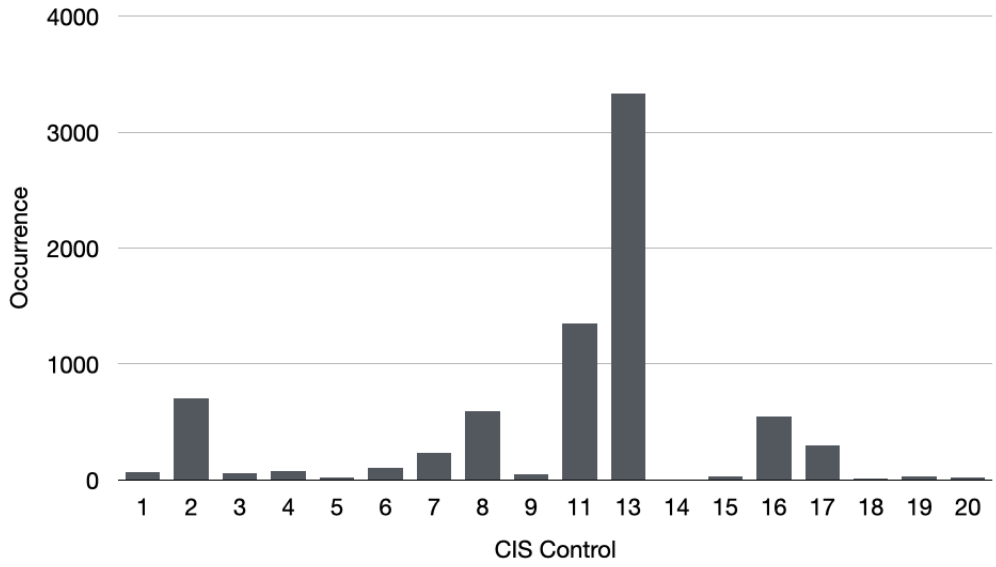


Figure 5.2: The occurrence rate of CIS-vectors. Null values are excluded.

we performed additional analysis on those articles that contained no such terms. We then derived statistics pertaining to sentence length and vocabulary size, which we then compared to third-party corpora (where available). Finally, we utilised sentiment analysis as an efficacy potential measurement tool, building on work by Kalra and Prasad [187], who used it for stock market assessments. This was done to decipher any trends that could inform self-efficacy potential.

5.2.1 CIS-vector occurrences

Figure 5.2 highlights the occurrences of our CIS-vectors in the corpus. The most-used CIS-vectors were CIS-13 (Data protection), CIS-11 (Limitation and control of network ports, protocols, and services), and CIS-2 (Inventory and control of software assets). CIS-13 highlights the growing trend towards data protection awareness and its relevance for individual users; it occurred 0.4 times per article, on average.

Delving deeper into the reasons for this expanding data protection coverage, we find that, between 2018 and 2019, the most significant topics were related to data breaches, data protection guidelines for individuals and organisations (such as the EU's General Data Protection Regulation (GDPR)[2]), and data privacy-

[2] `https://gdpr-info.eu/`

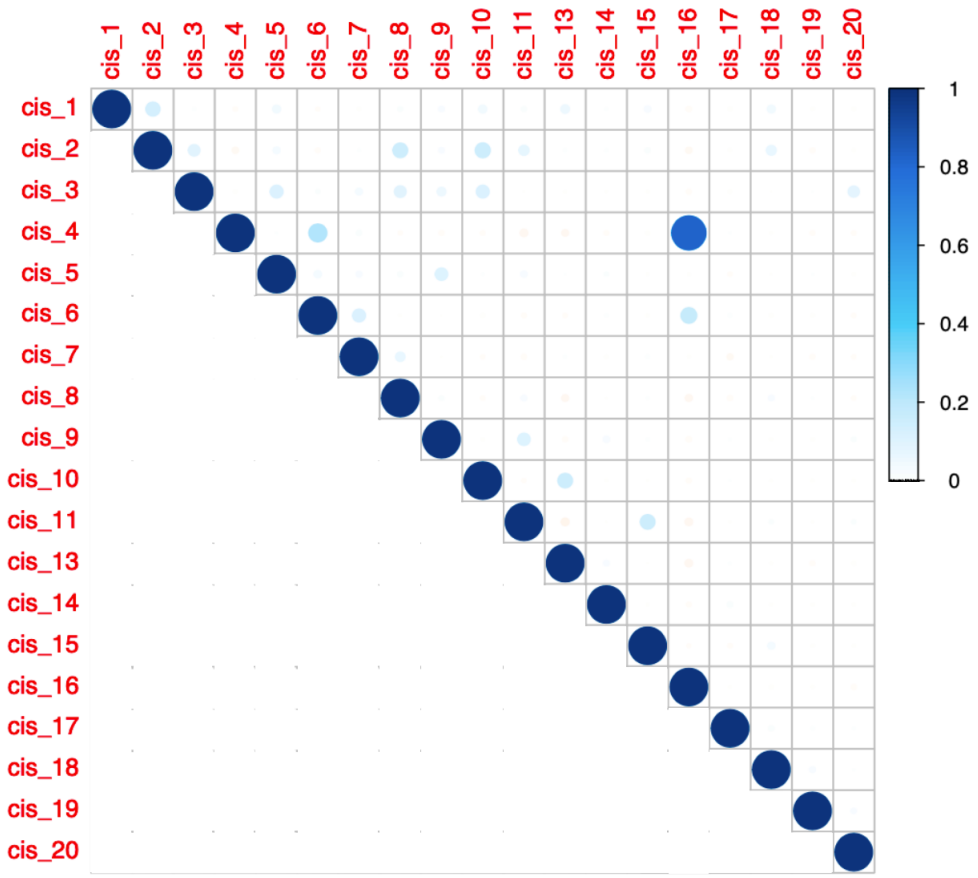


Figure 5.3: A correlation plot, highlighting in particular the strong correlation between CIS-4 and CIS-16. The larger and darker the circle, the stronger the correlation. Each CIS-vector is represented, with many have weak correlations. For a reference to what each CIS-Vector is, please refer to figure 3.3.

related security advice for social media users. In 2020 there was a shift towards protecting health-related data in medical contexts, with advice and threat messaging geared towards disease contact and exposure tracing applications, such as those mentioned by Yasaka et al. [391].

CIS-11 indicates network security-related information and advice, and its occurrence rate increased significantly between 2019 and the end of 2020. At least one publication ([233]) notes a similar increase in interest. Again, we found that most of this network security advice was related to privacy, and it appeared in texts ranging from technical articles to installation guides for the Tor Project[3]. In many cases, these articles contained more difficult vocabulary and technical

[3] `https://www.torproject.org`

Table 5.1: The five most common topics in the non-CIS articles.

Topic 3:'Systems security'	**Topic 6:**'Cyber health'	**Topic 9:**'Business threats'	**Topic 11:**'Cyberspace politics'	**Topic 14:**'Cybercrime'
security	safety	cyber	trump	police
internet	health	security	president	crime
system	recovery	attacks	election	cases
users	covid-19	business	russia	issue
data	protection	threats	u.s.	cyber

terminology than the average publication.

CIS-2 pertains to software assets and their associated CIS-vectors, and it proved to be one of the most diffuse topic. In our corpus, we found articles linked to Internet of Things home security, smart grid and connected vehicle software, and security issues that arise in connection with these devices and services.

Correlations between the CIS-vectors are depicted in Figure 5.3. The correlations were weak across the corpus, with one notable exception: the correlation between CIS-16 (Account monitoring and control) and CIS-4 (Controlled use of administrative privileges). Though CIS-16 appeared more frequently overall, tokens associated with both vectors appeared consistently between articles.

5.2.2 Articles containing no CIS-vectors

Table 5.1 lists the most common topics that occurred in those articles that featured no CIS-vectors from our classification (representing 48.2% of the corpus). The topics were derived through LDA topic modelling, as described in Section 5.1.

We can see that, despite the absence of CIS-vectors, security is still a focal point in these articles. In these cases, though, the focus is on national (cyber) security (Topic 11), cyber crime (Topic 14), business threats (Topic 9), and health and safety issues related to cyber crime and security (Topic 6). Topic 3 embodies similar concepts as CIS-vectors CIS-13 (Data protection), CIS-11 (Limitation and control of network ports, protocols, and services), and CIS-2 (Inventory and control of software assets).

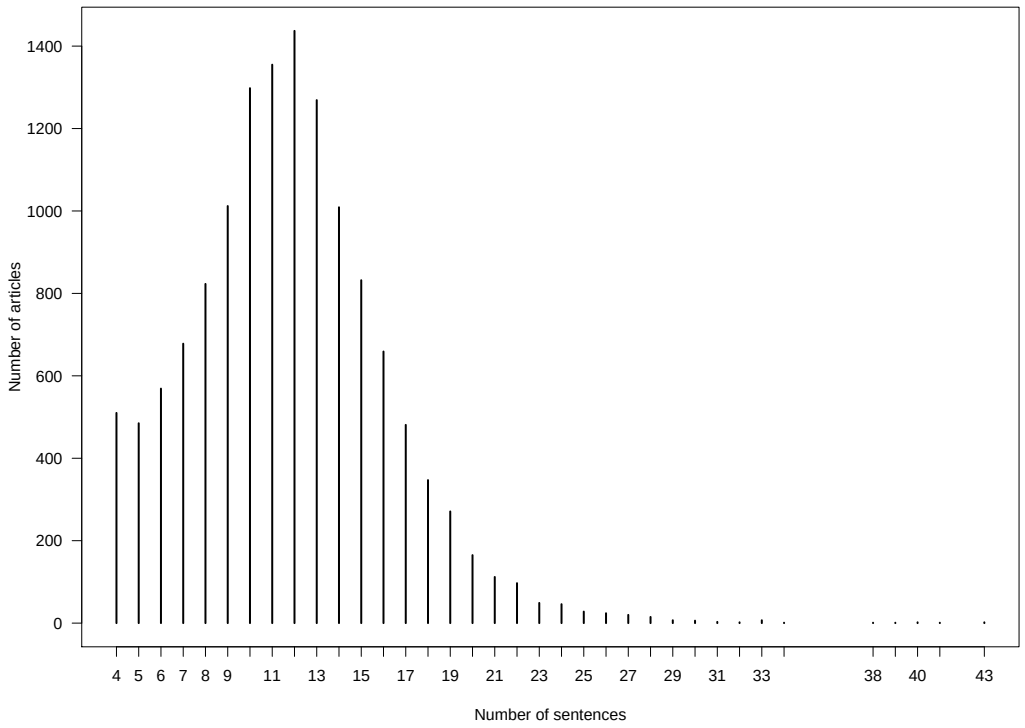


Figure 5.4: The distribution of sentences per article.

5.2.3 Sentence length and vocabulary size

We use sentence length, vocabulary size, and a selection of readability scores as proxies for difficulty. Sentence length is an often-utilised tool in the discovery of readability within corpora [139, 230]. Figure 5.4 displays the average article length. The mean article length was 9.92 sentences, and the median length was 10 sentences. We can compare to the work of Goldstein et al. [139] on the automated summarisation of news articles, which led to a corpus of 1,000 Reuters articles with a (post-summarisation) average length of 23 sentences. We can also compare this to the work of Lim et al. [230], whose smaller corpus yielded an average of 14 sentences per article.

The gap between the publication of these comparators (1999 and 2018, respectively) may suggest an overall decline in the length of news articles. It also suggests that our corpus of security-specific news is on the shorter side of the spectrum. This last point is, however, caveated by the fact that a comparison with a more

Table 5.2: A selection of readability metrics.

Metric	Score
Flesch—Kincaid	12.52
Gunning—Fog Index [314]	16.03
Coleman—Liau Index [84]	13.23
SMOG [250]	14.55
Automated Readability Index [201]	13
Average grade level	13.87

historical data, older versions of the CIS-ontology, and a wider potential variety of possible sources would be needed to further confirm this finding.

Moving on to vocabulary growth, we estimated the vocabulary growth of the corpus using Heaps' law [157], which describes the relationship between tokens and types. This law states that a vocabulary, expressed as v unique word types, is proportional to the power law of n, the number of tokens in an arbitrary text. The relation is expressed as

$$v = Kn^{\beta}$$

Here, K is a positive constant and β lies between 0 and 1. In effect, as a body of text increases, the potential to discover new distinct word types decreases. In our corpus, we can see from Figure 5.5 that the vocabulary range largely adheres to the predicted value (black line). This means that new vocabulary terms are continually arising in the data, which could complicate users' informal learning.

5.2.4 Readability scores

A readability index, such as the ones shown in Table 5.2, is an estimation of how difficult a text is to read. In online environments, it is often measured to assess click-through rates and user satisfaction [189]. Grinberg [142] utilised it, alongside sentence length, to model user engagement with news articles. As such, we consider it a variable when assessing the efficacy potential of the texts in our corpus.

Readability is determined by measuring a text's complexity, which is approximated via quantifiable attributes such as word length, sentence length, syllable count, and so on. The Flesch–Kincaid test [201] is one of the most utilised readability

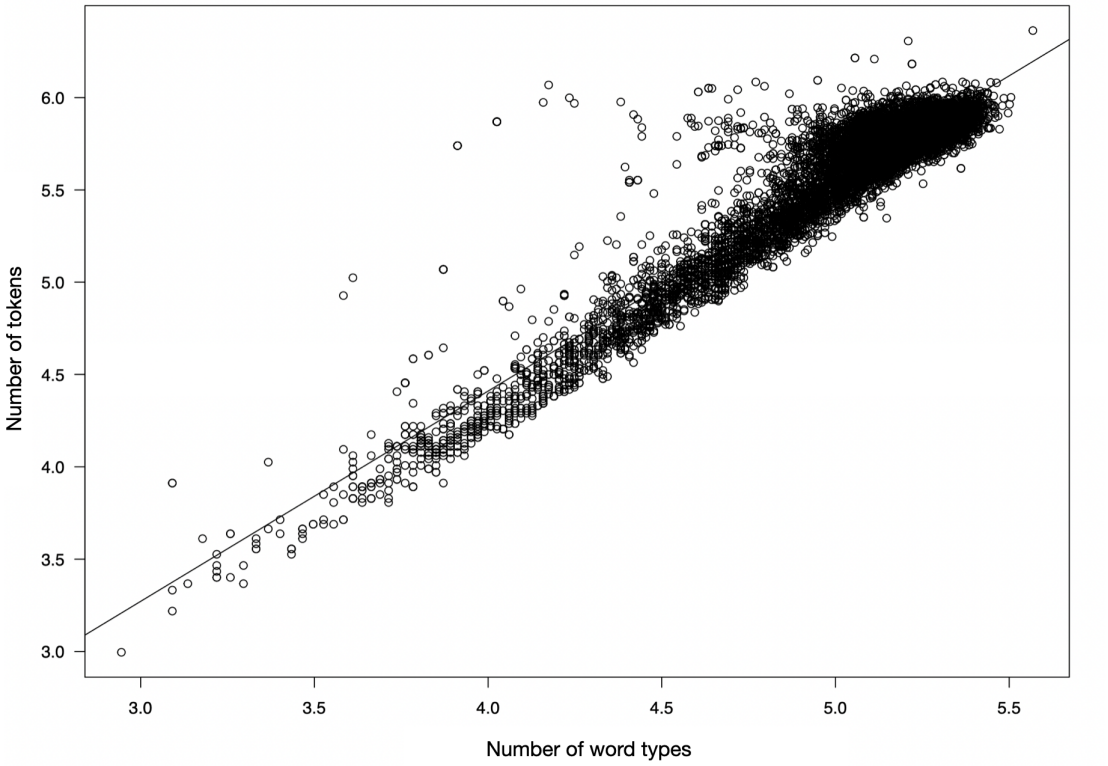


Figure 5.5: A visualisation of Heaps' law.

tests, and it calculates readability by (1) dividing the number of utilised words by the number of sentences and (2) dividing the average number of syllables per word by the number of utilised words. The scoring range starts at 100 for the easiest to read and descends to 0 for unreadable texts. As an example, the combined *Harry Potter* novels have a score of 72.83, and are often shown as a reference point for readability. By comparison, according to at least one study by Iu et al. on the readability of medical pamphlets, a score of 12 would be too difficult to read for most adults [235]. Other frequently used systems include the Gunning–Fog Index [314], which looks at sentence length and number of polysyllabic words; the Coleman–Liau Index [84], which does not assess syllables; the Automated Readability Index [330]; and the Simple Measure of Gobbledygook (or SMOG) [250], which utilises a similar methodology as the Flesch–Kincaid, but from sections within the text. All of these metrics utilise a 100–0 scoring system and are broadly comparable with each another. As such, we employ all of them in this chapter.

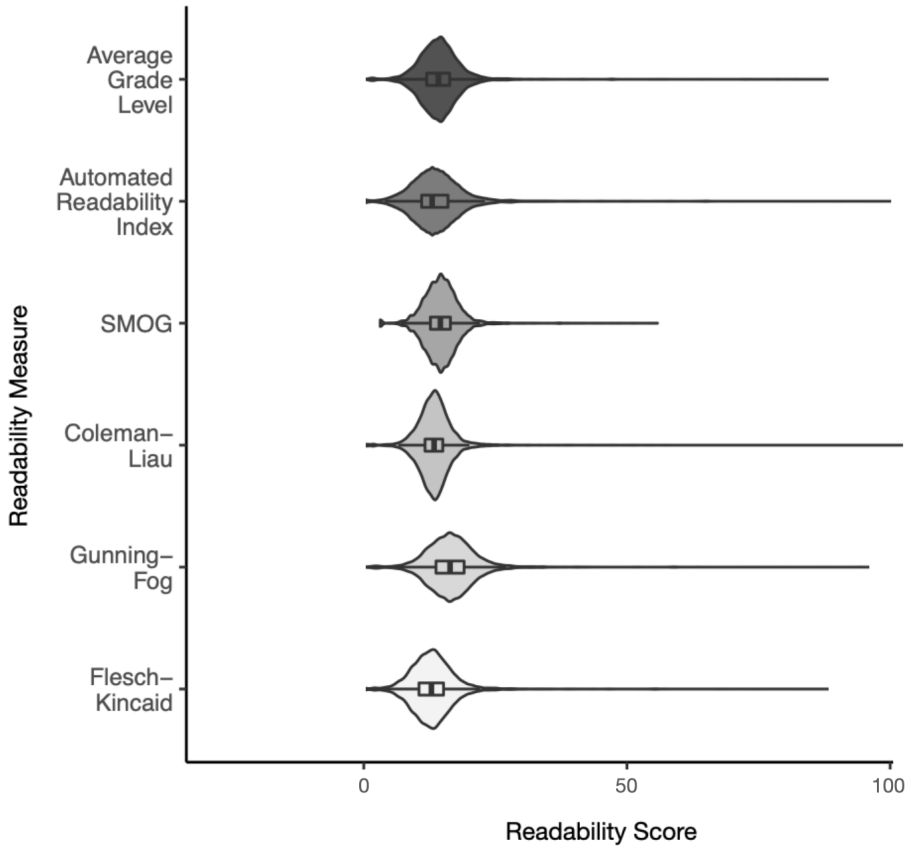


Figure 5.6: The distributions of our readability metrics.

Table 5.2 highlights a selection of readability scores, all utilising the same 100—0 scoring scale. In Figure 5.6, we see the distribution of these scores. Our p-value was less than the standard *alpha* value (set at 0.05). As we can see in Figure 5.6, there is no significant deviation in scores across the distribution of articles, which also indicates that the scores are statistically significant. The scores suggest a high degree of requisite prior knowledge in order to gain the most from reading the articles.

5.2.5 Sentiment analysis

Sentiment analysis is a group of text analysis techniques that allow for the automatic derivation of sentiment (positive or negative) from large data-sets [171]. Sentiment analysis is widely used across domains, from marketing [171] to stock market analysis [187]. Previous sentiment analysis work within the security field has focused on predicting cyber attacks or identifying potential perpetrators, for example, by

assessing sentiment in online hacker forums [238]. The lexicons generated from these studies (for example, those pertaining to sentiment within political analysis of sovereign cyber capabilities) are of limited use within our work, as their terminology often differs substantially from what could be construed as 'security advice' based on our definition. As such, we utilised Latent Semantic Scaling (LSS), which is a semi-supervised technique for scaling documents based on work by Deerwester et al. [100]. It allows for a limited set of pre-generated seed words, which are words embedded with a specific positive or negative value. To produce our small library of seed words, we utilised the SENTPROP [148] framework. We chose this framework as it combines word-vector embeddings with a label propagation approach, which are well-known techniques to generate seed-word libraries. Additionally, SENTPROP can generate accurate results with smaller corpora. [148]. In our system, the overall sentiment of a news article is correlated with the sentiments of individual words within that article, thereby allowing for a sentiment polarity check.

The results of this sentiment analysis process can be seen in Figure 5.7. The scores suggest an overall decrease in positive sentiment over the time period; however, these results are not statistically significant, likely because (1) the increase in published articles over the time period distorted the results and (2) a high p-value deviated significantly across the standard *alpha* value (set at 0.05).

5.3 Discussion

We now consider our results in the context of the research objectives of our two-part response. We focus on the results derived from our CIS framework and associated vectors in Section 5.3.1, and ascertain how the readability, vocabulary and sentiment of the corpus affects its efficacy potential in Section 5.3.2.

5.3.1 What kind of informally learnt and actionable security advice most often appears in news articles?

Three overarching themes prevail in our security corpus. The first is *data protection* (Theme 1), which is reflected in the strong focus on CIS-13 (Data protection)

Table 5.3: An overview of the themes and supporting evidence.

Theme	Supporting evidence
1. Data protection	CIS-13, Topic 3
2. Cyber-physical systems security	CIS-2, CIS-11, Topic 3
3. Personal and collective security	Topic 3, Topic 11, Topic 14

and Topic 3 of our LDA analysis. The second is *physical and digital security* (Theme 2), which is supported by CIS-11 (Limitation and control of network ports, protocols, and services), CIS-2 (Inventory and control of software assets), and Topic 3 of the LDA analysis. The third is *personal and collective security* (Theme 3) in the face of personal, business, or sovereign threats to one's security, which is supported by Topics 3, 11 and 14.

All of these themes represent a unique set of constructs and associated user behaviours. For Themes 1 and 3, a significant driver for personal security is privacy: "the right of a party to maintain control over, and confidentiality of, information about itself" [280]. Although privacy is a significant token by itself (appearing 4,887 times in the corpus), further indirect references to it suggest that it is the underlying motivation for a significant number of data protection-related articles, be they in the realm of health data, shopping data, or, more broadly, associated with the GDPR.

In Theme 2, personal security entails the need for user intervention in faulty systems, either because the system cannot determine the cause of a certain threat or the appropriate corrective action to take, or, in some cases, because the system itself is acting maliciously towards the user. These articles were the most likely to contain directly actionable security advice, and thus were the most efficacious for individual users.

Theme 3 also encapsulates threats to business and sovereignty. These articles are unlikely to contain actionable security advice, but they can aid in the creation of policy [86], which may then lead to actionable advice. These articles may even influence public opinion regarding the (cyber) security of national sovereignty, much like how terrorism news shaped national opinion and policy, as seen in work by Gadarian [129]. This cycle of influence leads to the creation of policies and

legislation, such as the aforementioned GDPR, which in turn influences public awareness of potential data security threats, ultimately stimulating new forms of cyber offense and defensive capabilities. These capabilities are then disseminated to individual users, potentially as a form of security advice. Assessing future developments within these themes and re-assessing their relevance periodically could provide a lens for evaluating the past, current, and future impact of news media on security advice efficacy potential.

5.3.2 What is the efficacy potential of this security advice as consumed by an individual user?

Many of the articles an individual user may access for cyber security advice may contain subject-specific vocabulary (such as that found within our ontological framework). Given that (1) there is limited overlap between advice sets within our ontological framework and (2) the average length of the articles in our corpus (expressed as sentence length) is shorter than the average length of comparator articles (see Section 5.2.3), there appears to be a certain level of focus within the articles that could indicate efficacy potential. However, we have also seen from ontological frameworks such as the CIS-Control schema that these tools may not encompass all of the possible security vectors within the current media environment. Furthermore, these results must be qualified given our topic modelling methodology. Our application of Heaps' law highlights the growing vocabulary within our corpus, demonstrating that the subject-specific terminology in news articles on security advice is continuously evolving. This may point to an increasingly diversified interest in security advice that is tailored to a specific, predetermined goal. This encourages us to question the efficacy potential of all-encompassing frameworks such as the CIS-Control schema.

The results of our readability tests and sentiment analysis may further challenge the efficacy potential of current media-mediated security dissemination. We find within our corpus a trend towards high reading difficulty levels: ease of reading correlated with publication type, and news articles ranked higher on all readability

indices. As all five of our assessment metrics reported statistically significant results with similar distribution scores (see Table 5.2), we can confidently assert that just 3% of our corpus was written at a U.S. school system 6th-grade level, which is typically the recommended reading level for standard distributed materials [197]. Most of the articles in this corpus require a reading level of a typical college undergraduate.

Recalling that an individual user must have (1) a sense of certainty about the content, (2) a personal interest in the content, and (3) sufficient ability to deploy the content in order to feel sufficiently compelled to act on the information, this threat control process could easily be derailed by the continued divergence and growth of subject-specific vocabulary and dense prose. Haney and Lutters [150] argue that there is a rejection threshold that informs the maintenance of security in a rapidly evolving landscape, and they maintain that individual users are approaching this threshold.

Security is not the only specialised field that deals with these dissemination issues, and it may be helpful to observe the solutions pursued in other contexts. For example, medical advice dissemination to the general public (taken here as the equivalent of our 'individual user') also involves communicating complicated concepts and extensive vocabulary to individuals who have no relevant formal training on the subject. Britt et al. [53] found that many readers stop reading medical texts if they gauge significant difficulty within the first few sentences. Consequently, the American Medical Association (AMA) and the U.S. Department of Health and Human Services (USDHHS) have set explicit guidelines that require public-facing information to achieve a U.S.-standardised readability level of 6th grade or below in terms of accessibility [197]. Extrapolating these considerations to our own corpus, it would stand to reason that increasing readability to a more generally accessible level could constitute a cost-effective remedy.

Although the overall sentiment of the corpus would not suggest that users may be being treated as an enemy (as, for example, was documented in Adams and Sasse's seminal 1999 paper [4]), it does appear that what we encountered would not fulfil Kerckhoffs' criterion for ease of use. Neither would we agree that cyber security

advice as portrayed in our corpus allows for self-efficacy upon reading. Instead, an individual user must face security topics using a multi-pronged approach, whereby self-efficacy is derived from multiple sources of increasing complexity. If the cyber security field is to continue down the path of increased specialisation, perhaps the time has come to recognise this emerging reality and clarify — in a transparent fashion — the expectations that are being placed on users.

5.4 The phenomenological aspects of cyber security advice dissemination

During the course of building the corpus we gathered a rich variety of meta-data surrounding these articles, with more than 95% of news articles containing CSS aesthetics and one or multiple images. We may remind ourselves of Section 2.6, where we learnt of the ways in which illustrations and images are often used to aid narratives. In particular, we see in Section 2.6.2 the strong potential for the links between image-use and self-efficacy potential in other fields, such as online-learning platforms and criminology. If such work highlights highlights a clear connection between aesthetics and news articles, situated within our context, then we may consider the question of our metadata as having a not-insignificant role to place in self-efficacy potential. Do these kind of aesthetics form a vital phenomenological aspect of cyberspace, as the major visual component, and if so, how may these aesthetics have an impact on the narrative which cyber security experts portray when constructing advice for dissemination? We attempt a novel form of exploration of aspect of cyberspace, taken in our familiar context of cyber security in Chapter 6.

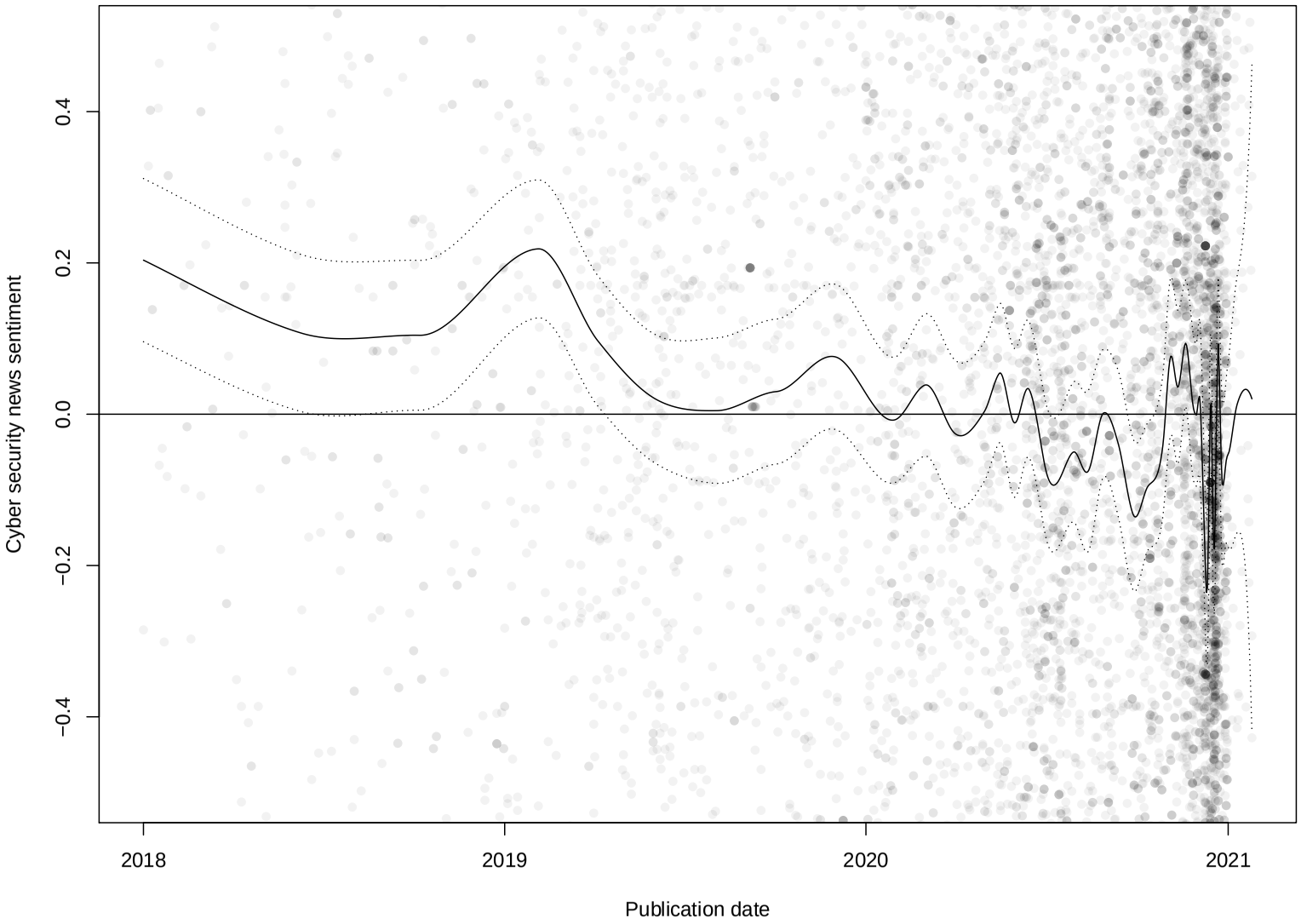


Figure 5.7: A visualisation of changing sentiment, depicting a slight increase in negative sentiment along with a corresponding increase in article generation.

6

The aesthetics of cyberspace security

Having identified some of the epistemic issues behind cyber security advice, the question of the phenomenological aspects behind the way in which they are delivered are now questioned, completing our dive from the environmental into the phenomenological elements of cyberspace.

Visual media like illustrations [231] and diagrams [154] have accompanied text since the very first written documents [273], providing clarification, communicating distinct emotions or opinions, and serving more subversive ends like propaganda [244, 88, 258].

Today, digital technologies have introduced new types and ways of accessing visual media while rapidly integrating media consumption into the daily lives of large segments of the global population [98]. Still, contemporary online news articles and blog posts are often accompanied by visual media that serve many of the same communicative purposes as those in the earliest human documents [263].

Understanding how visual media work to support communication and learning is a complex task, and it is divided amongst many scholarly disciplines. First and foremost amongst these is the ancient philosophical branch of aesthetics, which concerns itself with the nature of perception, taste, and sensory quality / value (e.g., beauty). In the context of this chapter, aesthetics entail the perceptual logic that allows individuals to instinctively analyse meaning and appraise quality / truth when

consuming visual media — whether as stand-alone objects, as part of a user interface, or as an accompaniment to text. By extension, learned aesthetic preferences may influence how individuals navigate information or environments [119, 184, 335, 70], and they may play a significant role in informal learning.

In the sub-area of cyber security aesthetics, Ma [237] outlined various cyber security visualisation techniques and Shires [335] looked at the adaptation of neo-noir aesthetics in cyber security visual media. Shires in particular is noteworthy as he investigated the content creator themselves, who often stated they were required to create content with neither insight into the issues they were meant to portray, nor the personal/professional cyber security background with which to relate [335]. There is also work within the field of digital exhibits [36] and the transfer of security aesthetics into cyber security [133].

These ideas are supported by what we saw in Chapter 2 , where the fields of usable security and cyber security have used visual media to support learning. Furthermore, in Section 2.6.2 we saw that an analysis of the aesthetics which accompany news articles about cyber security may also reap insight into their effect on the individual user. Returning to our research question in Section 1.1 (What do cyber security aesthetics look like to an individual user, and what are their efficacy potential?). In order to answer our question, a two-part response was developed:

1. *To ascertain what cyber security aesthetics consist of, from the perspective of an individual user (the reader is referred to Section 2.4 for this definition.)*

2. *To provide an explorative discussion as to the manner in which these aesthetics may affect users' perceived self-efficacy as they informally learn cyber security precepts.*

The remainder of the chapter is organised as follows. In Section 6.1 we provide the background to, and the motivation for, the work described in this chapter. In addition, we define some of the terms of interest. In Sections 6.2 and 6.3 we present and discuss our results, before placing them in a broader context in Section 6.4. Finally, Section 6.5 concludes the chapter.

6.1 Cyber security aesthetics: additional background

In this section we discuss the additional background we require to allow for an accurate assessment of our results. As aesthetics is such a broad and sometimes ambiguous term [102], we begin by providing an overview of aesthetics research in Sections 6.1.1 and 6.1.2, establishing its relevance for our research questions. We then consider the potential efficacy of aesthetics for cyber security in Section 6.1.3. Section 6.1.4 then summarises our expectations.

6.1.1 Aesthetics and meaning

In Ancient Greece, aesthetics were first described as a 'sensation', or the ability to interact with external stimuli through our bodily senses [30]. Later, Kant [188] espoused the importance of aesthetics for all human domains, arguing that, without its sense-making power, data would simply remain chaotic, lacking meaning and structure.[1] However, if aesthetics help to render a *shared* sensible reality, as asserted by Kant [188, 395], then aesthetic perception must be universal, narrative, and standardised. This brings us into the sphere of semiotics — the study of signs, symbols, and symbolisation, or of the devices and practices that help to stabilise meanings.

For the purposes of this chapter, we define aesthetics as the perceptual logic that allows individuals to instinctively analyse meaning in visual media, and semiotics as the conventionalised meanings arising from this perceptual process. In other words, where aesthetic objects exist solely for their own purposes [188], informing perceptible meaning [376, 387] without *requiring* a specific meaning to be understood, semiotic objects contain explicitly built-in meanings, whether skeuomorphic[2] or

[1] This could mean that data acquires a certain aesthetic once created (mathematical aesthetics [188]), or that, to have an aesthetic perspective, one must assemble data fragments into something meaningful regardless of outcome [188].

[2] Skeuomorphism is defined as an object or feature which imitates the design of another object, but does not serve the same purpose as the object it chose to imitate. However, the imitation is seen as necessary as its association with the object it chose to imitate enhances the skeuomorphic object's meaning in context [29].

otherwise [70, 26], and can enhance the meaning of words they are associated with (for example, as a compendium to a body of text [102]).

Both aesthetic and semiotic perspectives remain relevant in contemporary philosophical discourse, as well as in the practice of cyber security. For example, Cheng et al [81] describe how viewers attempt to derive meaning from *key referent objects* contained within an image. Insofar as these objects are universally understood, they may yield what Ranciere calls 'a shared sense of perception' [325]. Furthermore, in the context of cyber aesthetics, most interactions at the interface level are directed by symbols and imagery such as icons, pointers, image thumbnails — which themselves can contain semiotic objects — and so forth. All of these objects help to convey a system logic to end users, thus enhancing accuracy and intuitiveness [318].

6.1.2 Aesthetics and learning

Because we are primarily interested in how users may interpret cyber security aesthetics in an informal learning context (as highlighted in Section 2.5.2), our understanding of aesthetics informally learnt is informed by contributions such as that of Chatterjee [77], which draws from the humanities and sciences to illustrate how aesthetics influence the choices humans make in their given domains of activity. Earlier work by Carper [68] went further, identifying aesthetics as one of four distinct structures human beings use when developing knowledge, the other three being personal, empirical, and ethical. For Carper, the 'knowing' of aesthetics takes the other three structures and enhances them into a new understanding, creating meaning from otherwise abstract works [68]. Building on Ancient Greek notions of aesthetics, Keenan [194] proposed the concept of 'aesthetic knowledge', wherein sensory experiences form embedded relationships with phenomena such as colour and shape. According to Keenan, when prior aesthetic knowledge is combined with information (or, in our case, images) from user interfaces and other elements within a digital experience, users can associate prior meanings with this new information and thereby generate unanticipated interactions [194].

Taken as a form of knowledge, aesthetic design can enhance users' ability to make effective decisions based on a mixture of intuition and explicitly learnt knowledge [69]. We know that people often make decisions based on intuition rather than analytical inference, 'sensing' a correct choice without being able to offer a logical explanation for it [395]; we may also expect that aesthetic objects can serve to stimulate this intuition. For example, within human–computer interaction, supplementary visual assets that convey a feeling of uncertainty or ambiguity can help individuals to comprehend uncertainty even when it is not explicitly communicated in words [118]. It follows that aesthetic knowledge will impact knowledge acquisition in any given field, including fields where many users rely on informally learnt knowledge (such as cyber security [303]) or cases where decision makers do not have prior experience with the given situation [395].

6.1.3 Aesthetics and self-efficacy

Clearly, the way in which we are presented with information visually impacts our understanding of, and subsequent decision making towards, a particular topic. As such, usable security research, user interface design, and cognitive psychology theory have sought to better understand how and why users make aesthetic decisions, and how aesthetic attributes can be designed to achieve certain ends. For instance, some scholars studying the ethics of technological development have proposed tools to help designers build fairness and transparency into digital libraries and interface designs through deliberate aesthetic planning [26]. Other researchers have explored how particular aesthetic / semiotic interpretations of user interfaces can enable users to complete a given task more efficiently, for example, visual cues like broken glass or blurred text could denote danger or need for care [70]. This latter effect is particularly interesting in the context of cyber security, given the increasing responsibilisation that individual users have to bear for protecting themselves, their devices, and their networks online.

One important concept implicated in users' decision making is self-efficacy — a generative capability to organise one's skill-sets and beliefs towards a desired

outcome [25]. According to self-efficacy theory, individual users implicitly judge their own ability to cope with a given situation, thus developing self-efficacy beliefs for a specific domain. These beliefs inform whether individual users will initiate certain behaviours and carry them through to successful outcomes [241, 25]. Furthermore, self-efficacy is closely related to motivation: the greater the challenge a user faces, the more self-efficacy they will need to sustain their motivation with which to overcome barriers to their current ability [25, 352, 200]. Because cyber security is perceived to be both important and complex, users tend to exhibit limited self-efficacy in this domain (as explained by Herley [160] and explored by Halevi et al [146] through psychological and cultural means).

Many people develop some degree of self-efficacy through their identification with role models: people similar to themselves who display, and thereby make accessible, certain aspirational attitudes, behaviours, or capacities [7]. For example, Bosma et al [47] observed that role models in the media can encourage entrepreneurship amongst their viewers. Applying these insights to cyber security aesthetics, we may suggest that researchers can utilise aesthetics to enhance users' self-efficacy by providing models, structuring and directing behaviour towards goal setting, and measuring progress towards these goals [69].

6.1.4 Our expectations for this exploration

To summarise, we expect that users acquire an aesthetic literacy when they are repeatedly exposed to domain-specific content, and that this literacy helps them to navigate and derive meaning from future content. As per the first part of our response, we aspire to understand the aesthetics (and thus aesthetic literacies) operative in the domain of cyber security, and so we will imaginatively replicate the process whereby users develop these literacies — that is, repeated exposure to the aesthetic objects of cyber security — by compiling an image-set of cyber security's primary aesthetic objects, allowing us to appraise and compare them at once. We have defined these objects to be images that may themselves contain legible signs, and which are typically part of a larger piece of content like an online

article. For the second part of our response, we will interpret the resulting aesthetics in terms of their likely effects for users' self-efficacy.

Of course, in a nascent field like cyber security, aesthetic systems have not necessarily been formalised into stable semiotic resources. As such, we must not preemptively constrain our analysis to specific image contents, addressing instead the full spectrum of aesthetic objects relevant to cyber security communication. In this case, we define these to be *(visible) digital image-objects that may themselves contain semiotically legible signs, and which have been added as an adornment or supplement to relevant cyber security literature.* Although this definition presents some limitations (discussed in due course), it allows us to account for the narrative functions of aesthetics, as well as for its use in learning.

6.2 The image-set: results

Using the process described in Sections 3.2.3 and 3.2.4, we compiled an image-set that covered a wide swathe of cyber security topics and their associated aesthetics. The image-set spans 1,010 images and is derived from (English language) news and online magazine articles from the U.S., Canada, and the U.K. The images are organised into several classes, which we derived by extracting visual information from the raw images and mapping them to semantically meaningful keywords, and performed a colour similarity analysis. Small selections of images from each class are shown in Figures 6.1 and 6.2. Through the process described in Sections 3.2, we identified 32 distinct and internally consistent image classes in the image-set. These ranged from abstract interpretations of networked security to imagery depicting the binary view of cyber security as an eternal battle between malicious actors and their victims. However, because most of the images (80.6%) were concentrated in just ten major classes (as detailed in Table 6.1), we restrict our discussion to these classes. We further group these classes into four broad (but not mutually exclusive) categories: Objects, People, Places, and Others.

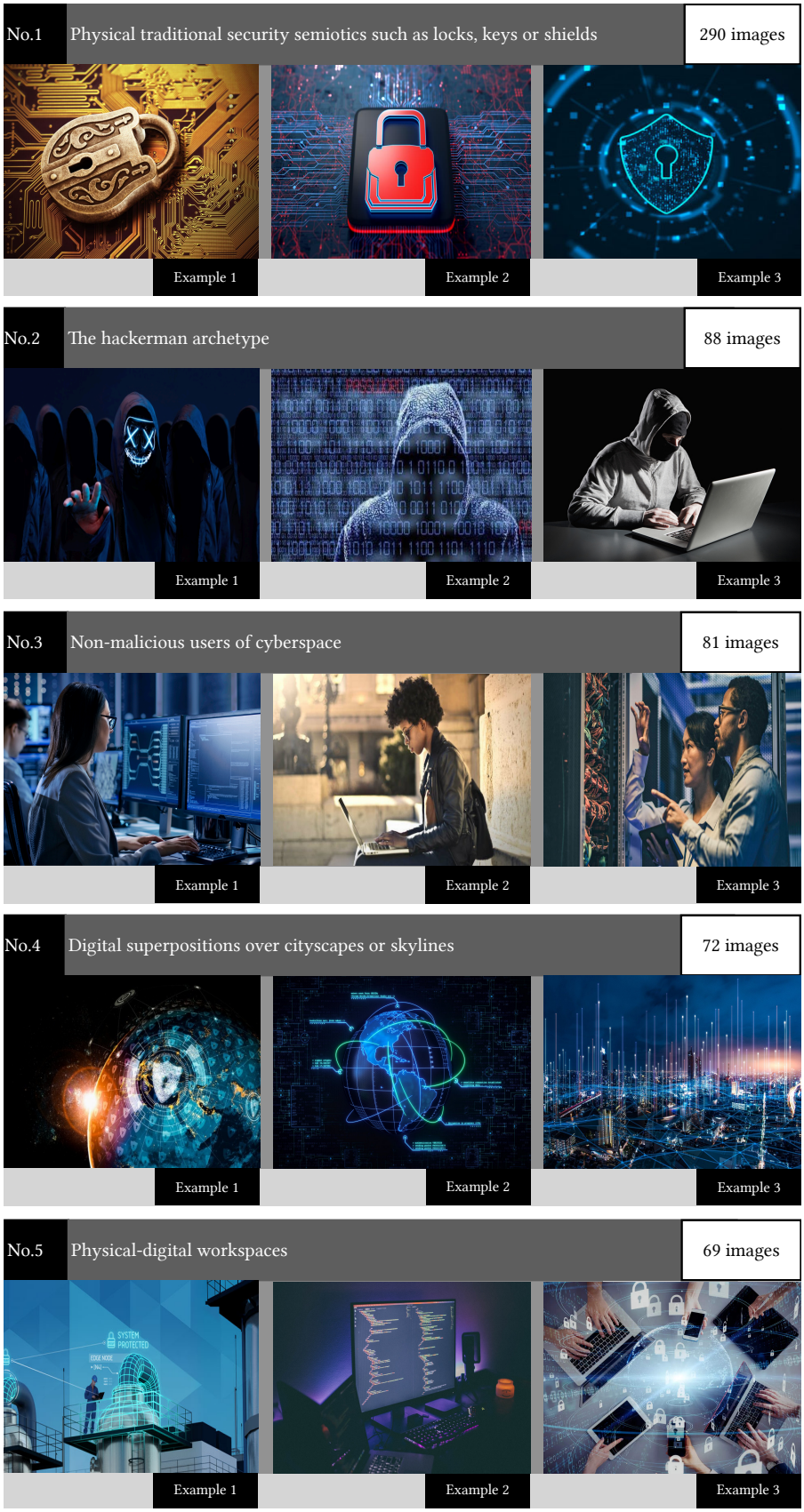


Figure 6.1: A random selection of images taken from classes 1-5.

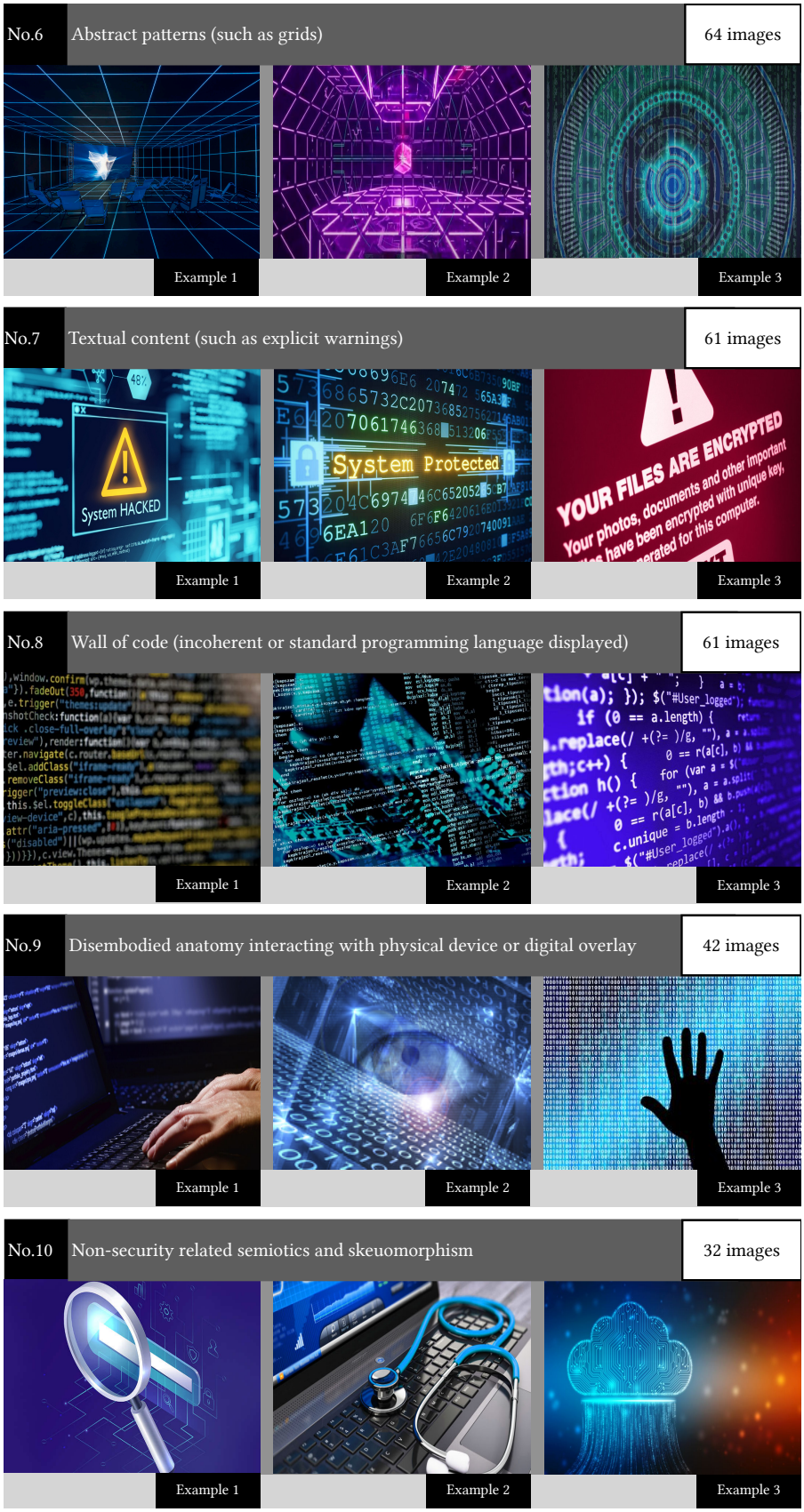


Figure 6.2: A random selection of images taken from classes 6-10.

Table 6.1: The top ten classes in our image-set.

Class	Description	No.
1.	Physical traditional security semiotics (such as lock, key, or shield)	290
2.	Hackerman archetype	88
3.	Non-malicious users of cyberspace	81
4.	Digital superpositions over cityscapes or skylines	72
5.	Physical-digital hybrid workspaces	69
6.	Abstract patterns (such as grids)	64
7.	Textual content (such as explicit warnings)	61
8.	Wall of code (incoherent or standard programming language)	61
9.	Disembodied anatomy interacting with a physical device or digital overlay	42
10.	Non-security-related skeuomorphism	32

6.2.1 Colour

As one would expect, colour features heavily across all of the classes in our image-set. If we use the heat-maps to discuss similarity potential across colour and texture (where radical differences may indicate domain-shift within the class [324]), then this section concerns itself with the qualitative *use* of colour as we see it across the complete image-set.

Where many of the abstract forms seen in Class 6 utilise hues running the gamut from greens to blues which are almost always contrasted by dark backgrounds, it is clear from the complete image-set that no 'universal' definition or convention on the usage of colour exists within cyber security, beyond the heavy use of cyan blue[3].

All of the heat-maps highlight these similarities in colour. Where we find points of interest are in Class-1, where colour is used to denote objects as being of specific importance, ranging from useful to dangerous. We may contrast this with another aspect of cyberspace, the video game, where emphasis is placed on the colour of objects the player may interact with [181]. This codification of objects

[3]This was already informally known to the cyber security community, where the cyan blue code #235594 was the most commonly found colour in a large image-set, but which is not explicitly referenced to here due to the fact it was not cleaned for duplicates and other issues, and contained little in the way of search methodology. It can be found here: `https://daylight.berkeley.edu/cybersecurity-imagery/`.

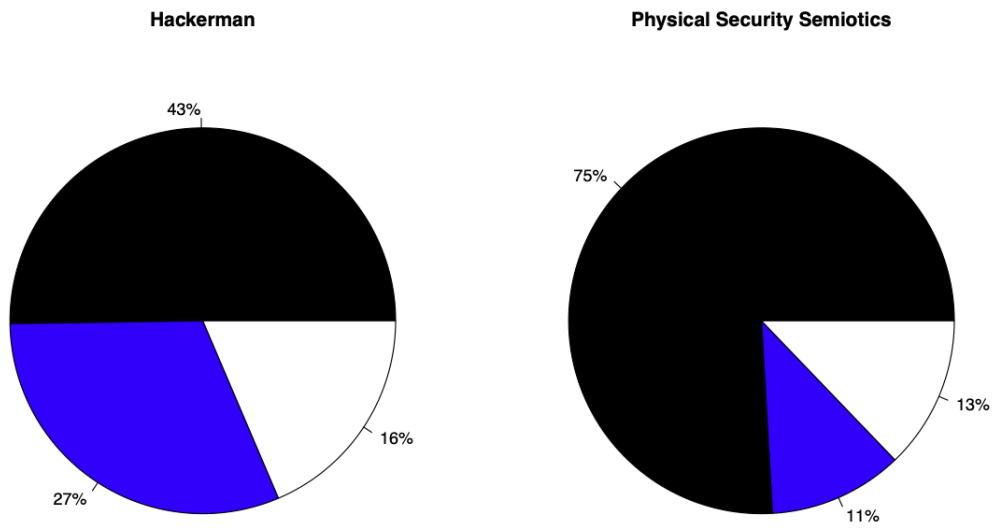


Figure 6.3: An example of the most commonly used colours within our top-two classes, simplified to 4-bit.

again lacks a specific narrative, and objects that are beneficial often share hues with those semiotics deemed dangerous.

In between the classes, a specific colour analysis leads to results of limited immediate utility. Turning our attention to Figure 6.3, we see that our top-two image classes share a penchant for blacks, blues and whites.

With this large amount of blacks and darker hues serving as background, we see in many classes a contrasting effect between the brightly coloured objects, spaces and vertices. In this manner, we hypothesise that colour may be used to draw the user's attention to these objects, which exist in a space with no other domains to draw inspiration from, similar to video games [181]. A colour analysis may not allow us to infer further specifics as to their self-efficacy potential, in which the colours may be used to deliver a decoding of the messages present in the accompanying textual content. Instead, we look towards the objects, people, places and other aspects of the image. In these cases, we find the heat-maps to be of more use as an accompaniment to assess the credibility of the assertions. Each heat-map represents the relationship any given image has to the other images within its class, with blue cell colours indicating greater similarity and red cell colours indicating lesser similarity.

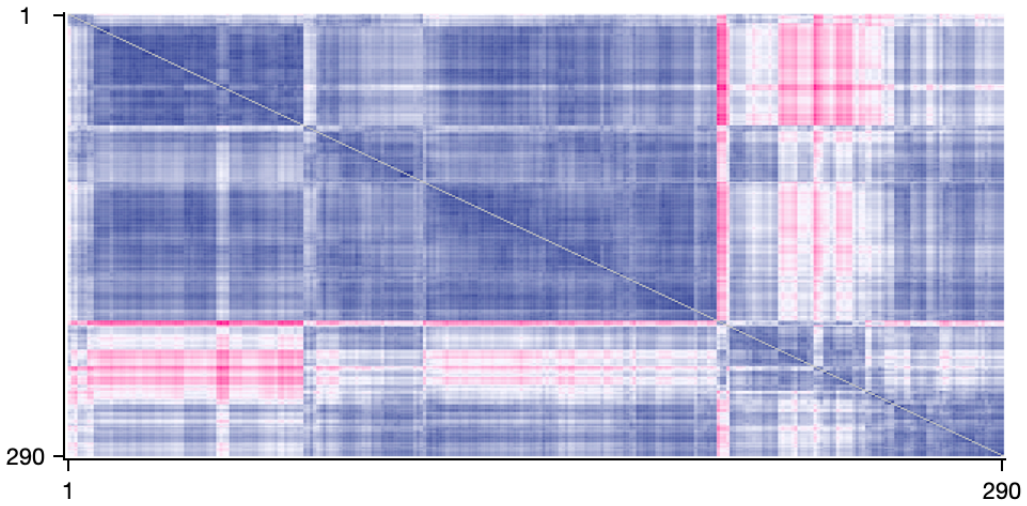


Figure 6.4: Heat-map highlighting the overall colour differences between images in Class 1 (Traditional physical-digital security semiotics).

6.2.2 Objects

Classes 1 and 10 feature objects associated with physical security, like locks, keys, and shields (and others identified by Ghertner [133]); objects appropriated from non-security domains, such as cameras; and skeuomorphic adaptations of real-world objects, like digitised versions of envelopes. Class 1 contains 290 unique images with extraordinary colour similarity (as per Figure 6.4), implying consistent use of similar semiotics and colour schemes throughout. Class 10 is much smaller, featuring only 32 unique images, but it is notable for its wider variety of objects and colours (see Figure 6.5).

6.2.3 People

Classes 2 and 3 feature individuals who are implied to be malicious (Class 2) or non-malicious (Class 3) users of cyberspace. We also include Class 9 within this group, given its emphasis on human anatomy. Class 2 contains 88 unique images with significant colour similarity (see Figure 6.6), which in this case implies similar compositions — individuals assuming similar stances against similar (dark) background colours. Class 3 consists of 81 unique images and is slightly more varied in its make-up (as per Figure 6.7). Class 9 is the smallest and most differentiated class

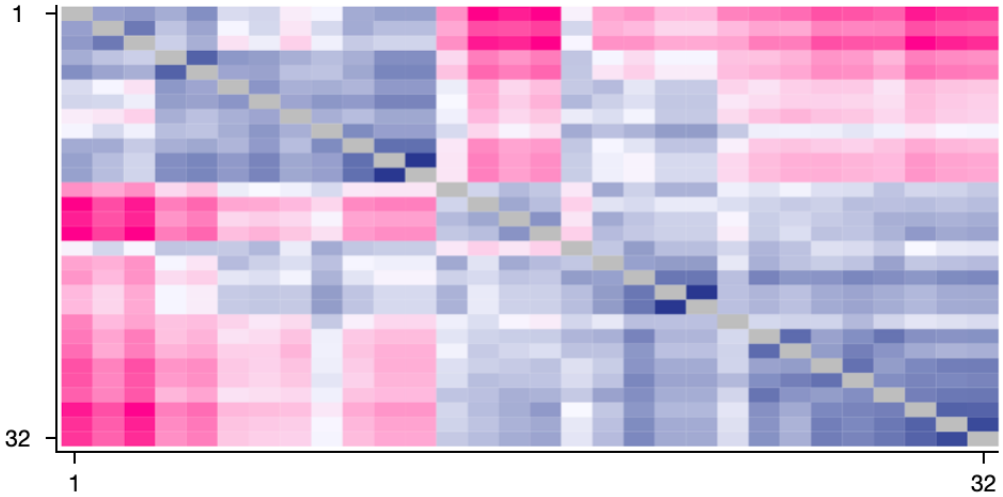


Figure 6.5: Heat-map highlighting the overall colour differences between images in Class 10 (Non-security semiotics and skeuomorphism).

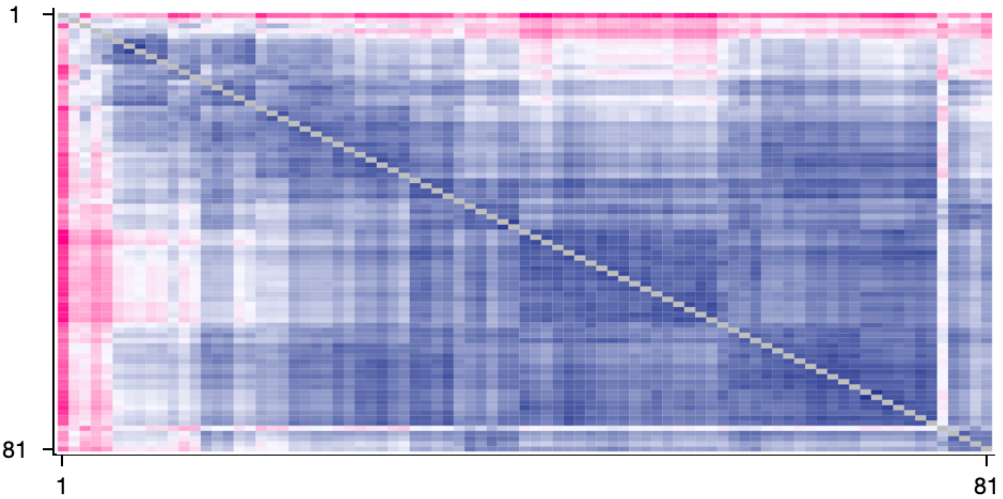


Figure 6.6: Heat-map highlighting the overall colour differences between images in Class 2 (Hackerman archetype).

in this group, consisting of only 42 unique images with wider colour discrepancies in the heat-map (see Figure 6.8). Figure 6.1 highlights some images from classes 2 and 3, with Figure 6.2 showing examples from class 9.

6.2.4 Places

Classes 4 and 5 feature specific places related to cyberspace and cyber security, such as futuristic urban spaces (Class 4) and workspaces (Class 5). Class 4 contains 72 unique images with significant colour similarity (see Figure 6.9), once again

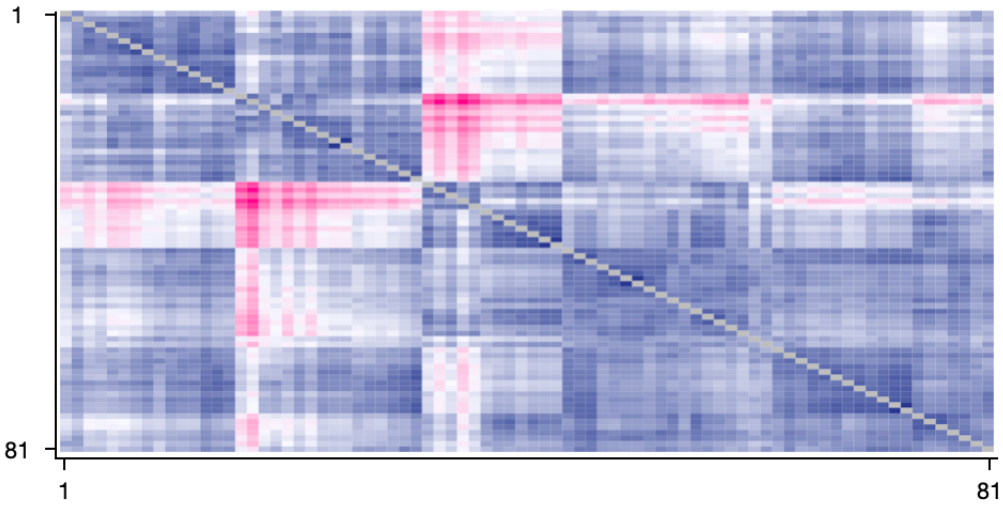


Figure 6.7: Heat-map highlighting the overall colour differences between images in Class 3 (Non-malicious users of cyberspace).

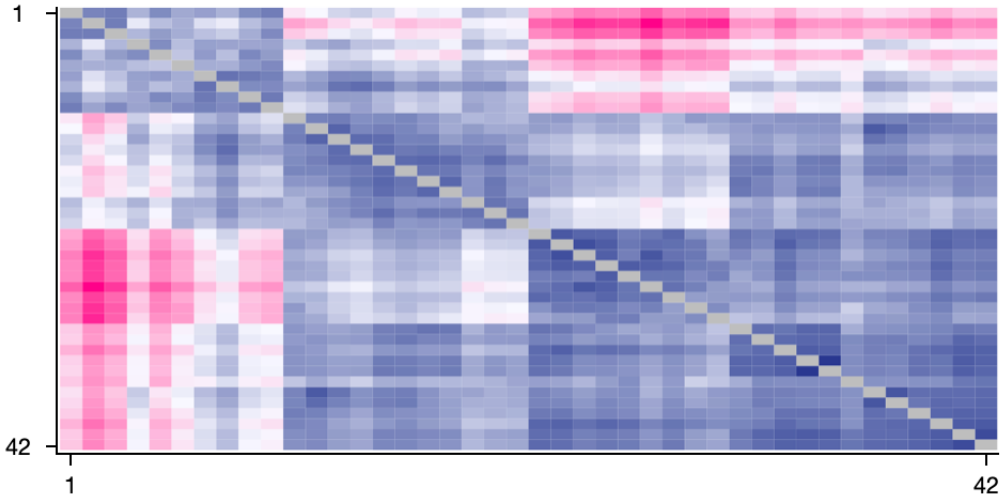


Figure 6.8: Heat-map highlighting the overall colour differences between images in Class 9 (Disembodied anatomy interacting with a physical device or digital overlay).

implying similar compositions and colour palettes. Class 5 consists of 69 unique images and is more varied, as can be seen in Figure 6.10. Figure 6.1 highlights some examples from Classes 4 and 5.

6.2.5 Other

Classes 6, 7, and 8 variously encompass imagery of digital patterns, alphanumeric symbols, and other two-dimensional or abstract representations of cyberspace and cyber security. Class 6 contains 64 unique images with reasonable colour similarity

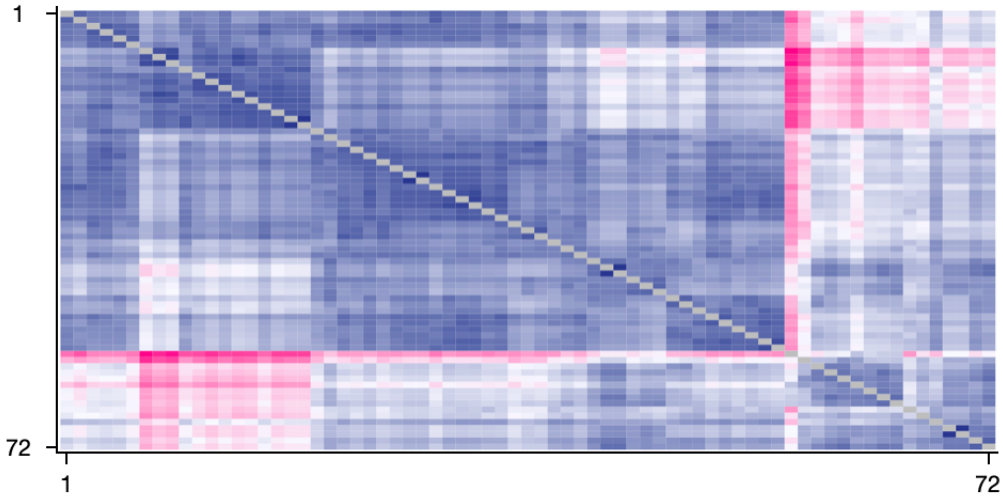


Figure 6.9: Heat-map highlighting the overall colour differences between images in Class 4 (Digital superpositions over cityscapes or skylines).

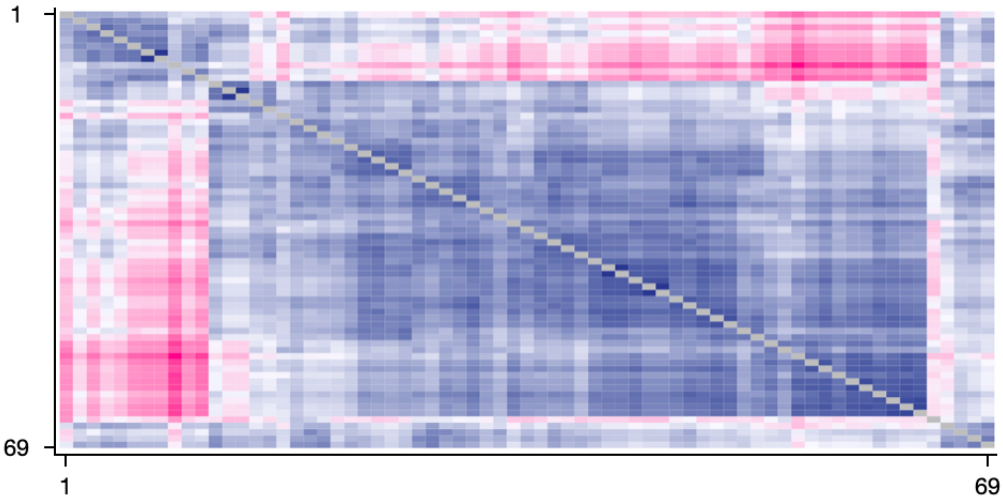


Figure 6.10: Heat-map highlighting the overall colour differences between images in Class 5 (Physical-digital hybrid workspaces).

(as per Figure 6.11); though similar background colours are frequently used to represent mathematically defined patterns and shapes, there is some variation based on other, supporting semiotic attributes in this category. Class 7 consists of 61 images that are slightly more varied, as seen in Figure 6.12). Meanwhile, Class 8 contains 61 images, and it is the most diverse of the three (as visible in Figure 6.13. However, the representativeness of Class 8's heat-map is limited by the content of the images, namely incoherent alphanumerical symbols or programming languages on a dark background. We expect that the variation in the heat-map reflects the

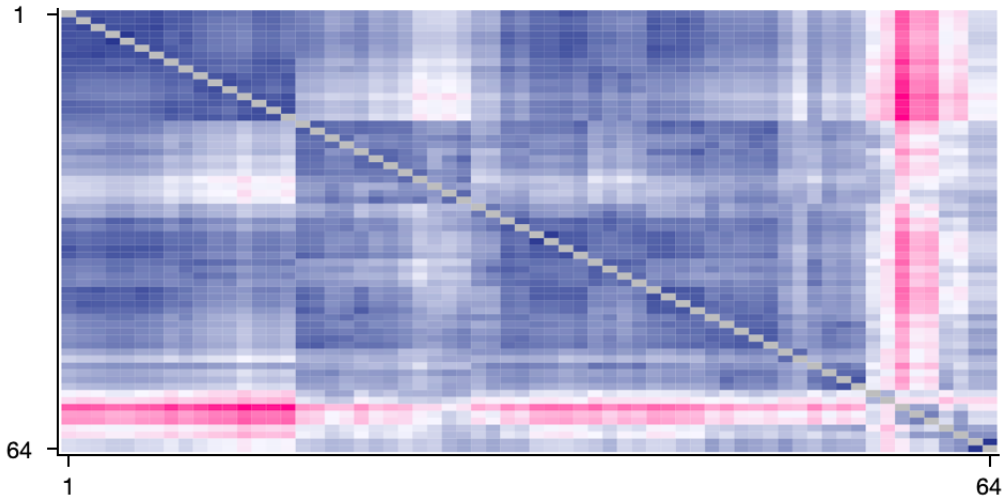


Figure 6.11: Heat-map highlighting the overall colour differences between images in Class 6 (Abstract patterns).

wide variety of colours used in these different symbols, despite larger compositional similarities. Figure 6.2 highlights some examples from Classes 6, 7, and 8.

6.3 Discussion

In this section we argue that the aesthetic classes established in the previous section can help to prime readers' interpretations of associated texts in ways that affect their self-efficacy. Insofar as the images that accompany cyber security texts are created and selected for this specific purpose (that is, for inclusion in these texts), we may say that the observed aesthetic trends are more or less deliberate attempts to frame cyber security in a certain manner. Accordingly, we begin with an analysis of the semantics of cyber security — the colours, shapes, and devices used throughout the image-set — to understand how cyber security is being framed. We proceed to analyse the image classes that feature objects, people, and places. We finish this section by framing these discussions in light of our research questions and what we learnt in Chapter 2 on media-based learning, and in Section 6.1.

6.3.1 The visual vocabulary of cyber security

Our image-set suggests that cyber security exists at the limits of traditional human visibility. Indeed, many of the image classes feature abstractions of objects,

situations, individuals, and landscapes rather than concrete subjects. This seems consistent with typical evocations of 'cyberspace' — a term coined in 1982 by science-fiction writer William Gibson [135] to designate 'a new universe' parallel to the physical but created by the digital [33] (as encapsulated in the 'fifth branch' metaphor utilised by the U.S. military [51]). Although the term has since become synonymous with global computer networks such as the Internet, it continues to encapsulate the 'sublime' sensations associated with a new frontier. Nye [277] explained that, when users are introduced to powerful new technologies (such as cyberspace or a digital system), they experience a pleasurable yet terrifying sensation that alerts them to the limits of their reality.

Multiple scholars have explored how aesthetic choices can help to acclimate users to the new reality of cyberspace 'environments'. Featherstone and Burrows [116], for instance, argued that aesthetics help to evoke imagery of life in the domain of cyberspace, while Croon [90] explained that imagery can provide insight into a domain and help to cultivate a form of spatial awareness within it. Within our image-set, we observed heavy use of mathematical aesthetics such as concentric arcs, simple and tileable shapes (such as hexagons, albeit with a higher area-to-perimeter ratio), and connecting lines. Where these devices construct the *shape* of cyberspace, *colour* establishes its tone. In our image-set, we observed a preponderance of dark shades and blue hues. This is consistent with the work of Shedrof and Nussel [333], who researched the use of colour within the domain of science fiction. One possible reason for this preference in science fiction and cyber security is the relative rarity of blues in nature [141]; because this colour is scarce in our physical domain, it effectively communicates cyberspace's distinction from the straightforwardly physical and natural.

Of the classes identified in our image-set, the ones that most optimally represent cyberspace as a techno-spatial domain separate from, but parallel to, our physical reality are Classes 3, 6 and 8, which represent 16% of our total image-set. These classes deploy the aforementioned aesthetic tactics most consistently / legibly.

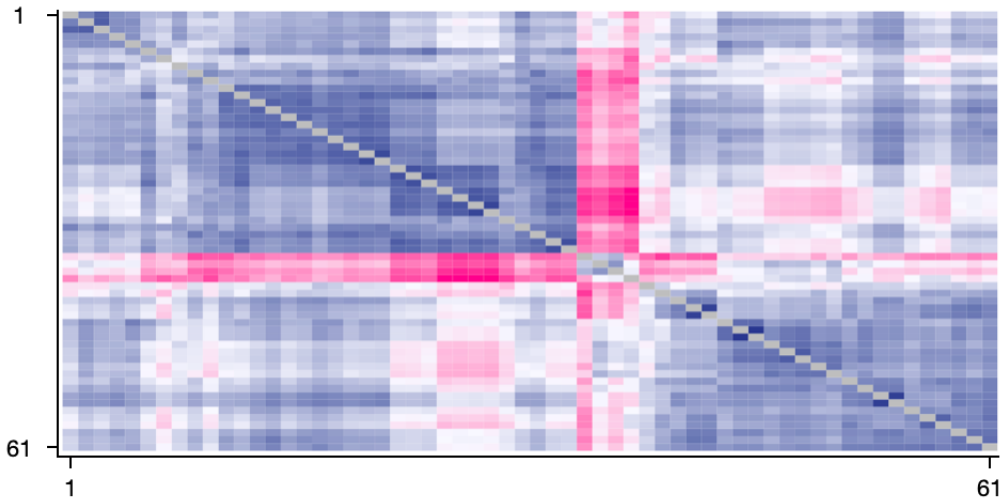


Figure 6.12: Heat-map highlighting the overall colour differences between images in Class 7 (Textual content such as explicit warnings).

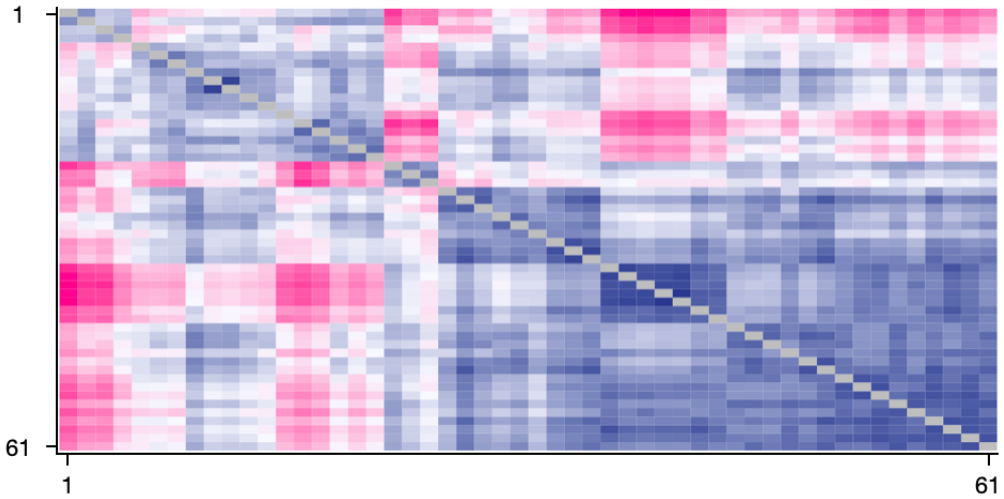


Figure 6.13: Heat-map highlighting the overall colour differences between images in Class 8 (Wall of code).

6.3.2 Physical traditional security semiotics

Beasly and Danesi [31] argue that semiotics researchers are mainly interested in understanding how individual signs, objects, and concepts coalesce into a coherent visual narrative. Objects such as locks, shields, and keys appeared frequently in our image-set, either as digital manifestations of physical objects or, in rare cases, as physical objects in a hybridised physical-digital environment. These objects represent 20% of the total image-set, and a selection can be found in Figures 6.1 and 6.2.

As these objects often pre-date the development of cyberspace, they may initially evoke physical, rather than digital, security, being grafted onto cyber security only later to represent what security might mean in cyberspace. As is the case with skeuomorphic interface design, wherein new signs or symbols are developed from prior objects (retaining the original's ornamental design cues), the new semiotic interpretation may have superseded the older meaning. Nonetheless, any theoretical constructs associated with the originator sign have likely been carried forward [193].

According to Ghertner et al [133], security could be seen as a form of negation, with security signs suggesting the *absence* of malicious activity. The lock is a powerful symbol of security in the real world, the key a symbol of legitimate authority, and the shield a symbol indicating defense in the event of an attack. These symbols can also be rendered differently to present a kind of advanced warning system; imagery of a broken lock, key, or shield might alert the user to potential security infractions.[4]

6.3.3 Hackers: anatomy, gender, and race

Humans were represented in 16.4% of the images in our image-set. Using our codebook, we assigned each of these images to one of two binary categories: the malicious *hackerman archetype* (8% of our total image-set, and just over 52% of our total human representations) or non-malicious users (7.8% of our total image-set, and just under 48% of our total human representations). An additional 4% of our image-set contained anatomical images, such as those seen in Class 9. These anatomical images were largely restricted to two types: those featuring hands and those featuring eyes.

Our image-set broadly suggests a lack of equal representation in cyber security aesthetics, and thus a lack of diverse role models. Just under 1% of our hackerman archetype features feminine-presenting people; all others were either masculine-presenting (63%), implied to be men, or had their secondary-sex characteristics obscured (for instance, by a mask). While we do see a wider variety of individuals

[4]It must be pointed out, however, that we did not come across any broken or damaged semiotic objects in our image-set.

amongst the non-malicious users — 63% of these images contained masculine-presenting individuals, 37% contained feminine-presenting individuals, and 20% contained people who appeared to be of a non-white background — this does not necessarily represent the gender or racial/ethnic background ratio of audiences who engage with cyber security content, but that of the organisations that produce cyber security digital media.[5]

Our image-set also seems to attribute disparate expertise — and thus responsibility for cyber security — to different individuals. The hackerman, for instance, is presented as a 'lone wolf', whereas non-malicious individuals are more frequently depicted in groups than as solo actors.[6] One could interpret this to mean that individuals lack the talents or other requisite knowledge that the lone hackerman possesses [343], and must therefore work together to counter the hackerman's threats. The media promotes this association by applying the hackerman stereotype to organisations such as 'Anonymous' and online communities such as 4chan, placing these groups in a position to dominate the conversation. In turn, individual users may view these entities as malicious experts, abdicating their own responsibility for cyber security based on their feelings of powerlessness [343].

Finally, our image-set features moral ambiguity and vague representations that could make it difficult for users to derive context from images. For example, while the hackerman is supposed to engage in malicious online activities, he is sometimes presented with morally ambiguous or vigilante imagery like the 'V for Vendetta' mask, complicating the viewer's understanding of his aims. While non-malicious individuals are consistently depicted as benign or neutral, they are frequently engaged in a variety of nondescript tasks, like interacting with hacked devices, responding to being hacked, or performing some kind of professional work (for instance, as cyber security professionals). Images of human anatomy were similar; though hands are an important and highly visible part of the human body [177]

[5]Statistics from the U.S. Bureau of Labor Statistics indicate that 18% of cyber security specialists are women [179], which may provide a reference point for the 37% of human images featuring feminine-presenting people.

[6]This is particularly pronounced in images featuring feminine-presenting people, who in many cases are accompanied by masculine-presenting people.

that can serve as a heuristic to facilitate learning [137],[7] in our image-set they were engaged in a variety of mostly unclear / un-directed movements and positions, often in connection with physical devices like laptops. Images in which the eye was dominant were similarly varied, but in many cases represented the moral ambiguity of a panopticon (alongside images from other classes that render a retina and cornea from composite imagery) or enjoined the user to pay attention [130].

By depriving users of role models, clear contexts / goals, and the means or abilities to achieve such goals, these issues likely undermine individual users' self-efficacy. We believe that these issues stem, at least in part, from cyber security's reliance on stock photography. Stock photography is characteristically nondescript and visually homogeneous because it must make individual images salient to various use cases — hence the images of individuals in vague contexts and unclear narratives. Furthermore, stock photography in western media features a 'discrimination implied by a well-calculated, almost mandatory inclusion of gender and ethnic minorities' [288], yielding the nominally inclusive images that nonetheless fail to actually bestow agency to the individuals represented.

6.3.4 Digital-Physical spheres

Representing 7% of our total image-set, hybrid digital-physical representations, such as digital networks superimposed over cityscapes, the earth, or a more abstract sphere, were of some note to us. To understand what these images mean and how they may affect self-efficacy, we consulted work in other domains that use similar styles of visualisation. Most prominently, Sloterdijk, a German philosopher, studied the history of spherical maps, overlays, and designs, tracing these visual tactics as far back as the late 15th Century [340]. Sloterdijk argues that these kinds of images arose naturally from our changing understanding of our planet at that time, which was no longer an enclosed space or the centre of the universe, but a single, contingent celestial body. According to this account, disoriented European map

[7] Hands are often used to model movements or convey information by assuming specific positions.

makers began to fetishise spherical imagery as a sense-making device capable of conveying that we were no longer living inside a world, but rather *on* one.

Although the overlays in our image-set differ from these earlier precedents in that they overlay networked security graphs instead of shipping lanes, they may nonetheless embody a return to such 'spheric-security' in the face of new metaphysical uncertainties, at least from an aesthetic viewpoint [340]. Indeed, a subconscious spheric-security can also be seen in images outside our image-set like network traffic maps, which often take a spherical view despite not being technically constrained in this manner. According to Hall et al [147], spherical shapes suggest something which can be contained and kept secure, and so they may help to imaginatively 'bound' the sprawling endlessness of Network traffic, which always threatens to deviate into the unknown.

6.4 Trends and Recommendations

In the above, we explored the attributes of cyber security aesthetics and speculated about the kind of self-efficacy that these attributes afford. In the following, we highlight the trends we observed across classes and the key issues that cyber security aesthetics must address to improve its effect on users' self-efficacy.

A practical philosophy for cyber security

According to the philosophical discourse on aesthetics presented in Section 6.1, aesthetics provide a basis for savoring sensation, organising sensations into orderly meaning [188], and orienting contexts [199]. Moreover, the meanings and contexts thus constructed can influence our decisions [77]. While cyber security aesthetics seem to fulfil the first element of sensation, adapting a long history of mathematical and even science fiction aesthetics (alongside other disciplinary symbols) to frame cyberspace as an other-worldly future domain that is not restricted to what we currently understand, they fail to provide sufficient context for effective navigation or learning.

Instead, they present a dazzling spectacle of abstractions and powerful traditional security semiotics without much in the way of meaning. The hackerman archetype,

powerful but elusive, and our other subjects involved in procedural and ambiguous work, encourage users to abdicate responsibility based on their own comparative lack of expertise and perceived powerlessness, while the digital-physical spheres, like Sloterdijk's historical spheres, reify a world that may not match our experience of reality. According to Sloterdijk, humans no longer believe in an all-seeing singularity encompassing us, be it supernatural or human exceptionalism [340]. Nonetheless, much user-facing cyber security media depicts cyberspace as a fraught and hostile environment that individuals can't hope to navigate without expert assistance, a strategy that amounts to 'fear-mongering' and allows those with vested interests in the cyber security field to turn security into an all-important and all-encompassing issue [270].

Solving these problems is no simple task, and so no easy solution presents itself. One high-level, long-term suggestion is to develop a practical philosophy based on narratives. For example, McSweeney [256] frame security as a form of resilience that individuals can build through everyday tasks that make them feel secure. Where the person performing these tasks is a trusted friend or confidante, security could also be framed as *relational* security.

Improving role models for cyber security

Systemic under-representation in certain occupations is a complex and multi-causal problem that needs to be examined using both interdisciplinary and context-specific approaches.[8] Fortunately, we can begin to bolster all users' self-efficacy through much more straightforward steps.[9] For example, insofar as stereotypes can have positive self-efficacy effects in certain contexts [95],[10] we could co-opt the male-dominated hackerman stereotype and make it more inclusive, extending its connotations of moral ambiguity and power to individuals across demographics.

[8]These approaches must also account for under-representation at multiple phases / points in time, including factors that influence the admission, participation, and progression of under-represented individuals in these industries.

[9]In our case, self-efficacy is linked to the context in which these images are used for informally learnt cyber security.

[10]In the field of education, positive stereotypes have been shown to influence which goals individuals choose to pursue [95].

We believe that such role models can help to reduce users' cognitive load when assimilating cyber security knowledge, and that they can make the field as a whole seem more user-friendly.

The paradox of simplification

In the world of user interface design, developers build persuasive and easy-to-use interfaces to pursue a kind of universal simplicity. This objective could also be applied to cyber security aesthetics, where it could help to magnify users' self-efficacy. For instance, cyber security aesthetics could become simpler, cleaner, and more pertinent to the subject matter, or they could feature more rhetorical imagery. Where the digital workspaces, networked landscapes, text walls, and semiotic padlocks in our image-set all pose exploratory questions (prompting internal narrative reflection), rhetorical imagery makes a specific point, is designed with a specific audience in mind, and is focused on narrative integrity above all.

Of course, the problem is not just about exploratory imagery; we have seen that cyber security aesthetics feature many abstractions and visual devices that confuse the core concept being depicted. If cyber security aesthetics are supposed to simplify the complex nature of cyber security, it appears that we must first simplify the aesthetics themselves. However, simplification can itself lead to misunderstanding, as was the case in the Space Shuttle disaster, which was partially attributable to the oversimplification of data in a graph [364]. This is the cyber security aesthetic paradox: that simplification can aid as well as hinder understanding in equal measure. To overcome this challenge, we might look to other fields that have developed unique aesthetic norms that enhance learners' self-efficacy. The field of chemistry, for instance, has spent centuries developing a standard aesthetic system that simplifies complex concepts and narratives without rendering them ineffective [166].

6.5 Summary

In this chapter we have presented work on an image-set of cyber security illustrations and imagery generated from mainstream news articles as might be faced by individual

users on a regular basis. The work was oriented by two aims: (1) to ascertain what cyber security aesthetics consist of, from the perspective of an individual user, and (2) to provide an explorative discussion as to the manner in which these aesthetics may affect users' perceived self-efficacy as they informally learn cyber security precepts.

Our findings for (1) indicate that cyber security aesthetics depict a threatening and confusing environment with systemic semiotic and social deficiencies — a distorted vision of cyberspace without clarity of thought. The narrative of cyber security is abstract and opaque, but through informal learning, individual users can assemble a mental representation of this concept, using their senses to intuit meaning and perspective from the visual elements that accompany cyber security texts.

For (2) our findings raise important obstacles to self-efficacy potential, from the way that participants of cyberspace are portrayed to the moral ambiguity that characterises a significant proportion of the image-set. Nonetheless, as cyber security continues to evolve into a core concept within cyberspace, we believe that these issues can be overcome. Indeed, several of these problems, and the simplification paradox itself, arise from a lack of vision on the part of cyber security content creators, an obstacle that could be addressed through greater standardisation. Having covered this major phenomenological aspect of cyberspace we turn our attention to the final next chapter, in which we will endeavour to bring together the contributions into a coherent set of qualitative reflections.

7
Reflections and conclusions

This dissertation began with an outline of the challenges within understanding the users of cyberspace and their perceived apathy towards cyber security. To aid our research we framed it in terms of a high-level research question: *How might we help users overcome the challenges faced when attempting to stay secure in cyberspace?* This broad and expansive question demanded a layered approach, starting with an investigation of the environmental level in Chapter 4, which yielded results that led to two further contributions, discussed in Chapters 5 and 6. Each successive chapter narrowed the scope of the question further. In the grand context of cyberspace, we see these contributions as covering the environmental, epistemological and phenomenological levels of cyberspace and cyber security, which is visualised in Figure 7.1. What the figure highlights is that what was covered at each level represented a mere fraction of what could be explored in the quest to improve the user's experience of staying secure in cyberspace. We have presented the etymology of three applications of pre-existing methods that allow us to derive insight from the stochastic entity that is cyberspace. These methods are embryonic, but hopefully represent a sufficient set of first steps. The potential benefits, limitations and future directions of the overall work are discussed on a chapter-by-chapter basis in the following. Section 7.4 provides concluding remarks.

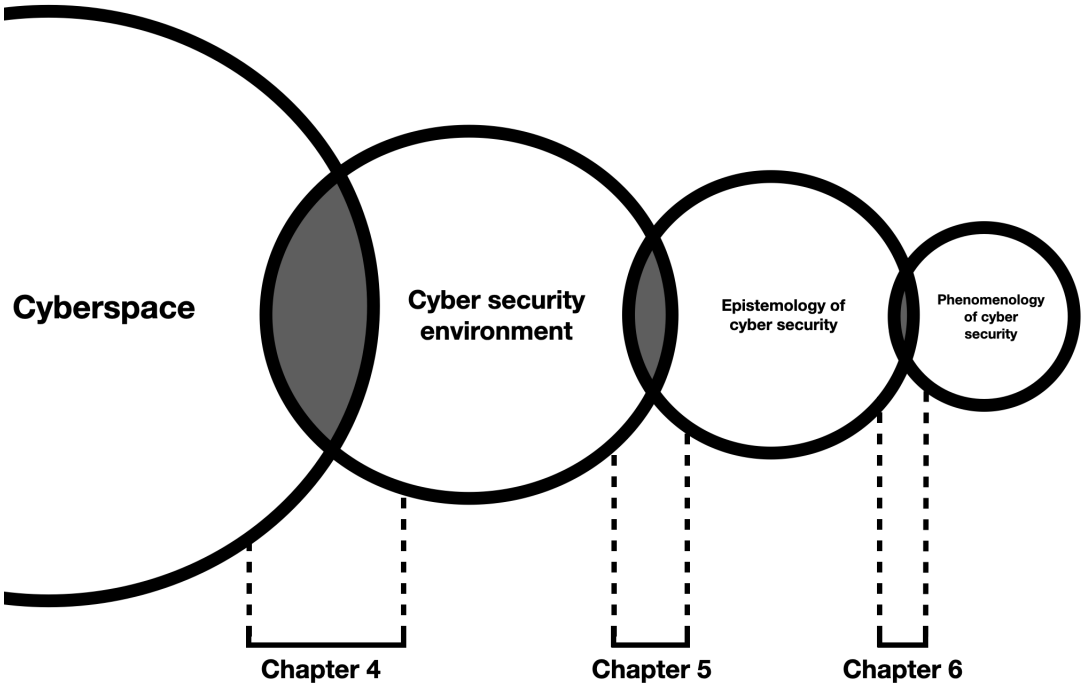


Figure 7.1: The way in which the research progressed.

7.1 Chapter 4: On the blending of metaphors as a basis for cyberspace exploration

Chapter 4 covered research question RQ1: *Given that users have complex motivation and decision-making patterns when interacting with cyberspace, can we establish a more contextually appropriate environment in which security decisions are made by users?*. To do so, we applied a four-spaces blended theory model to create our techno-spatial 'framework' of cyberspace as an environment, adapting the method slightly to allow for a hierarchical arrangement of our actors. This allowed us to distinguish between deliberative and autonomous actors and to begin accounting for differential agency and influence in cyberspace, even if only at the metaphorical level.

However, at present, we have only a vague statement of the physical constraints that are placed upon various actors within the cyberspace system, and we have only a vague idea of actors' roles within this system. And although these models can also extend to encompass the risk behaviours of the user-actor in cyberspace, allowing for risk within an optimal-control-based framework would at best offer a framework that covers worst-case and expectation-based risk formulations. Even

with more information, there is considerable doubt that we would succeed in fully integrating the system due to its extreme complexity and likelihood to exceed our initial expectations [33, 294].

7.1.1 Reflections on the experiment

We are not unique in highlighting the importance of the agent-based model to the idea of enhancing usable security research, with positional papers dating back at least as far as 2014 [208]. In Chapter 4 we were able to employ a 'bottom up' structural style through the usage of metaphors to symbolise the environment. What the experiment allowed us to attempt was to cut out motivational aspects of user-behaviour, and model the decisions made based on this environment. However we believe that it went further, as future development would potentially allow for the undertaker of said experiment to model a hypothetical user's subjective orientation to cyberspace, and then to non-subjectively test the rationality of this model in the face of real threats. Crucially, this applies to both sides of the spectrum; in our case we tested a model against the realities of cyberspace, whereas in closed system experiments the use of metaphor extends to the design of the *environment* in which agent's are placed. Within this environment, we believe the experiment agent's behaviour underscores their risk appetites for basic interaction with cyberspace. We believe the choices highlight the agent's beliefs and cognitive burden when undertaking these basic interactions. In this sense, we believe the experiment aided in exploring what happens after a decision is made, which itself feeds back into the contextual aspect laid out in **RQ1**.

7.1.2 The limitations of metaphor

Not every metaphor is as successful as the biological/virtual virus. Because metaphors create associations between concepts, rather than embodying any concept or meaning in and of themselves, they sacrifice accuracy and truth in order to facilitate discourse [223]. Thus, while high-level themes (such as the 'transmission of infection') provide useful behavioural metaphors, the effectiveness of this comparison

between the technological and biological tends to diminish when examining highly specific traits [225].

For example, a cautionary tale expounding these limits of metaphor blending effectiveness between fields can be found within the input spaces of computer science and the cognitive sciences, where metaphor blending takes place with computer science as the primary input space. For example, Unsworth and Engle [367] used the term primary and secondary memory in order to aid with their investigation into individual differences in working memory. In computer science, primary memory refers primarily to temporary and quickly accessible data that is often directly linked to the processing unit. Secondary memory what we might commonly refer to as storage, and not directly accessible by the processor. Secondary memory is not volatile and is not lost when the system is powered down. Unsworth and Engle instead ascribe primary memory as an active but very limited workspace where new input replaces old information, and secondary memory as a long-term directly searchable storage facility. The similarity here is at the highest levels, and lacks the sufficient levels of metaphor blending that allows for the terms to take on new meaning without confusion [24][1]. Staying within the confines of the memory metaphor, the example of Baddeley's episodic buffer [23] additionally stands out. In Baddeley's metaphor, the buffer is taken to mean the linking of information to form new coherent memories that are visually ordered, however the term was taken from the buffer concept in computer science, where it relates to data being kept temporarily in service of of some input/output operation. Arguably, usage of surface-level metaphors has only increased in recent years given the Internet-of-Things, wherein terminology such as 'kill switch'[2] is often obscured, their original meanings and intent diminished through a loss of trust in the metaphor [282].

[1]For example, there is no mention made of processing access.

[2]Traditionally a circuit-breaker, now with both analogue and digital equivalents within the Internet-of-things [282].

7.1.3 Future directions

There is considerable scope for improvement of our testing methodology that would enable it to test the efficacy our model. Simon [337] introduced the theory by modelling constraints to the assumption that an individual perfect knowledge about the distributions of risk, supply, and benefits. Furthermore, an individual may have incomplete information regarding the alternative to the desired action. Kahneman and Tversky [185, 365] find that individuals make different decisions with the same facts when presented in a different way. Within information technology research, Acquisti and Grossklags [3] use this concept to explain the privacy paradox. While bounded rationality[3] may provide some explanation for why security advice is ignored or the reason for why individuals participate in risky activities overall, there is also the reality that individuals enjoy risky activities [45].

Optimal control theory describes the process for determining the level and trajectory of control in a dynamic system over a period of time. We could apply this to our framework of cyberspace, for example in connection with the two models of cyberspace (complexity/control and prevalence/complexity). It may be feasible to develop an optimal control model of cyberspace that synthesises these relationships into a complete, dynamic system. Within this system, cyberspace would embody the continuous state-space, while micro- and macro-level actors and their associated processes would constitute the variables within the state-space. In this manner, and provided sufficient information, we could temporally and mathematically model cyberspace and thereby manage or assess the risk of cyberspace actors and/or their activities.

To do this, we would first have to model smaller elements of cyberspace, something that several projects have already done with various actors. For example, Bradley and Atkins [50] developed a continuous state-space model of cyber-physical systems (CPSs),[4] and Zhu et al [397] did the same for rumour propagation within

[3]The concept of *bounded rationality*, refers to where an individual is thought to make rational decisions about actions in order to maximise benefit [337].

[4]We have imagined cyberspace as a techno-spatial domain. It may also be conceived of as the ultimate CPS, as research in the CPS area concerns itself with the integration of physics-based and computational models into a discrete paradigm.

social media. Optimal control has precedent in the wider cyber-security sphere also; for example, Saurabh et al [14] looked at security-constrained optimal control over discrete time periods. In particular, they considered Denial-of-Service attack models and attempted to find a solution that minimised the objective function of the problem.

In this sense, our metaphorical approach can work in tandem with imperfect/incomplete optimal control models to supplement these deficiencies. This holds promise for a functional (if informal) integration between the blended theory domains, especially given the fact that our model was coherent enough to accord with our risk hypothesis and with the results of Seib et al's epidemiological study [329]. Additionally, optimal control elements could compensate for the deficiencies in our metaphorical approach.

Given these considerations, metaphorical models can help to imaginatively fill in gaps in optimal control models, and optimal control models can help to substantiate and operationalise metaphorical models, achieving a genuine 'simulation' for risk *prediction*, rather than retroactive risk *conceptualisation*. In the present chapter, our conceptual model was more a theoretical and interpretative lens that helped us to configure the user actor and make sense of the experiment's results. Future refinement and integration of our model may make it possible to identify actors' capabilities and vulnerabilities that have thus far gone unaddressed.

7.1.4 Improving security advice through agent-based simulation

Like cyberspace itself, user behaviour can be thought of as stochastic, as we can derive statistics after the fact but neither are easily measured *in situ*. Certainly a user study, which in many prior cases assumed deterministic elements and discrete advice to combat deterministic situations, can be enhanced through the use of this method, perhaps in conjunction with further user behaviour testing. The impracticability of testing solutions to security problems on the users has been shown by studies mentioned in Chapter 1, and we contend that agent-based simulations such as the

one shown in Chapter 4 may serve as a test-bed for solutions such as security advice, where discrete advice is tested in the innately risk-carrying stochastic cyberspace before taught to users. If implemented alongside high-quality risk metrics, it could serve to alter the fundamental balance of burden between users and security experts, we reduce the flood of new advice to only what is necessary. That is not to say we remove the user from security processes or limit their agency even further, but rather recognise the importance of the user in the successful execution of security processes, as per the advice of Kerckhoffs in 1882. Kerckhoffs' succinct point, which still holds true today, that "the system must be easy to use and must neither require stress of mind nor the knowledge of a long set of rules" [196].

However, we are not suggesting that agent-based modeling is some solution of all solutions that can be used to address any security issue relating to usable security. It has clear limits. Instead of trying to predict *how* a user is going to react to security stimuli such as security advice, instead the benefit is derived from the limited reprieve of the "other-minds problem" we referred to in Chapter 1.

7.2 Chapter 5: Gauging the difficulty of learning security advice

Learning about security advice, as discussed in Chapter 2, is accomplished through many different means. One such means is informal learning, and this is what was used to develop part of the experiment seen in Chapter 4 (specifically, Section 4.5). It directly led us to consider the question *Considering that the dissemination of security advice about cyberspace takes place through multitude of vectors, is it possible to measure the efficacy potential of such advice through one such dissemination vector?* In short, we believe the results highlight that not only can we reasonably assume to be able to assess the self-efficacy potential of an individual user when security advice is disseminated, the results highlight the difficulties and barriers currently in effect around easy security advice dissemination. This in effect then compounds further the problem that Chapter 4 aimed to reduce: if we cannot reduce the amount of security advice, then we need to ensure what advice is created is at

least easy to read and understand. Therefore, despite the narrowing of the scope, we believe the clear benefit in this research derives from the fact that tools are in place to allow for the testing of this advice, perhaps even before the dissemination stage. A reasonably simple reflection, then, but perhaps more implementable than what we were able to deduce at the environmental level.

7.2.1 The limits of assessing news-mediated cyber security advice

The scope of what we were able to accomplish in our pursuit of **RQ2** in Chapter 5 was limited by the type and amount of information we were able to acquire to build the corpus. In our case, this meant focusing on English-language material, even though a preliminary search conducted before implementation unearthed a rich catalogue of data in other languages. This also means that our security topics, analysis, and findings likely exhibit Anglo-Saxon bias. The technical tools utilised for the readability scores were also designed for English-language articles. There is significant scope for the enhancement of our search methodology, where for example users may only utilise the first page of any search enquiry [164]. It is our hope that this methodology be utilised to answer the same research objectives in other languages and cultural contexts. Finally, although the CIS ontology proved adequate for the scope of this project, the primary focus of CIS is technologists. Although our search for a suitable ontology was non-exhaustive, we believe the inclusion of CIS serves to highlight the need for further development in user-focused cyber security ontologies which may serve as a better basis upon which to base work such as ours. One additional issue with third party ontologies to consider is the fact that they require updating. As our chosen ontology receives updates at reasonable intervals, version control becomes necessary in order for this method to remain effective at cataloguing the content of advice contained within the news articles.

We utilised automated methodologies in order to classify topics and measure sentiment and reading difficulty, and the results are tempered by the respective limitations of these methodologies. Moreover, our results represent a specific

snapshot in the security timeline; access to a larger historical data-set would inevitably change the overall results, potentially yielding a more statistically significant sentiment analysis.

Our approach to tackling the second research objective (*to explore ways of determining the efficacy potential of news-mediated security advice through quantitative means*) may limit the usefulness of our conclusions. We approximated article efficacy potential by using text analysis to predict user engagement, and we did not consider other metrics that could have enhanced the findings. Traditionally speaking, reading-difficulty assessments in laboratory settings involve comprehension tests, eye tracking, and brain-imaging. Knowledge of how users interact with our corpus in these terms would allow for a significantly richer analysis of security advice efficacy potential.

7.2.2 Future directions

The aforementioned limitations can, of course, be addressed in future research that builds upon what is presented here — not least because our research method (described in Section 3.2) allows for continuous data capture. Furthermore, the data within this corpus could serve as the foundation for further analysis of security advice dissemination. Because this corpus contains a significant variety of sources, structural analysis of sentence construction for threat messaging could reveal the rhetorical structure of fear appeals, as per previous work in the field such as that of Renaud and Dupuis [310]. A fear appeal is designed to motivate the reader to execute security advice, and an in-depth analysis of its features could yield results that would improve the efficacy potential of security advice dissemination.

The corpus itself could be augmented with social media data, which would add the significant vector of digital naïve advice [328]. Bias within the articles could be used as another indicator of efficacy potential via methods like that presented by Lim et al [230]. We believe that the results of this contribution can provide a basis for further reflection on security advice dissemination, and that it can stimulate a conversation about individual users' learning environment.

Sentiment analysis

7.3 Chapter 6: On the benefits of cyber security aesthetics

The metadata captured during the data-gathering phase of the news-scraper allowed us to consider **RQ3**: *What do cyber security aesthetics look like to an individual user, and what are their efficacy potential?* We aimed to answer it in two parts: *What* are the aesthetics, and *why* are these important to usable-security researchers? On the first part, without going into detail on the exact aesthetics of cyber security here, we believe the analysis of the image-set provides a further burden on the consumer of security advice. From the preceding chapters we have awareness of the amount of information they receive, we know how difficult this information may be to read, and, with this chapter, we derive some understanding as to how the phenomenological (in our case, aesthetic) accompaniments to this advice may aid, or hinder this advice. The second part of the question is no less important. Why are these findings important? Beyond the surface-level findings, we believe that there is benefit to continuing the line of inquiry established by the chapter. In Kemp et al's work on cyber visualisations [147], the authors looked primarily at data visualisations and how these had efficacy potential (although they did not label it as such). We consider this to be part of the epistemological aspect of cyber security, as the visualisations provide meaningful data that the viewer is meant to interpret. Instead, this research looks to provide meaning to what can be interpreted by the layman, at best, as random colour and shape, and, at worst, a confusing reality of cyberspace that is best avoided. The primary opportunity is to utilise this line of questioning, which would allow researchers the ability to tailor the phenomenological aspects of cyber security, already difficult in the environmental and epistemological level, towards a set of semiotics that allow the user greater insight.

7.3.1 Cyber-security Aesthetics: A lack of suitable analysis methods?

The contributions within Chapter 6 were limited by the definitions we used and the inclusion / exclusion criteria we applied to guide our assembly of the image-set. Many of these were similar to what we encountered during the work in Chapter 5. We were required to restrain focus on English-language material, despite preliminary searches showcasing a rich catalogue of images in other languages. This also means that our analysis and our findings likely exhibit a western bias. Nevertheless, we expect that our methodology can be adapted to explore the same research questions in other languages and cultural contexts, enabling a more universal understanding of cyber security aesthetics.

Similarly, given the background we provided in Section 2.6.2, our definition of aesthetics likely exhibits a western bias, failing to encapsulate the aesthetic philosophies of other cultures. It may also be limiting for other reasons, as we focused narrowly on their ability to provide context for, and inlays to, the world of cyberspace, making it more interpretable and navigable for informal learners. Other definitions might yield different insights and support other kinds of research questions.

We utilised semi-automated methodologies to classify images based on the semiotic objects within them, and the results are tempered by the respective limitations of these methodologies. Moreover, our results represent a specific snapshot in the security timeline; access to a larger historical image-set would inevitably change the overall results, potentially yielding a more statistically significant sentiment analysis. Furthermore, in order to assemble a unique image-set, we ignored duplicates. However, insofar as aesthetic literacies arise from *exposure* to images, rather than the absolute number of unique images, including duplicates could help us to ascertain the effective rate of gender representation, as perceived by viewers.

Lastly, we did not consider other metrics that could have enhanced the findings, and we did not engage in other kinds of data collection (like surveys) that could have revealed real users' reactions. Traditionally speaking, image recognition

assessments in lab settings involve comprehension tests, eye tracking, and brain-imaging. Knowledge of how users interact with cyber security aesthetics in these terms would allow for a significantly richer analysis of aesthetic effects on self-efficacy.

All of these limitations present myriad opportunities to expand on this work, perfecting our understanding of cyber security aesthetics and the effects it can have on cyberspace and its users.

7.3.2 Future directions

Because self-efficacy is a fluid construct that may vary based on specific emotional awareness and specific tasks or contexts [190], future research in this field could assess the emotional associations of more granular aesthetic elements, like each colour within each image class. For example, [265] crowd-sourced an inventory of colour-word associations that reveal the specific emotions attached to specific colours, which could be used to analyse the colour trends in our image-set, and complement existing work. This could lead to an extension of the work, as although currently the image-set is classified and analyzed according to shapes and colour (Figure 6.3 provides a good example of this), no such analysis has taken place. In this case, sentiment analysis represents a suitable immediate next step. As image sentiment analysis involves automatically detecting the emotional content or sentiment depicted within images, the immediate goal would be to classify images as conveying positive, negative, or neutral sentiment based on their visual content, not unlike what was completed for Section 5.2.5 for the news-corpus. Considering the labels we already possess for each image within the image-set, using a method involving a pre-trained model on our current image-set could serve as an extension of what we saw in Chapter 6. Alternatively, another approach that would yield potentially richer results would be to first conduct qualitative analysis of human aesthetic judgements on our image-set, compiling profiles of aesthetic reactions associated with positive, negative, and neutral sentiment classifications [192]. Interviews would provide deeper insight into individuals' thought processes and contextual interpretations informing their subjective aesthetic evaluations of

cyber security images [283, 74]. This knowledge could then enrich future image sentiment models with more nuanced, cyber security specific capabilities when automatically judging the sentiments expressed in new visual data, and allow for future use by other researchers in the cyber security field.

7.4 Final thoughts

Becoming self-efficacious in any complex task has many potential difficulties, and cyber security is no exception. This dissertation was driven by research findings in prior work that highlighted these self-efficacy challenges associated with users, which in turn motivated the question of *how we might help users overcome the challenges faced when attempting to stay secure in cyberspace*. What we have discovered is that users face challenges on multiple levels of cognition, which are not especially restricted to what we originally thought may have been a purely discrete education problem. Instead, we believe this research merely scratched the surface of what is possible to learn about user behaviour in cyberspace, and so much more could be done before our research question could get the answer it deserved. In particular we believe that in the area of agent-based modelling, better methodologies could eventually lead to the alleviation of the user needing to learn superfluous or counter-intuitive advice, and in the area of cyber-security aesthetics, a larger image-set could lead to novel ways of learning not imagined in this dissertation today. As we continue to develop cyberspace as a fully human-derived and developed domain, we hope it develops into a vision more inherently associative and holistic (while also centering human experience).

Bibliography

[1] Abomhara, M., and Køien, G. M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility 4*, 1 (January 2015), 65–88.

[2] Abrams, M. H., and Harpham, G. *A glossary of literary terms*. Nelson Education, 2014.

[3] Acquisti, A., and Grossklags, J. Privacy and rationality in individual decision making. *IEEE Security Privacy 3*, 1 (Jan 2005), 26–33.

[4] Adams, A., and Sasse, M. A. Users are not the enemy. *Commun. ACM 42*, 12 (Dec. 1999), 40–46.

[5] Agrawal, A., Fantham, D., Ghosh, D., Kelley, D., Florio, E., Avena, E., Douglas, E., Tan Seng, F., Trull, J., Borenstein, J., Selvaraj, K., Kaplinska, K., Laidler, K., Duncan, M., Simos, M., Henry, P., Pandey, P., Pliskin, R., McGee, R., Kathuria, S., Wacker, S., Ganacharya, T., Grebennikov, V., and Zohar, Y. Microsoft security intelligence report. 173–190.

[6] Ajzen, I. From intentions to actions: A theory of planned behavior. In *Action control*. Springer, 1985, pp. 11–39.

[7] Ajzen, I. The theory of planned behaviour. organizational behaviour and human decision processes, 50 (2), 179-211. *View at* (1991).

[8] Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., and Abdulkareem, K. H. Cyber-security incidents: a review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications 9*, 1 (2018), 499–508.

[9] Alagheband, M. R., Mashatan, A., and Zihayat, M. Time-based gap analysis of cybersecurity trends in academic and digital media. *ACM Transactions on Management Information Systems (TMIS) 11*, 4 (2020), 1–20.

[10] Alexa. The cis ontological framework for cyber security. `https://learn.cisecurity.org/cis-controls-download`, March 2021.

[11] Alexa. The top 500 sites on the web. `https://www.alexa.com/topsites`, March 2021.

[12] Almog, J. *What am I?: Descartes and the mind-body problem*. Oxford University Press on Demand, 2005.

[13] Alsudani, F., and Casey, M. The effect of aesthetics on web credibility. *People and Computers XXIII Celebrating People and Technology* (2009), 512–519.

[14] Amin, S., Cárdenas, A. A., and Sastry, S. S. Safe and secure networked control systems under denial-of-service attacks. In *International Workshop on Hybrid Systems: Computation and Control* (2009), Springer, pp. 31–45.

[15] Anderson, K. H., Foster, J. E., and Frisvold, D. E. Investing in health: The long-term impact of head start on smoking. *Economic Inquiry 48*, 3 (2010), 587–602.

[16] Apvrille, A., and Strazzere, T. Reducing the window of opportunity for android malware gotta catch'em all. *Journal in Computer Virology 8*, 1-2 (2012), 61–71.

[17] Araujo, T., Wonneberger, A., Neijens, P., and de Vreese, C. How much time do you spend online? understanding and improving the accuracy of self-reported measures of internet use. *Communication Methods and Measures 11*, 3 (2017), 173–190.

[18] Aristotle. *Rhetoric and On poetics*. Franklin Library, 1981.

[19] Arora, P. *The next billion users: Digital life beyond the West*. Harvard University Press, 2019.

[20] Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J., and Weyl, E. G. Should we treat data as labor? moving beyond "free". In *AEA Papers and Proceedings* (May 2018), vol. 108, pp. 38–42.

[21] Aung, M. N., Koyanagi, Y., Nagamine, Y., Nam, E. W., Mulati, N., Kyaw, M. Y., Moolphate, S., Shirayama, Y., Nonaka, K., Field, M., et al. Digitally inclusive, healthy aging communities (dihac): A cross-cultural study in japan, republic of korea, singapore, and thailand. *International Journal of Environmental Research and Public Health 19*, 12 (2022), 6976.

[22] Bada, M., Sasse, A. M., and Nurse, J. R. C. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[23] Baddeley, A. The episodic buffer: a new component of working memory? *Trends in Cognitive Sciences 4*, 11 (2000), 417–423.

[24] Bahr, G. S., Bell, M. G., Metz, J., Sowle, S., and Beasley, E. A modern integration of cognitive and computer sciences. In *International Conference on Universal Access in Human-Computer Interaction* (2009), Springer, pp. 441–449.

[25] Bandura, A., Freeman, W. H., and Lightsey, R. Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy 13*, 2 (1999), 158–166.

[26] Barbosa, S. D. J., Barbosa, G. D. J., Souza, C. S. d., and Leitão, C. F. A semiotics-based epistemic tool to reason about ethical issues in digital technology design and development. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (2021), pp. 363–374.

[27] Barlow, J. P. A declaration of the independence of cyberspace. Electronic Frontier Foundation, 1996.

[28] Barnes, S. B. A privacy paradox: Social networking in the United States. *First Monday 11*, 9 (2006).

[29] Basalla, G. *The evolution of technology*. Cambridge University Press, 1988.

[30] Beardsley, M. C. *Aesthetics from classical Greece to the present*, vol. 13. University of Alabama Press, 1975.

[31] Beasley, R., and Danesi, M. *Persuasive signs: The semiotics of advertising*, vol. 4. Walter de Gruyter, 2010.

[32] Belk, R. Extended self and the digital world. *Current Opinion in Psychology 10* (2016), 50–54.

[33] Benedikt, M. L. *Cyberspace: First steps*. MIT Press, 1991.

[34] Benyon, D. Presence in blended spaces. *Interacting with Computers 24*, 4 (2012), 219–226.

[35] Bergmans, A. Meaningful communication among experts and affected citizens on risk: challenge or impossibility? *Journal of risk research 11*, 1-2 (2008), 175–193.

[36] Bernal, V. 1. the aesthetics of cyber insecurity: Displaying the digital in three american museum exhibits. In *Futureproof*. Duke University Press, 2020, pp. 33–62.

[37] Bertino, E., and Islam, N. Botnets and internet of things security. *Computer 50*, 2 (2017), 76–79.

[38] Betz, D. J., and Stevens, T. Analogical reasoning and cyber security. *Security Dialogue 44*, 2 (2013), 147–164.

[39] Bishop, M., and Gates, C. Defining the insider threat. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead* (2008), pp. 1–3.

[40] Black, D., Bissessar, C., and Boolaky, M. Online education as an opportunity equalizer: The changing canvas of online education. *Interchange 50*, 3 (2019), 423–443.

[41] Blei, D. M., Ng, A. Y., and Jordan, M. I. Latent dirichlet allocation. *Journal of machine Learning research 3*, Jan (2003), 993–1022.

[42] Blythe, J. M., Coventry, L., and Little, L. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. pp. 103–122.

[43] Boden, M. Artificial intelligence and natural man. *Synthese 43*, 3 (1980), 433–451.

[44] Bonaccio, S., and Dalal, R. S. Advice taking and decision-making: An integrative literature review, and implications for the organizational sciences. *Organizational Behavior and Human Decision Processes 101*, 2 (2006), 127–151.

[45] Borsky, S., and Raschky, P. A. The hedonics of hedonism–estimating the value of risk-taking activities. *Kyklos 62*, 2 (2009), 210–225.

[46] Bortolotti, L. The epistemic innocence of motivated delusions. *Consciousness and cognition 33* (2015), 490–499.

[47] Bosma, N., Hessels, J., Schutjens, V., Van Praag, M., and Verheul, I. Entrepreneurship and role models. *Journal of economic psychology 33*, 2 (2012), 410–424.

[48] Bou, F., Schorlemmer, M., Corneli, J., Gómez-Ramírez, D., Maclean, E., Smaill, A., and Pease, A. The role of blending in mathematical invention. In *Proceedings of the Sixth International Conference on Computational Creativity June* (2015), Citeseer, p. 55.

[49] Boyd-Barrett, O. Cyberspace, globalization and empire. *Global Media and Communication 2*, 1 (2006), 21–41.

[50] Bradley, J. M., and Atkins, E. M. Toward continuous state–space regulation of coupled cyber–physical systems. *Proceedings of the IEEE 100*, 1 (2011), 60–74.

[51] Branch, J. What's in a name? Metaphors and cybersecurity. *International Organization 75*, 1 (2021), 39–70.

[52] Brandimarte, L., Acquisti, A., and Loewenstein, G. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science 4*, 3 (2013), 340–347.

[53] Britt, R. K., Collins, W. B., Wilson, K., Linnemeier, G., and Englebert, A. M. ehealth literacy and health behaviors affecting modern college students: A pilot study of issues identified by the american college health association. *Journal of Medical Internet Research 19*, 12 (2017), e392.

[54] Broersma, M. J. *Form and Style in Journalism. European Newspapers and the representation of News 1880-2005.* Peeters, 2007.

[55] Brown, J., Zhou, Z. Q., and Chow, Y.-W. Metamorphic testing of navigation software: A pilot study with google maps. In *51st Annual Hawaii International Conference on System Sciences (HICSS-51)* (Waikoloa Village, HI, Jan. 2018).

[56] Bruschi, D., Martignoni, L., and Monga, M. Code normalization for self-mutating malware. *IEEE Security & Privacy Magazine 5*, 2 (2007), 46–54.

[57] Buchholz, R. A., and Rosenthal, S. B. Integrating ethics all the way through: The issue of moral agency reconsidered. *Journal of Business Ethics 66*, 2 (2006), 233–239.

[58] Bull, G., Thompson, A., Searson, M., Garofalo, J., Park, J., Young, C., and Lee, J. Connecting informal and formal learning experiences in the age of participatory media. *Contemporary Issues in Technology and Teacher Education 8*, 2 (2008), 100–107.

[59] Burns, A., McDermid, J., and Dobson, J. On the meaning of safety and security. *The computer journal 35*, 1 (1992), 3–15.

[60] Busse, K., Schäfer, J., and Smith, M. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (Santa Clara, CA, Aug. 2019), USENIX Association.

[61] Byrd, T. A., Cossick, K. L., and Zmud, R. W. A synthesis of research on requirements analysis and knowledge acquisition techniques. *MIS quarterly* (1992), 117–138.

[62] Byrne, Z., Weidert, J., Liff, J., Horvath, M., Smith, C., Howe, A., and Ray, I. Perceptions of internet threats: Behavioral intent to click again. In *Proceedings of the 27th Annual Conference of the Society for Industrial and Organizational Psychology* (2012), pp. 26–28.

[63] Caballero, A. Security education, training, and awareness. In *Computer and information security handbook*. Elsevier, 2017, pp. 497–505.

[64] Cabeza Pereiro, J., and Rodríguez Rodríguez, E. Is the employer entitled to survey employee's internet communications in the workplace? case of "barbulescu v. romania". In *Media and Metamedia Management* (2017), Springer, pp. 87–93.

[65] Cains, M. G., Flora, L., Taber, D., King, Z., and Henshel, D. S. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis 42*, 8 (2022), 1643–1669.

[66] Caldwell, T. Plugging the cyber-security skills gap. *Computer Fraud & Security 2013*, 7 (2013), 5–10.

[67] Cao, J., Xia, T., Li, J., Zhang, Y., and Tang, S. A density-based method for adaptive lda model selection. *Neurocomputing 72*, 7–9 (2009), 1775–1781.

[68] Carper, B. A. Fundamental patterns of knowing in nursing. *Advances in Nursing Science 1*, 1 (1978), 13–24.

[69] Carroll, F. Designing (for) experiences in photorealistic vr environments. *New Review of Hypermedia and Multimedia 16*, 1-2 (2010), 181–194.

[70] Carroll, F. Usable security and aesthetics: Designing for engaging online security warnings and cautions to optimise user security whilst affording ease of use. In *European Symposium on Usable Security 2021* (2021), pp. 23–28.

[71] Casas, P., Soro, F., Vanerio, J., Settanni, G., and D'Alconzo, A. Network security and anomaly detection with big-dama, a big data analytics framework. In *2017 IEEE 6th International Conference on Cloud Networking (CloudNet)* (Prague, Czech Republic, Sep. 2017), IEEE, pp. 1–7.

[72] Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. The economic impact of cyber-attacks. *Congressional Research Service Documents, CRS RL32331 (Washington, DC)* (2004), 2.

[73] Çelen, B., Kariv, S., and Schotter, A. An experimental test of advice and social learning. *Management Science 56*, 10 (2010), 1687–1701.

[74] Cetinic, E., Lipic, T., and Grgic, S. A deep learning perspective on beauty, sentiment, and remembrance of art. *IEEE Access 7* (2019), 73694–73710.

[75] Chang, Y.-n., Lim, Y.-k., and Stolterman, E. Personas: from theory to practices. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges* (2008), pp. 439–442.

[76] Charney, S. Collective defense: Applying public health models to the internet. *IEEE Security & Privacy 10*, 2 (2011), 54–59.

[77] Chatterjee, A. *The aesthetic brain: How we evolved to desire beauty and enjoy art*. Oxford University Press, 2014.

[78] Chaudhuri, A. Sustaining cooperation in laboratory public goods experiments: A selective survey of the literature. *Experimental Economics 14*, 1 (2011), 47–83.

[79] Chen, H., Chiang, R. H. L., and Storey, V. C. Business intelligence and analytics: From big data to big impact. *MIS Quarterly 36* (2012), 1165–1188.

[80] Chen, K., and Rea Jr, A. I. Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems 44*, 4 (2004), 85–92.

[81] Cheng, L., Pei, J., and Danesi, M. A sociosemiotic interpretation of cybersecurity in u.s. legislative discourse. *Social Semiotics 29*, 3 (2019), 286–302.

[82] Cleland, E. E. Trait divergence and the ecosystem impacts of invading species. *New Phytologist 189*, 3 (2011), 649–652.

[83] Cliff, O. M., Harding, N., Piraveenan, M., Erten, E. Y., Gambhir, M., and Prokopenko, M. Investigating spatiotemporal dynamics and synchrony of influenza epidemics in australia: an agent-based modelling approach. *Simulation Modelling Practice and Theory 87* (2018), 412–431.

[84] Coleman, M., and Liau, T. L. A computer readability formula designed for machine scoring. *Journal of Applied Psychology 60*, 2 (1975), 283–284.

[85] Contandriopoulos, D., Lemire, M., Denis, J.-L., and Tremblay, É. Knowledge exchange processes in organizations and policy arenas: a narrative systematic review of the literature. *The Milbank Quarterly 88*, 4 (2010), 444–483.

[86] Cook, T. E. *Governing with the news: The news media as a political institution*. University of Chicago Press, 1998.

[87] Coombs, W. T. The internet as potential equalizer: New leverage for confronting social irresponsibility. *Public Relations Review 24*, 3 (1998), 289–303.

[88] Cooper, N., and Holman, V. War and visual culture since 1900. *Journal of War & Culture Studies 1*, 3 (2008), 219–222.

[89] Coughlan, E., Mindel, A., and Estcourt, C. S. Male clients of female commercial sex workers: HIV, STDs and risk behaviour. *International Journal of STD & AIDS 12*, 10 (2001), 665–669. PMID: 11564334.

[90] Croon, A. Making sense of cyberspace: a question of being-with information technology. In *Exploring Cyber Society* (1999), Univeristy of Northumbria at Newcastle, pp. 1–9.

[91] Csurka, G., Dance, C., Fan, L., Willamowski, J., and Bray, C. Visual categorization with bags of keypoints. In *Workshop on statistical learning in computer vision, ECCV* (2004), vol. 1, Prague, pp. 1–2.

[92] Currie, J., Neidell, M., and Schmieder, J. F. Air pollution and infant health: Lessons from new jersey. *Journal of Health Economics 28*, 3 (2009), 688–703.

[93] Curtis, A. *Rhetoric of flat design and skeuomorphism in Apple's iOS graphical user interface*. University of Rhode Island, 2015.

[94] Cutrell, E., and Guan, Z. What are you looking for? an eye-tracking study of information usage in web search. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, CA, Apr. 2007), pp. 407–416.

[95] Czopp, A. M., Kay, A. C., and Cheryan, S. Positive stereotypes are pervasive and powerful. *Perspectives on Psychological Science 10*, 4 (2015), 451–463.

[96] Dack, C., McHugh, L., and Reed, P. Generalization of causal efficacy judgments after evaluative learning. *Learning & Behavior 37*, 4 (2009), 336–348.

[97] Das, S., Lo, J., Dabbish, L., and Hong, J. I. Breaking! a typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–12.

[98] David, A., and Glore, P. The impact of design and aesthetics on usability, credibility, and learning in an online environment. *Online Journal of Distance Learning Administration 13*, 4 (2010).

[99] Davidson, D. What metaphors mean. *Critical Inquiry 5*, 1 (1978), 31–47.

[100] Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., and Harshman, R. Indexing by latent semantic analysis. *Journal of the American Society for Information Science 41*, 6 (1990), 391–407.

[101] DeNardis, L. *The global war for internet governance*. Yale University Press, 2014.

[102] Dewey, J. Art as experience. new york: Wideview, 1934.

[103] Djamasbi, S., and Strong, D. User experience-driven innovation in smart and connected worlds. *AIS Transactions on Human-Computer Interaction 11*, 4 (2019), 215–231.

[104] Dorogovtsev, S. N., and Mendes, J. F. *Evolution of networks: From biological nets to the Internet and WWW*. OUP Oxford, 2013.

[105] Dreibelbis, R. C., Martin, J., Coovert, M. D., and Dorsey, D. W. The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industrial and Organizational Psychology 11*, 2 (2018), 346–365.

[106] Dulleck, U., and Kerschbamer, R. On doctors, mechanics, and computer specialists: The economics of credence goods. *Journal of Economic Literature 44*, 1 (2006), 5–42.

[107] Dunbar-Jacob, J., Schlenk, E., and McCall, M. 12 patient adherence to treatment regimen. *Handbook of Health Psychology* (2012), 271.

[108] Eiband, M., Völkel, S. T., Buschek, D., Cook, S., and Hussmann, H. When people and algorithms meet: User-reported problems in intelligent everyday applications. In *Proceedings of the 24th International Conference on Intelligent User Interfaces* (Marina del Ray, CA, Mar. 2019), pp. 96–106.

[109] Ensafi, R., Winter, P., Mueen, A., and Crandall, J. R. Analyzing the great firewall of China over space and time. *Proc. Priv. Enhancing Technol. 2015*, 1 (2015), 61–76.

[110] Eubank, S., Guclu, H., Anil Kumar, V., Marathe, M. V., Srinivasan, A., Toroczkai, Z., and Wang, N. Modelling disease outbreaks in realistic urban social networks. *Nature 429*, 6988 (2004), 180–184.

[111] Fan, W., and Yeung, K. Online social networks—paradise of computer viruses. *Physica A: Statistical Mechanics and its Applications 390*, 2 (2011), 189–197.

[112] Farhang, S., Weidman, J., Kamani, M. M., Grossklags, J., and Liu, P. Take it or leave it: A survey study on operating system upgrade practices. In *Proceedings of the 34th Annual Computer Security Applications Conference* (San Juan, PR, Dec. 2018), pp. 490–504.

[113] Farn, K.-J., Lin, S.-K., and Fung, A. R.-W. A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces 26*, 6 (2004), 501–513.

[114] Fauconnier, G., and Turner, M. *Mental spaces*. De Gruyter Mouton, 2008.

[115] Fauconnier, G., and Turner, M. B. Rethinking metaphor. In *Cambridge Handbook of Metaphor and Thought* (2008), R. Gibbs, Ed., New York: Cambridge University Press.

[116] Featherstone, M., and Burrows, R. *Cyberspace/cyberbodies/cyberpunk: Cultures of technological embodiment*. Sage, 1996.

[117] Feld, S. Sound structure as social structure. *Ethnomusicology 28*, 3 (1984), 383–409.

[118] Fernandes, M., Walls, L., Munson, S., Hullman, J., and Kay, M. Uncertainty displays using quantile dotplots or cdfs improve transit decision-making. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–12.

[119] Flavián, C., Gurrea, R., and Orús, C. A heuristic evaluation of websites design for achieving the web success. *International Journal of Services and Standards 5*, 1 (2009), 17–41.

[120] Flechais, I., Mascolo, C., and Sasse, M. A. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics 1*, 1 (2007), 12–26.

[121] Fleming, W. H., and Rishel, R. W. *Deterministic and stochastic optimal control*, vol. 1. Springer Science & Business Media, 2012.

[122] Fogg, B. J. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology* (2009), pp. 1–7.

[123] Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)* (2016), pp. 97–111.

[124] Foucault, M. *The Foucault effect: Studies in governmentality*. University of Chicago Press, 1991.

[125] Fransman, M. Innovation in the new ict ecosystem: How new knowledge is endogenously created in the ict sector. *Communications & Strategies 68* (4th Quarter 2007), 89.

[126] French, P. A. *Corporate Moral Agency*. John Wiley Sons, Ltd, 2015, pp. 1–3.

[127] Friston, K. The free-energy principle: a unified brain theory? *Nature Reviews Neuroscience 11*, 2 (2010), 127–138.

[128] Fulton, K. R., Gelles, R., McKay, A., Roberts, R., Abdi, Y., and Mazurek, M. L. The effect of entertainment media on mental models of computer security. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS)* (2019), pp. 79–95.

[129] Gadarian, S. K. The politics of threat: How terrorism news shapes foreign policy attitudes. *The Journal of Politics 72*, 2 (2010), 469–483.

[130] Gaines, B. *Machinic Eyes: New and Post-Digital Aesthetics, Surveillance, and Resistance*. PhD thesis, Clemson University, 2019.

[131] Garrick, J. Informal learning in corporate workplaces. *Human Resource Development Quarterly 9*, 2 (1998), 129–144.

[132] Gerber, M., and Von Solms, R. Management of risk in the information age. *Computers & Security 24*, 1 (2005), 16–30.

[133] Ghertner, D. A., McFann, H., and Goldstein, D. M. *Futureproof: Security aesthetics and the management of life*. Duke University Press, 2020.

[134] Gibbs Jr, R. W., and Steen, G. J. *Metaphor in cognitive linguistics: Selected papers from the 5th international cognitive linguistics conference, Amsterdam, 1997*, vol. 175. John Benjamins Publishing, 1999.

[135] Gibson, W. *Neuromancer*, vol. 1. Aleph, 1984.

[136] Glasser, T. L. The aesthetics of news. *ETC: A Review of General Semantics* (1980), 238–247.

[137] Goldin-Meadow, S., and Wagner, S. M. How our hands help us learn. *Trends in Cognitive Sciences 9*, 5 (2005), 234–241.

[138] Goldman, E. O., and Arquilla, J. Cyber analogies. Tech. Rep. NPS-DA-14-001, Naval Postgraduate School, Monterey, CA, 2014.

[139] Goldstein, J., Kantrowitz, M., Mittal, V., and Carbonell, J. Summarizing text documents: Sentence selection and evaluation metrics. In *Proceedings of the 22nd annual international ACM SIGIR conference on Research and development in information retrieval* (1999), pp. 121–128.

[140] Goodin, D. Big-name sites hit by rash of malicious ads spreading crypto ransomware. *Ars Technica* (16 Mar 2016).

[141] Greenspan, S. Future screens are mostly blue. *99*

[142] Grinberg, N. *Identifying modes of user engagement with online news and their relationship to information gain in text. In* Proceedings of the 2018 World Wide Web Conference *(2018), pp. 1745–1754.*

[143] Grosholz, J., and Kubrin, C. *Crime in the news: How crimes, offenders and victims are portrayed in the media.* Journal of Criminal Justice and Popular Culture 14 *(2007), 59–83.*

[144] Guan, Y., Li, C., Lu, H., and Wong, M. F. *Regulations and brain drain: Evidence from wall street star analysts' career choices.* Management Science 65*, 12 (2019), 5766–5784.*

[145] Gupta, A., Thakkar, K., Gandhi, V., and Narayanan, P. *Nose, eyes and ears: Head pose estimation by locating facial keypoints. In* ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) *(2019), IEEE, pp. 1977–1981.*

[146] Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., and Chen, J. *Cultural and psychological factors in cyber-security. In* Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services *(2016), pp. 318–324.*

[147] Hall, P., Heath, C., and Coles-Kemp, L. *Critical visualization: a case for rethinking how we visualize risk and security.* Journal of Cybersecurity 1*, 1 (Dec 2015), 93–108.*

[148] Hamilton, W. L., Clark, K., Leskovec, J., and Jurafsky, D. *Inducing domain-specific sentiment lexicons from unlabeled corpora. In* Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing *(2016), vol. 2016, NIH Public Access, pp. 595–605.*

[149] Hands, D. W. *Popper and lakatos in economic methodology'. In* Rationality, institutions and economic methodology*. Routledge, 1993, pp. 72–86.*

[150] Haney, J. M., and Lutters, W. G. *" it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In* Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) *(2018), pp. 411–425.*

[151] Harnad, S. *Minds, machines and turing. In* The Turing Test*. Springer, 2003, pp. 253–273.*

[152] Hasegawa, A. A., Yamashita, N., Mori, T., Inoue, D., and Akiyama, M. *Understanding {Non-Experts'} security-and {Privacy-Related} questions on a {Q&A} site. In* Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) *(2022), pp. 39–56.*

[153] Hassenzahl, M. The Thing and I: Understanding the Relationship Between User and Product*. Springer International Publishing, Cham, 2018, pp. 301–313.*

[154] Hattwig, D., Bussert, K., Medaille, A., and Burgess, J. *Visual literacy standards in higher education: New opportunities for libraries and student learning.* Portal: Libraries and the Academy 13*, 1 (2013), 61–89.*

[155] Hausman, D. M. The philosophy of economics: An anthology*. Cambridge University Press, 1994.*

[156] He, W. *A review of social media security risks and mitigation techniques.* Journal of Systems and Information Technology *(2012).*

[157] Heaps, H. S. Information retrieval, computational and theoretical aspects*. Academic Press, 1978.*

[158] Heidegger, M. The question concerning technology*. Garland Publishing Inc, New York, 1977.*

[159] Hemphill, T. A., and Longstreet, P. *Financial data breaches in the us retail economy: Restoring confidence in information technology security standards.* Technology in Society 44 *(2016), 30–38.*

[160] Herley, C. E. *So long, and no thanks for the externalities: The rational rejection of security advice by users. In* Proceedings of the 2009 Workshop on New Security Paradigms Workshop *(New York, NY, USA, 2009), NSPW '09, Association for Computing Machinery, pp. 133–144.*

[161] Herley, C. E., Keogh, B. W., Hulett, A. M., Marinescu, A. M., Williams, J. S., and Nurilov, S. *Us patent 9,021,590: Spyware detection mechanism, April "28" 2015.*

[162] Hight, S. D. *The importance of a security, education, training and awareness program, november 2005.* Security 27601 *(2005), 1–5.*

[163] Hina, S., and Dominic, D. D. *Information security policies: Investigation of compliance in universities. In* 2016 3rd International Conference on Computer and Information Sciences (ICCOINS) *(2016), IEEE, pp. 564–569.*

[164] Höchstötter, N., and Lewandowski, D. *What users see–structures in search engine results pages.* Information Sciences 179*, 12 (2009), 1796–1812.*

[165] Hoertel, N., Blachier, M., Blanco, C., Olfson, M., Massetti, M., Rico, M. S., Limosin, F., and Leleu, H. *A stochastic agent-based model of the sars-cov-2 epidemic in france.* Nature Medicine 26*, 9 (2020), 1417–1421.*

[166] Hoffmann, R. *Thoughts on aesthetics and visualization in chemistry.* HYLE–International Journal for Philosophy of Chemistry 9*, 1 (2003), 7–10.*

[167] Holden, J. The mathematics of secrets: cryptography from caesar ciphers to digital encryption. *Princeton University Press, 2018.*

[168] Howe, A. E., Ray, I., Roberts, M., Urbanska, M., and Byrne, Z. *The psychology of security for the home computer user. In* 2012 IEEE Symposium on Security and Privacy *(San Francisco, CA, May 2012), IEEE, pp. 209–223.*

[169] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., and Mahmood, S. *Cyber-security threats and vulnerabilities: a systematic mapping study.* Arabian Journal for Science and Engineering 45*, 4 (2020), 3171–3189.*

[170] Huppes, G. *Macro-environmental policy: principles and design.*

[171] Hussein, D. M. E.-D. M. *A survey on sentiment analysis challenges.* Journal of King Saud University - Engineering Sciences 30*, 4 (2018), 330–338.*

[172] Hyslop, A. Other minds*, vol. 246. Springer Science & Business Media, 2013.*

[173] Ion, C. G., et al. *Husserl, habermas, and the lifeworld as the overall horizon within which individuals act.* Linguistic and Philosophical Investigations*, 14 (2015), 115–120.*

[174] Ion, I., Reeder, R., and Consolvo, S. *"... no one can hack my mind": Comparing expert and non-expert security practices. In* Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) *(2015), pp. 327–346.*

[175] Jackson, M. *Thinking through the body: An essay on understanding metaphor.* Social Analysis: The International Journal of Social and Cultural Practice*, 14 (1983), 127–149.*

[176] Jain, P., Djamasbi, S., and Wyatt, J. *Creating value with proto-research persona development. In* International Conference on Human-Computer Interaction *(2019), Springer, pp. 72–82.*

[177] Jakubietz, R. G., Jakubietz, M. G., Kloss, D., and Gruenert, J. G. *Defining the basic aesthetics of the hand.* Aesthetic Plastic Surgery 29*, 6 (2005), 546–551.*

[178] Jang-Jaccard, J., and Nepal, S. *A survey of emerging threats in cybersecurity.* Journal of Computer and System Sciences 80*, 5 (2014), 973–993.*

[179] Jethwani, M. M., Memon, N., Seo, W., and Richer, A. *"i can actually be a super sleuth" promising practices for engaging adolescent girls in cybersecurity education.* Journal of Educational Computing Research 55*, 1 (2017), 3–25.*

[180] Johnson, D. R., and Post, D. *Law and borders: The rise of law in cyberspace.* stanford Law Review 48*, 5 (1996), 1367–1402.*

[181] Johnson, M. R. *The history of cyberspace aesthetics in video games. In* Cyberpunk and Visual Culture*. Routledge, 2017, pp. 139–154.*

[182] Johnston, A. C., and Warkentin, M. *Fear appeals and information security behaviors: An empirical study.* MIS Quarterly 34*, 3 (2010), 549–566.*

[183] Josephson, S., and Holmes, M. E. *Attention to repeated images on the world-wide web: Another look at scanpath theory.* Behavior Research Methods, Instruments, & Computers 34*, 4 (2002), 539–548.*

[184] Joshi, D., Datta, R., Fedorovskaya, E., Luong, Q.-T., Wang, J. Z., Li, J., and Luo, J. *Aesthetics and emotions in images.* IEEE Signal Processing Magazine 28*, 5 (2011), 94–115.*

[185] Kahneman, D., and Tversky, A. *Prospect theory: An analysis of decision under risk.* Econometrica 47*, 2 (1979), 363–391.*

[186] Kainda, R., Flechais, I., and Roscoe, A. *Security and usability: Analysis and evaluation. In* 2010 International Conference on Availability, Reliability and Security *(2010), IEEE, pp. 275–282.*

[187] Kalra, S., and Prasad, J. S. *Efficacy of news sentiment for stock market prediction. In* 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) *(2019), IEEE, pp. 491–496.*

[188] Kant, I. The Critique of Judgment*. Prometheus Books, 1892.*

[189] Kanungo, T., and Orr, D. *Predicting the readability of short web summaries. In* Proceedings of the Second ACM International Conference on Web Search and Data Mining *(2009), pp. 202–211.*

[190] Karademas, E. C., Kafetsios, K., and Sideridis, G. D. *Optimism, self-efficacy and information processing of threat-and well-being-related stimuli.* Stress and Health: Journal of the International Society for the Investigation of Stress 23*, 5 (2007), 285–294.*

[191] Karas, T. H., Moore, J. H., and Parrott, L. K. *Metaphors for cyber security.* Sandia Report SAND2008-5381. Sandia Labs, NM *(2008).*

[192] Kaur, R., and Kautish, S. *Multimodal sentiment analysis: A survey and comparison.* Research Anthology on Implementing Sentiment Analysis Across Multiple Disciplines *(2022), 1846–1870.*

[193] Kearney, R., and Rasmussen, D. *Continental aesthetics: Romanticism to postmodernism: An anthology.*

[194] Keenan, T. M. The use of aesthetic knowledge in decision making processes in mega projects*. PhD thesis, Queensland University of Technology, 2016.*

[195] Kemp, S. *Digital 2019: Global digital overview.* `https://datareportal.com/reports/digital-2019-global-digital-overview`*, Jan 2019.*

[196] Kerckhoffs, A. *La cryptographie militaire.* Journal des Sciences Militaires IX *(1883), 5–38.*

[197] Kher, A., Johnson, S., and Griffith, R. *Readability assessment of online patient education material on congestive heart failure.* Advances in Preventive Medicine 2017 *(2017).*

[198] Khoo, C., Robertson, K., and Deibert, R. *Installing fear: A canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications.* University of Toronto Citizen Lab Report *(2019).*

[199] Kikuchi, J. F., and Simmons, H. *Philosophic inquiry in nursing.*

[200] Kim, Y., Chung, S., and So, J. *Success expectancy: A mediator of the effects of source similarity and self-efficacy on health behavior intention.* Health Communication 35*, 9 (2020), 1063–1072.*

[201] Kincaid, J. P., Fishburne Jr, R. P., Rogers, R. L., and Chissom, B. S. *Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel.*

[202] Klonick, K. *The facebook oversight board: Creating an independent institution to adjudicate online free expression.* Yale LJ 129 *(2019), 2418.*

[203] Klopfer, P. H., and Rubenstein, D. I. *The concept privacy and its biological basis.* Journal of Social Issues 33*, 3 (1977), 52–65.*

[204] Kolbitsch, C., Livshits, B., Zorn, B., and Seifert, C. *Rozzle: Decloaking internet malware. In* 2012 IEEE Symposium on Security and Privacy *(2012), IEEE, pp. 443–457.*

[205] Kollolu, R. *A review on wide variety and heterogeneity of iot platforms.* The International journal of analytical and experimental modal analysis, analysis 12 *(2020), 3753–3760.*

[206] Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., and Vigna, G. *Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In* Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security *(2018), pp. 1714–1730.*

[207] Kosar, T., Bohra, S., and Mernik, M. *Protocol of a systematic mapping study for domain-specific languages.* Journal of Information and Software Technology 21*, C (2016), 77–91.*

[208] Kothari, V., Blythe, J., Smith, S., and Koppel, R. *Agent-based modeling of user circumvention of security. In* Proceedings of the 1st International Workshop on Agents and CyberSecurity *(2014), pp. 1–4.*

[209] Krämer, J., Wiewiorra, L., and Weinhardt, C. *Net neutrality: A progress report.* Telecommunications Policy 37*, 9 (2013), 794–813.*

[210] Kraus, J. P. *Selbstreproduktion bei programmen (on self-reproducing programs).* University Dortmund *(Feb 1980).*

[211] Kuang, X. J., Weber, R. A., and Dana, J. *How effective is advice from interested parties?: An experimental test using a pure coordination game.* Journal of Economic Behavior & Organization 62*, 4 (2007), 591–604.*

[212] Kumar, D., Ma, Z., Durumeric, Z., Mirian, A., Mason, J., Halderman, J. A., and Bailey, M. *Security challenges in an increasingly tangled web. In* Proceedings of the 26th International Conference on World Wide Web *(Perth, Australia, Apr. 2017), International World Wide Web Conferences Steering Committee, pp. 677–684.*

[213] Lagun, D., and Lalmas, M. *Understanding user attention and engagement in online news reading. In* Proceedings of the Ninth ACM International Conference on Web Search and Data Mining *(San Francisco, CA, Feb. 2016), WSDM '16, ACM, pp. 113–122.*

[214] Lahlou, S., Langheinrich, M., and Röcker, C. *Privacy and trust issues with invisible computers.* Communications of the ACM 48*, 3 (2005), 59–60.*

[215] Lakoff, G., and Johnson, M. *Conceptual metaphor in everyday language.* The journal of Philosophy 77*, 8 (1980), 453–486.*

[216] Lambach, D. *The territorialization of cyberspace.* International Studies Review 22*, 3 (2020), 482–506.*

[217] Lanier, J. Who owns the future? *Simon and Schuster, 2014.*

[218] Larkin, M. *Mask confusion in nyc with abrupt cdc guidance changes.* The Lancet Infectious Diseases 21*, 7 (2021), 921–921.*

[219] Lasswell, H. D. *The structure and function of communication in society. In* The Communication of Ideas *(1948), L. Bryson, Ed., Harper and Row, pp. 37–51.*

[220] Lawson, S. T., Yeo, S. K., Yu, H., and Greene, E. *The cyber-doom effect: The impact of fear appeals in the us cyber security debate. In* 2016 8th International Conference on Cyber Conflict (CyCon) *(2016), IEEE, pp. 65–80.*

[221] Lee, C., Lee, C. C., and Kim, S. *Understanding information security stress: Focusing on the type of information security compliance activity.* Computers & Security 59 *(2016), 60–70.*

[222] Lee, M., Kwahk, J., Han, S. H., Jeong, D., Park, K., Oh, S., and Chae, G. *Developing personas & use cases with user survey data: A study on the millennials' media usage.* Journal of Retailing and Consumer Services 54 *(2020), 102051.*

[223] Lepore, E., and Stone, M. *Against metaphorical meaning.* Topoi 29*, 2 (2010), 165–180.*

[224] Li, F., Rogers, L., Mathur, A., Malkin, N., and Chetty, M. *Keepers of the machines: Examining how system administrators manage software updates. In* Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security *(Santa Clara, CA, Aug. 2019), USENIX Association, pp. 273–288.*

[225] Li, J., and Knickerbocker, P. *Functional similarities between computer worms and biological pathogens.* Computers & Security 26*, 4 (2007), 338–347.*

[226] Li, Q., Morris, M. R., Fourney, A., Larson, K., and Reinecke, K. *The impact of web browser reader views on reading speed and user experience. In* Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems *(Glasgow, Scotland, May 2019), pp. 1–12.*

[227] Li, T., Convertino, G., Tayi, R. K., and Kazerooni, S. *What data should i protect? recommender and planning support for data security analysts. In* Proceedings of the 24th International Conference on Intelligent User Interfaces *(2019), pp. 286–297.*

[228] Libicki, M. C. *Cyberspace is not a warfighting domain.* Isjlp 8 *(2012), 321–321.*

[229] Lientz, B. P. *Issues in software maintenance.* ACM Computing Surveys (CSUR) 15*, 3 (1983), 271–278.*

[230] Lim, S., Jatowt, A., and Yoshikawa, M. *Understanding characteristics of biased sentences in news articles. In* CIKM Workshops *(2018), pp. 121–128.*

[231] Lin, F., and Yao, M. *The impact of accompanying text on visual processing and hedonic evaluation of art.* Empirical Studies of the Arts 36*, 2 (2018), 180–198.*

[232] Lin, H. *The existential threat from cyber-enabled information warfare.* Bulletin of the Atomic Scientists 75*, 4 (2019), 187–196.*

[233] Lindner, A. M., Pryciak, G., and Elsner, J. *Tor and the city: Msa-level correlates of interest in anonymous web browsing.* Surveillance & Society 18*, 4 (2020), 507–521.*

[234] Lisova, E., Šljivo, I., and Čaušević, A. *Safety and security co-analyses: A systematic literature review.* IEEE Systems Journal 13*, 3 (2019), 2189–2200.*

[235] Liu, F., Abdul-Hussain, S., Mahboob, S., Rai, V., and Kostrzewski, A. *How useful are medication patient information leaflets to older adults? a content, readability and layout analysis.* International journal of clinical pharmacy 36 *(2014), 827–834.*

[236] Luft, S. *Husserl's theory of the phenomenological reduction: between life-world and cartesianism.* Research in Phenomenology 34*, 1 (2004), 198–234.*

[237] Ma, K.-L. *Cyber security through visualization. In* Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation-Volume 60 *(2006), Citeseer, pp. 3–7.*

[238] Macdonald, M., Frank, R., Mei, J., and Monk, B. *Identifying digital threats in a hacker web forum. In* Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015 *(2015), pp. 926–933.*

[239] Maclean, M., Harvey, C., and Kling, G. *Pathways to power: Class, hyper-agency and the french corporate elite.* Organization Studies 35*, 6 (2014), 825–855.*

[240] Macnish, K., and van der Ham, J. *Ethics in cybersecurity research and practice.* Technology in Society 63 *(2020), 101382.*

[241] Maddux, J. E. *Self-efficacy theory. In* Self-efficacy, adaptation, and adjustment*. Springer, 1995, pp. 3–33.*

[242] Malcolm, J., Hodkinson, P., and Colley, H. *The interrelationships between informal and formal learning.* Journal of Workplace Learning 15*, 7/8 (2003), 313–318.*

[243] Malmendier, U., and Shanthikumar, D. *Are small investors naive about incentives?* Journal of Financial Economics 85*, 2 (2007), 457–489.*

[244] Marland, A. *Political photography, journalism, and framing in the digital age: The management of visual media by the prime minister of canada.* The International Journal of Press/Politics 17*, 2 (2012), 214–233.*

[245] Marotta, A., Martinelli, F., Nanni, S., Orlando, A., and Yautsiukhin, A. *Cyber-insurance survey.* Computer Science Review 24 *(2017), 35–61.*

[246] Marres, N., and Weltevrede, E. *Scraping the social? issues in live social research.* Journal of Cultural Economy 6*, 3 (2013), 313–335.*

[247] Martinez, M., Besold, T. R., Abdel-Fattah, A., Gust, H., Schmidt, M., Krumnack, U., and KÃ1/4hnberger, K.-U. *Theory blending as a framework for creativity in systems for general intelligence. In* Theoretical foundations of artificial general intelligence*. Springer, 2012, pp. 219–239.*

[248] Matias, Jr., R., Oliveira, G. D., and de Araujo, L. B. *Operating system reliability from the quality of experience viewpoint: An exploratory study. In* Proceedings of the 28th Annual ACM Symposium on Applied Computing *(Coimbra, Portugal, Mar. 2013), SAC '13, ACM, pp. 1644–1649.*

[249] Mc Grath-Lone, L., Marsh, K., Hughes, G., and Ward, H. *The sexual health of female sex workers compared with other women in England: Analysis of cross-sectional data from genitourinary medicine clinics.* Sexually Transmitted Infections 90*, 4 (2014), 344–350.*

[250] Mc Laughlin, G. H. *Smog grading—a new readability formula.* Journal of Reading 12*, 8 (1969), 639–646.*

[251] McCombs, M. E. *A look at agenda-setting: Past, present and future.* Journalism Studies 6*, 4 (2005), 543–557.*

[252] McCombs, M. E., and Shaw, D. L. *The agenda-setting function of mass media.* Public Opinion Quarterly 36*, 2 (1972), 176–187.*

[253] McCormack, C. *Five stages of a web malware attack, 2016. https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos-five-stages-of-a-web-malware-attack.pdf.*

[254] McLaughlin, M. M., Chow, E. P. F., Wang, C., Yang, L.-G., Yang, B., Huang, J. Z., Wang, Y., Zhang, L., and Tucker, J. D. *Sexually transmitted infections among heterosexual male clients of female sex workers in China: A systematic review and meta-analysis.* PLOS ONE 8*, 8 (Aug 2013), 1–11.*

[255] McLuhan, M. Understanding media*. The MIT Press, 1964.*

[256] McSweeney, B., McSweeney, W., and Bill, M. Security, identity and interests: a sociology of international relations*. No. 69. Cambridge University Press, 1999.*

[257] Metzinger, T. K. *Why is virtual reality interesting for philosophers?* Frontiers in Robotics and AI 5 *(2018), 101–101.*

[258] Meyer, B., and Verrips, J. Aesthetics*. Routledge, 2008.*

[259] Meyer, M. *The rise of the knowledge broker.* Science Communication 32*, 1 (2010), 118–127.*

[260] Miller, S., Wagner, C., Aickelin, U., and Garibaldi, J. M. *Modelling cyber-security experts' decision making processes using aggregation operators.* computers & security 62 *(2016), 229–245.*

[261] Milne, G. R., Labrecque, L. I., and Cromer, C. *Toward an understanding of the online consumer's risky behavior and protection practices.* Journal of Consumer Affairs 43*, 3 (2009), 449–473.*

[262] Mindermann, K. *Are easily usable security libraries possible and how should experts work together to create them? In* Proceedings of the 9th international workshop on cooperative and human aspects of software engineering *(2016), pp. 62–63.*

[263] Mitchell, C., and Weber, S. *Just who do we think we are... and how do we know this?: Re-visioning pedagogical spaces for studying our teaching selves. In* Just who do we think we are? *Routledge, 2013, pp. 1–9.*

[264] Modini, J., Lynar, T., Sitnikova, E., and Joiner, K. *Applications of epidemiology to cybersecurity. In* European Conference on Cyber Warfare and Security *(2020), Academic Conferences International Limited, pp. 483–490.*

[265] Mohammad, S. *Colourful language: measuring word-colour associations. In* Proceedings of the 2nd Workshop on Cognitive Modeling and Computational Linguistics *(2011), pp. 97–106.*

[266] Montroll, E. W. *Social dynamics and the quantifying of social forces.* Proceedings of the National Academy of Sciences 75*, 10 (1978), 4633–4637.*

[267] Moran, R. *Seeing and believing: Metaphor, image, and force.* Critical Inquiry 16*, 1 (1989), 87–112.*

[268] Moshchuk, A., Bragin, T., Gribble, S. D., and Levy, H. M. *A crawler-based study of spyware in the web. In* Proceedings of the Network and Distributed System Security Symposium (NDSS) *(San Diego, CA, Feb. 2006), vol. 1, p. 2.*

[269] Nam, T. *Understanding the gap between perceived threats to and preparedness for cybersecurity.* Technology in Society 58 *(2019), 101122.*

[270] Neocleous, M. Critique of security*. Edinburgh University Press, 2008.*

[271] Ng, B.-Y., and Rahim, M. *A socio-behavioral study of home computer users' intention to practice security.* Pacific Asia Conference on Information Systems *(2005).*

[272] Ng, B.-Y., and Xu, Y. *Studying users' computer security behavior using the health belief model.* PACIS 2007 Proceedings *(2007), 45–45.*

[273] Nichols, J. Illustrations of the literary history of the eighteenth century*, vol. 8. Nichols; Bentley, 1858.*

[274] Nicholson, J., Coventry, L., and Briggs, P. *"if it's important it will be a headline" cybersecurity information seeking in older adults. In* Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems *(2019), pp. 1–11. Paper No. 349.*

[275] Nivala, M., Hauser, F., Mottok, J., and Gruber, H. *Developing visual expertise in software engineering: An eye tracking study. In* 2016 IEEE Global Engineering Education Conference (EDUCON) *(Abu Dhabi, U.A.E., Apr. 2016), IEEE, pp. 613–620.*

[276] Nthala, N., and Flechais, I. *"if it's urgent or it is stopping me from doing something, then i might just go straight at it": a study into home data security decisions. In* International Conference on Human Aspects of Information Security, Privacy, and Trust *(2017), Springer, pp. 123–142.*

[277] Nye, D. E. American technological sublime*. MIT Press, 1996.*

[278] O'Gorman, G., and McDonald, G. Ransomware: A growing menace*. Symantec Corporation, 2012.*

[279] Öğütçü, G., Testik, Ö. M., and Chouseinoglou, O. *Analysis of personal information security behavior and awareness.* Computers & Security 56 *(2016), 83–93.*

[280] Oldehoeft, A. E. Foundations of a Security Policy for Use of the National Research and Educational Network*. No. 4734. U.S. Department of Commerce, National Institute of Standards and Technology, 1992.*

[281] Ollis, T. *Learning in social action: The informal and social learning dimensions of circumstantial and lifelong activists.* Australian Journal of Adult Learning 51*, 2 (2011), 248–268.*

[282] Oravec, J. A. *Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things.* Technology in Society 51 *(2017), 189–198.*

[283] Ortis, A., Farinella, G. M., and Battiato, S. *An overview on image sentiment analysis: Methods, datasets and current challenges.* ICETE (1) *(2019), 296–306.*

[284] Ottaviani, M., and Sorensen, P. N. *Professional advice.* University College London, Department of Economics Working Paper *(1999).*

[285] Page, T. *Skeuomorphism or flat design: future directions in mobile device user interface (ui) design education.* International Journal of Mobile Learning and Organisation 8*, 2 (2014), 130–142.*

[286] Pais, A. Inward bound: of matter and forces in the physical world. *ocford University Press, Oxford, 1986.*

[287] Pan, B., Hembrooke, H. A., Gay, G. K., Granka, L. A., Feusner, M. K., and Newman, J. K. *The determinants of web page viewing behavior: An eye-tracking study. In* Proceedings of the 2004 Symposium on Eye Tracking Research & Applications *(San Antonio, TX, Mar. 2004), Association for Computing Machinery, pp. 147–154.*

[288] Papadopoulou, A. *As seen in your prospectus: A critical essay on the representation of ethnic diversity in stock photography.*

[289] Pariser, E. The filter bubble: What the Internet is hiding from you. *Penguin U.K., 2011.*

[290] Park, J.-y. *An analysis on training curriculum for educating information security experts.* Management & Information Systems Review 31*, 1 (2012), 149–165.*

[291] Pfeiffer, B. A., Clay, S. W., and Conatser JR, R. R. *A green prescription study: does written exercise prescribed by a physician result in increased physical activity among older adults?* Journal of Aging and Health 13*, 4 (2001), 527–538.*

[292] Pfleeger, S. L., and Caputo, D. D. *Leveraging behavioral science to mitigate cyber security risk.* Computers Security 31*, 4 (2012), 597–611.*

[293] Pfleeger, S. L., Sasse, M. A., and Furnham, A. *From weakest link to security hero: Transforming staff security behavior.* Journal of Homeland Security and Emergency Management 11*, 4 (2014), 489–510.*

[294] Phister Jr, P. W. *Cyberspace: The ultimate complex adaptive system. Tech. rep., AIR FORCE RESEARCH LAB ROME NY, 2010.*

[295] Piasecki, S., Urquhart, L., and McAuley, D. *Defence against the dark artefacts: Smart home cyber crimes and cyber-security standards.* Computer Law & Security Review 42 *(2021), 105542.*

[296] Plantin, J.-C., Lagoze, C., Edwards, P. N., and Sandvig, C. *Infrastructure studies meet platform studies in the age of Google and Facebook.* New Media & Society 20*, 1 (2018), 293–310.*

[297] Podins, K., and Lavrenovs, A. *Security implications of using third-party resources in the world wide web. In* 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) *(Vilnius, Lithuania, Nov. 2018), pp. 1–6.*

[298] Provos, N., McNamee, D., Mavrommatis, P., Wang, K., Modadugu, N., et al. *The ghost in the browser: Analysis of web-based malware.* HotBots 7 *(2007), 4–4.*

[299] Pu, J., Liu, J., and Wang, J. *A vision-based approach for deep web form extraction. In* Advanced Multimedia and Ubiquitous Engineering*. Springer, 2017, pp. 696–702.*

[300] Quinlan, M., Zhao, J., and Simpson, A. *Connected vehicles: a privacy analysis. In* International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage *(2019), Springer, pp. 35–44.*

[301] Rader, E., and Wash, R. *Identifying patterns in informal sources of security information.* Journal of Cybersecurity 1*, 1 (2015), 121–144.*

[302] Rader, E., Wash, R., and Brooks, B. *Stories as informal lessons about security. In* Proceedings of the Eighth Symposium on Usable Privacy and Security *(Washington, DC, Jul. 2012), ACM, p. 6.*

[303] Rader, E., Wash, R., and Brooks, B. *Stories as informal lessons about security. In* Proceedings of the Eighth Symposium on Usable Privacy and Security *(2012), pp. 1–17.*

[304] Rafiee, A., Spooren, W., and Sanders, J. *Framing similar issues differently: a cross-cultural discourse analysis of news images.* Social Semiotics 33*, 3 (2023), 515–538.*

[305] Redmiles, E. M., Kross, S., and Mazurek, M. L. *How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. In* 2019 IEEE Symposium on Security and Privacy (SP) *(San Francisco, CA, May 2019), vol. 00, IEEE, pp. 227–244.*

[306] Redmiles, E. M., Kross, S., and Mazurek, M. L. *How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In* 2019 IEEE Symposium on Security and Privacy (SP) *(2019), vol. 00, IEEE, pp. 227–244.*

[307] Redmiles, E. M., Malone, A. R., and Mazurek, M. L. *I think they're trying to tell me something: Advice sources and selection for digital security. In* 2016 IEEE Symposium on Security and Privacy (SP) *(2016), IEEE, pp. 272–288.*

[308] Reeder, R. W., Ion, I., and Consolvo, S. *152 simple steps to stay safe online: Security advice for non-tech-savvy users.* IEEE Security & Privacy 15*, 5 (2017), 55–64.*

[309] Renaud, K. *How smaller businesses struggle with security advice.* Computer Fraud & Security 2016*, 8 (2016), 10–18.*

[310] Renaud, K., and Dupuis, M. *Cyber security fear appeals: unexpectedly complicated. In* Proceedings of the New Security Paradigms Workshop, Costa Rica *(2019), pp. 42–56.*

[311] Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., and Orgeron, C. *Is the responsibilization of the cyber security risk reasonable and judicious?* Computers & Security 78 *(2018), 198–211.*

[312] Reyna, J. *The importance of visual design and aesthetics in e-learning.* Training and Development 40*, 5 (2013), 28–31.*

[313] Rhee, H.-S., Kim, C., and Ryu, Y. U. *Self-efficacy in information security: Its influence on end users' information security practice behavior.* Computers & Security 28*, 8 (2009), 816–826.*

[314] Roberts, J. C., Fletcher, R. H., and Fletcher, S. W. *Effects of peer review and editing on the readability of articles published in annals of internal medicine.* JAMA 272*, 2 (1994), 119–121.*

[315] Robinson, L., Schulz, J., Blank, G., Ragnedda, M., Ono, H., Hogan, B., Mesch, G., Cotten, S. R., Kretchmer, S. B., Hale, T. M., et al. *Digital inequalities 2.0: Legacy inequalities in the information age.*

[316] Rose, G. Visual methodologies: An introduction to researching with visual materials. *Sage, 2016.*

[317] Rubner, Y., Tomasi, C., and Guibas, L. J. *The earth mover's distance as a metric for image retrieval.* International Journal of Computer Vision 40*, 2 (2000), 99–121.*

[318] Rudner, R. *On semiotic aesthetics.* The Journal of Aesthetics and Art Criticism 10*, 1 (1951), 67–77.*

[319] Ruohonen, J., and Kimppa, K. K. *Updating the wassenaar debate once again: Surveillance, intrusion software, and ambiguity.* Journal of Information Technology & Politics 16*, 2 (2019), 169–186.*

[320] Ruoti, S., Monson, T., Wu, J., Zappala, D., and Seamons, K. *Weighing context and trade-offs: How suburban adults selected their online security posture. In* Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS) *(2017), pp. 211–228.*

[321] Rushkoff, D. Present shock: When everything happens now. *Current, 2014.*

[322] Safa, N. S., Von Solms, R., and Furnell, S. *Information security policy compliance model in organizations.* Computers & Security 56 *(2016), 70–82.*

[323] Saks, A. M., and Ashforth, B. E. *Proactive socialization and behavioral self-management.* Journal of Vocational behavior 48*, 3 (1996), 301–323.*

[324] Samek, W., Binder, A., Montavon, G., Lapuschkin, S., and Müller, K.-R. *Evaluating the visualization of what a deep neural network has learned.* IEEE Transactions on Neural Networks and Learning Systems 28*, 11 (2016), 2660–2673.*

[325] Sayers, S. *Jacques rancière (2004) the politics of aesthetics: the distribution of the sensible.* Culture Machine, Reviews *(2005).*

[326] Schatz, D., Bashroush, R., and Wall, J. *Towards a more representative definition of cyber security.* Journal of Digital Forensics, Security and Law 12*, 2 (2017), 53–74.*

[327] Schirrmacher, N.-B., Ondrus, J., and Tan, F. T. C. *Towards a response to ransomware: Examining digital capabilities of the WannaCry attack. In* PACIS *(2018), p. 210.*

[328] Schotter, A. *Decision making with naïve advice.* American Economic Review 93*, 2 (2003), 196–201.*

[329] Seib, C., Debattista, J., Fischer, J., Dunne, M., and Najman, J. M. *Sexually transmissible infections among sex workers and their clients: Variation in prevalence between sectors of the industry.* Sexual Health 6*, 1 (2009), 45–50.*

[330] Senter, R. J., and Smith, E. A. *Automated readability index. Tech. rep., AMRL-TR. Aerospace Medical Research Laboratories, 1967.*

[331] Shahin, S. *Framing "bad news" culpability and innocence in news coverage of tragedies.* Journalism Practice 10*, 5 (2016), 645–662.*

[332] Shapere, D. *The causal efficacy of space.* Philosophy of Science 31*, 2 (1964), 111–121.*

[333] Shedroff, N., and Noessel, C. Make it so: interaction design lessons from science fiction*. Rosenfeld Media, 2012.*

[334] Shelley, J. *The concept of the aesthetic. In* Stanford Encyclopedia of Philosophy*. 2017.*

[335] Shires, J. *Cyber-noir: Cybersecurity and popular culture.* Contemporary Security Policy 41*, 1 (2020), 82–107.*

[336] SimilarWeb*. Official measure of the digital world.* `https://www.similarweb.com/`*, Mar 2021.*

[337] Simon, H. A. *Theories of bounded rationality.* Decision and Organization 1*, 1 (1972), 161–176.*

[338] Singer, A., and Bishop, M. *Trust-based security; or, trust considered harmful. In* New Security Paradigms Workshop 2020 *(Online, USA, Oct. 2020), pp. 76–89.*

[339] Slater, M., Sanchez-Vives, M. V., Rizzo, A., and Bergamasco, M. The Impact of Virtual and Augmented Reality on Individuals and Society*. Frontiers Media SA, 2019.*

[340] Sloterdijk, P. *Spheres volume i: Bubbles microspherology.* Los Angeles: Semiotext (e) *(2011).*

[341] Smith, A. D. *Cybercriminal impacts on online business and consumer confidence.* Online Information Review 28*, 3 (2004), 224–234.*

[342] Smith, R. E. *A contemporary look at saltzer and schroeder's 1975 design principles.* IEEE Security & Privacy 10*, 6 (2012), 20–25.*

[343] Sob, T. *"Hackerman": How diverging cyberspace portrayals influence the adf's perception of cybersecurity and the cultural ramifications of these judgements.* Australian Defense Force - Cyber Security Challenges 1*, 1 (2021), 1–1.*

[344] Solove, D. J. *Conceptualizing privacy.* California law review *(2002), 1087–1155.*

[345] Šorgo, A., Bartol, T., Dolničar, D., and Boh Podgornik, B. *Attributes of digital natives as predictors of information literacy in higher education.* British Journal of Educational Technology 48*, 3 (2017), 749–767.*

[346] Sowndarajan, K., and Binu, S. *Android security issues and solutions. In* 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) *(2017), IEEE, pp. 686–689.*

[347] Stanton, B., Theofanos, M. F., Prettyman, S. S., and Furman, S. *Security fatigue.* IT Professional 18*, 5 (2016), 26–32.*

[348] Steinel, W., Abele, A. E., and De Dreu, C. K. *Effects of experience and advice on process and performance in negotiations.* Group Processes & Intergroup Relations 10*, 4 (2007), 533–550.*

[349] Stock, B., Johns, M., Steffens, M., and Backes, M. *How the web tangled itself: Uncovering the history of client-side web (in)security. In* Proceedings of the 26th USENIX Security Symposium *(Vancouver, BC, Aug. 2017), USENIX Association, pp. 971–987.*

[350] Stokes, J. W., Andersen, R., Seifert, C., and Chellapilla, K. *Webcop: Locating neighborhoods of malware on the web. In* LEET *(2010).*

[351] Straub, J. *Defining, evaluating, preparing for and responding to a cyber pearl harbor.* Technology in Society 65 *(2021), 101599.*

[352] Stumpf, S. A., Brief, A. P., and Hartman, K. *Self-efficacy expectations and coping with career-related events.* Journal of Vocational Behavior 31*, 1 (1987), 91–108.*

[353] Sung, I., Choi, B., and Nielsen, P. *On the training of a neural network for online path planning with offline path planning algorithms.* International Journal of Information Management 57 *(2021), 102142.*

[354] Taylor, M., and Wolff, M. The Victorians since 1901: Histories, representations and revisions*. Manchester University Press, 2004.*

[355] Tharangie, K., Irfan, C., Marasinghe, C., and Yamada, K. *Kansei engineering assessing system to enhance the usability in e-learning web interfaces: Colour basis. In* 16th International Conference on Computers in Education *(2008), vol. 1, pp. 145–150.*

[356] The Spamhaus Project. *Botnet threat report 2019.* `https://www.spamhaus.org/news/images/full-2019/spamhaus-botnet-threat-report-2019.pdf`*, Jan 2020.*

[357] Theng, Y. L., and Thimbleby, H. W. *Addressing design and usability issues in hypertext and on the world wide web by re-examining the "lost in hyperspace" problem.* Journal of Universal Computer Science 4*, 11 (1998), 839–855.*

[358] Thibodeau, P., Winneg, A., Frantz, C., and Flusberg, S. *The mind is an ecosystem: systemic metaphors promote systems thinking.* Metaphor and the Social World 6*, 2 (2016), 225–242.*

[359] Thomas, S. Technobiophilia: Nature and cyberspace*. A&C Black, 2013.*

[360] Thomson-Jones, K., and Moser, S. *The philosophy of digital art.*

[361] Tourangeau, R., and Sternberg, R. J. *Understanding and appreciating metaphors.* Cognition 11*, 3 (1982), 203–244.*

[362] Townsend, K. *18.5 million websites infected with malware at any time. Security Week,* `https://www.securityweek.com/185-million-websites-infected-malware-any-time`*, March 2018.*

[363] Tregear, J. *Risk assessment.* Information Security Technical Report 3*, 6 (2001), 19–27.*

[364] Tufte, E. R. Beautiful evidence*. Graphis Pr, 2006.*

[365] Tversky, A., and Kahneman, D. *Advances in prospect theory: Cumulative representation of uncertainty.* Journal of Risk and Uncertainty 5*, 4 (Oct 1992), 297–323.*

[366] Ugarte-Pedrero, X., Graziano, M., and Balzarotti, D. *A close look at a daily dataset of malware samples.* ACM Transactions on Privacy and Security (TOPS) 22*, 1 (2019), 1–30.*

[367] Unsworth, N., and Engle, R. W. *The nature of individual differences in working memory capacity: active maintenance in primary memory and controlled search from secondary memory.* Psychological Review 114*, 1 (2007), 104–32.*

[368] Venkatesh, A. *Social media, digital self, and privacy: a socio-analytical perspective of the consumer as the digital avatar.* Journal of the Association for Consumer Research 1*, 3 (2016), 378–391.*

[369] Viet, H. N., Van, Q. N., Trang, L. L. T., and Shone, N. *Using deep learning model for network scanning detection. In* Proceedings of the 4th International Conference on Frontiers of Educational Technologies *(2018), pp. 117–121.*

[370] von Neumann, J., and Burks, A. W. Theory of self-reproducing automata*. University of Illinois Press, 1966.*

[371] Von Solms, R., and Van Niekerk, J. *From information security to cyber security.* Computers & Security 38 *(2013), 97–102.*

[372] W3Counter*. Browser platform market share.* `https://www.w3counter.com/globalstats.php`*, Mar 2021.*

[373] Wagner, N., Şahin, C. Ş., Pena, J., and Streilein, W. W. *Automatic generation of cyber architectures optimized for security, cost, and mission performance: A nature-inspired approach. In* Advances in Nature-Inspired Computing and Applications*. Springer, 2019, pp. 1–25.*

[374] Wäldchen, J., and Mäder, P. *Plant species identification using computer vision techniques: A systematic literature review.* Archives of Computational Methods in Engineering 25*, 2 (2018), 507–543.*

[375] Wall, J. D., and Buche, M. W. *To fear or not to fear? a critical review and analysis of fear appeals in the information security context.* Communications of the Association for Information Systems 41*, 1 (2017), 13.*

[376] Walsh, D. *Aesthetic objects and works of art.* The Journal of Aesthetics and Art Criticism 33*, 1 (1974), 7–12.*

[377] Wang, D., Zhang, Z., Wang, P., Yan, J., and Huang, X. *Targeted online password guessing: An underestimated threat. In* Proceedings of the 2016 ACM SIGSAC conference on computer and communications security *(2016), pp. 1242–1254.*

[378] Wang, W., and Lu, Z. *Cyber security in the smart grid: Survey and challenges.* Computer Networks 57*, 5 (2013), 1344–1371.*

[379] Wang, Y., Wang, Y., Liu, J., and Huang, Z. *A network gene-based framework for detecting advanced persistent threats. In* 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing *(2014), IEEE, pp. 97–102.*

[380] Wang, Y., Xiong, H., Liu, S., Jung, A., Stone, T., and Chukoskie, L. *Simulation agent-based model to demonstrate the transmission of covid-19 and effectiveness of different public health strategies.* Frontiers in Computer Science *(2021), 82–82.*

[381] Warner, M. *Cybersecurity: A pre-history.* Intelligence and National Security 27*, 5 (2012), 781–799.*

[382] Weinstein, B. D. *What is an expert?* Theoretical Medicine 14*, 1 (1993), 57–73.*

[383] Weller, H. I., and Westneat, M. W. *Quantitative color profiling of digital images with earth mover's distance using the R package* `colordistance`*.* PeerJ 7 *(2019), e6398.*

[384] Wenger, E. *Communities of practice: Learning as a social system.* Systems Thinker 9*, 5 (1998), 2–3.*

[385] Whitten, A., and Tygar, J. D. *Why johnny can't encrypt: A usability evaluation of pgp 5.0. In* USENIX security symposium *(1999), vol. 348, pp. 169–184.*

[386] Wiederhold, B. K. *The role of psychology in enhancing cybersecurity.* Cyberpsychology, Behavior, and Social Networking 17*, 3 (2014), 131–132.*

[387] Wissenburg, I. *Aesthetic communication on the possibility of combining semiotics and aesthetics: analysis of 'delftsche slaolie'by jan toorop. B.S. thesis, 2012.*

[388] Wong, N. C., and Cappella, J. N. *Antismoking threat and efficacy appeals: effects on smoking cessation intentions for smokers with low and high readiness to quit.* Journal of Applied Communication Research 37*, 1 (2009), 1–20.*

[389] Wood, C. C. *Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature.* Computer Fraud & Security 2004*, 1 (2004), 16–17.*

[390] Xing, X., Meng, W., Lee, B., Weinsberg, U., Sheth, A., Perdisci, R., and Lee, W. *Understanding malvertising through ad-injecting browser extensions. In* Proceedings of the 24th international Conference on World Wide Web *(Florence, Italy, May 2015), pp. 1286–1295.*

[391] Yasaka, T. M., Lehrich, B. M., and Sahyouni, R. *Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app.* JMIR mHealth and uHealth 8*, 4 (2020), e18936.*

[392] Yee, K.-P. *Aligning security and usability.* IEEE Security & Privacy 2*, 5 (2004), 48–55.*

[393] Yoo, C. W., Sanders, G. L., and Cerveny, R. P. *Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance.* Decision Support Systems 108 *(2018), 107–118.*

[394] Yuan, S., Fernando, A., and Klonoff, D. C. *Standards for medical device cybersecurity in 2018.* Journal of Diabetes Science and Technology 12*, 4 (2018), 743–746. PMID: 29575925.*

[395] Zander, T., Öllinger, M., and Volz, K. G. *Intuition and insight: Two processes that build on each other or fundamentally differ?* Frontiers in Psychology 7 *(2016), 1395.*

[396] Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. *Internet of things for smart cities.* IEEE Internet of Things Journal 1*, 1 (2014), 22–32.*

[397] Zhu, L., Huang, X., Liu, Y., and Zhang, Z. *Spatiotemporal dynamics analysis and optimal control method for an si reaction-diffusion propagation model.* Journal of Mathematical Analysis and Applications 493*, 2 (2021), 124539.*

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

[399] Zurko, M. E., and Simon, R. T. *User-centered security. In* Proceedings of the 1996 workshop on New Security Paradigms Workshop *(1996), pp. 27–33.*