Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education

Andreas Haggman

Submitted to Royal Holloway, University of London
for the award of Doctor of Philosophy in Information Security

Supervised by
Professor Keith Martin
Professor Klaus Dodds

February 2019

Declaration of authorship

I, Andreas Haggman, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

Date:

Abstract

This thesis investigates, and contributes to, the use of wargaming in cyber security education. Wargaming has a rich history of pedagogic use, but little work exists that addresses the critically important subject of cyber security. Cyber security is a global problem that frequently makes news headlines, yet the field is dogged with a reputation as a domain only for technologists, when in fact cyber security requires a whole gamut of approaches to be properly understood.

The thesis is broadly divided into three parts. The first part is a comprehensive literature review of wargaming scholarship, analysing the benefits and drawbacks of wargaming, and some of the justifications for why a tabletop boardgame may be more effective than a game enhanced by technology. Following on from this, the thesis provides an outline of current work in cyber wargaming by analysing existing games, evaluating their contributions as educational tools, and identifying successful game mechanics and components.

The second part of the thesis outlines the design process of an original wargame created for cyber security education and awareness training. The analysis outlines what the game design intends to achieve in terms of pedagogical outcomes and how the design evolved through the development process. In this part some methodological considerations around the research are also analysed, including how the thesis uses grounded theory and ethnography as academic underpinnings, and issues around the researcher's positionality during fieldwork.

The final part of the thesis reports on the deployment of the original game to a wide variety of organisations. Both quantitative and qualitative data is analysed to ascertain what players learned from playing the game and evaluates the effectiveness of the game by comparing it to previous theoretical findings. Finally, the researcher's experiences of conducting the thesis are evaluated with close reference to the identified methodological considerations.

Acknowledgements

I want to acknowledge the stimulating and supportive Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (funded by the EPSRC and the UK government (EP/K035584/1)). The CDT is an amazing programme and I am proud to have been a part of it.

Thanks to Tom Mouat and Rob Black for helping arrange and take part in some of the most valuable game sessions; to Thorsten Kodalle for making possible one of the most incredible experiences of my professional life; and to Simon Shiu for believing in the research at its earliest stages.

This thesis has been far from ordinary in many ways, and enormous thanks goes to my supervisors Klaus Dodds and Keith Martin for enduring more trials and tribulations than could reasonably be expected. Their advice and guidance has been nothing short of invaluable.

Thanks to all the participants who played the game, whom I regret I cannot thank individually in these pages, but especially to my peers at Royal Holloway who contributed to early playtesting sessions when the game was, frankly, rubbish. Without their input the game would not be what it is today.

Thanks to Kim Burchill for casting her expert eye over the final drafts to pick out my spelling and grammar errors.

Thanks also to my parents for their nurture and care. Who knew lilla gubben would end up writing a PhD thesis?!

Finally, on a personal level, my eternal gratitude goes to my partner Ellie, without whose support and understanding none of this would have been possible.

Andreas Haggman
Twickenham, February 2019

Table of Contents

DECLARATION OF AUTHORSHIP 2
ABSTRACT 3
ACKNOWLEDGEMENTS 4
LIST OF FIGURES 8
LIST OF TABLES 9

CHAPTER 1: INTRODUCTION – WHY CYBER WARGAMING? 10

1.1 MOTIVATION 11
1.2 A DEARTH OF CYBER GAMES 12
1.3 GENESIS OF THE THESIS 14
1.4 THESIS STRUCTURE 16
1.5 KEY ORIGINAL CONTRIBUTIONS 18

CHAPTER 2: USES, ADVANTAGES, AND LIMITATIONS OF WARGAMING 19

2.1 USES OF WARGAMING 20
2.1.1 CATEGORISING THE USES OF WARGAMING 21
2.1.2 FUTURES AND ANTICIPATION 26
2.1.3 SKILLS 32
2.1.4 PLAY AND PLAYFULNESS 36
2.2 ADVANTAGES OF WARGAMING 39
2.2.1 ADVANTAGES OVER COMPUTERS 39
2.2.2 THE HUMAN FACTOR 43
2.2.3 COST 45
2.2.4 CREATIVITY 46
2.2.5 EXPERIENCE AND SIMULATION 47
2.2.6 FLEXIBILITY 48
2.2.7 SAFETY 49
2.3 LIMITATIONS OF WARGAMING 50
2.3.1 ABSTRACTION 50
2.3.2 OPPONENTS 53
2.3.3 OUTCOME 54
2.3.4 POLITICS OF REPRESENTATION 55
CHAPTER 2 CONCLUSION 57

CHAPTER 3: THE STATE OF PLAY – EXISTING CYBER WARGAMES 60

3.1 LUDIC COMPONENTS 64
3.1.1 GAMES THAT ARE PLAYABLE AND ENJOYABLE 64
3.1.2 GAMES THAT ARE NOT QUITE GAMES 69
3.2. ADVERSARIAL NATURE 72
3.2.1 PLAYER VERSUS PLAYER 73

3.2.2 Player versus system 76
3.3 Cards 78
3.4 Simulating unpredictability 81
3.5 Marketplace 84
Chapter 3 Conclusion 88

CHAPTER 4: DESIGNING A CYBER SECURITY WARGAME 90

4.1 Realism versus complexity in game design 92
4.1.1 Length of rules 93
4.2 Key constituents of cyberspace 94
4.2.1 Entities 96
4.2.2 Relationships between constituents 107
4.3 Strategic goal-setting in cyber security 111
4.3.1 Player Objectives 113
4.3.2 Managing limited resources 116
4.4 Cyber attack and defence dynamics 118
4.4.1 Dynamics of time progression 118
4.4.2 Dynamics of cyber capability development 121
4.4.3 Attack Vectors 127
4.4.4 Dynamics of attack risk and reward 130
4.4.5 Dynamics of attribution 132
4.5 Geopolitical realities of cyber security 134
4.5.1 Clumsy Civil Servant Event Card 135
4.5.2 Banking Error Event Card 136
4.5.3 People's Revolt Event Card 137
4.5.4 Quantum Breakthrough Event Card 138
4.6 Visibility in cyberspace 139
Chapter 4 Conclusion 141

CHAPTER 5: METHODOLOGY FOR STUDYING GAMES AND PLAYERS 144

5.1 Grounded theory and its links to wargaming 146
5.2 Ethnographic practice 149
5.2.1 Strategic positionality 150
5.2.2 Strategy for targeting research participants 155
5.2.3 Security and classification of information 157
5.3 Facilitation and adjudication 159
5.3.1 Tactical Positionality I 161
5.4 Methods for capturing game results and player experiences 163
5.4.1 Data gathering methods 164
5.4.2 Tactical Positionality II 170
5.5 Data analysis methods 171
Chapter 5 Conclusion 173

CHAPTER 6: PEDAGOGY AND PRACTICE IN CYBER WARGAMING 174

6.1 Gaming by numbers: quantitative uses of metadata and game data **175**
6.1.1 The gender imbalance in wargaming 176
6.1.2 In-game performance as a guide to real-world performance 177
6.1.3 In-game results as a guide to real-world results 179
6.1.4 Playing styles of different groups 181
6.2 Learning through the game: expected and unexpected results **183**
6.2.1 Entities 184
6.2.2 Entity relationships 189
6.2.3 Objectives 191
6.2.4 Resource management 194
6.2.5 Attack and defence dynamics 196
6.2.6 Geopolitical realities and landscapes 209
6.2.7 Visibility in and of cyberspace 211
6.3 Practicing wargaming theory **214**
6.3.1 Realism versus complexity 215
6.3.2 Decision-making experience 217
6.3.3 Engagement 218
6.3.4 Manual wargaming and advantages over computers 227
Chapter 6 conclusion **230**

CHAPTER 7: A WARGAMING PRACTITIONER'S EXPERIENCE **233**

7.1 The impact of the researcher's positionality **234**
7.1.1 Creating research opportunities 235
7.1.2 Tactical positionality 242
7.2 Secrecy, security, and classification of information **258**
7.2.1 Access denied 259
7.2.2 Stifled participants 261
7.3 Humour as a pedagogical tool **263**
7.3.1 Elevating mundanity through humour 265
7.3.2 Poking fun at Presidents 267
7.3.3 Using humour to engineer affective atmospheres 268
Chapter 7 conclusion **270**

CHAPTER 8: CONCLUSIONS **274**

8.1 Research findings compared to the literature **275**
8.1.1 Corroborating the story-living experience 276
8.1.2 Corroborating the modifiability advantage of manual games 276
8.1.3 Corroborating the balance between realism and complexity 277
8.1.4 Game rules are not easy to write 278
8.2 Novel takeaways for wargamers **278**
8.2.1 Merging distant literature 279
8.2.2 A catalogue for best-practice in cyber games design 279
8.3 Key original contributions of the research **280**
8.3.1 Development of a novel cyber wargame 280
8.3.2 A wargaming practitioner's experience 281

8.3.3 ADDRESSING THE CENTRAL THESIS OBJECTIVE 282
8.4 THE WAY AHEAD 283

APPENDICES 285

APPENDIX A: PLAYER DOSSIERS 285
UK GOVERNMENT 285
ELECTORATE 286
UK PLC 287
GCHQ 288
UK ENERGY 289
RUSSIA GOVERNMENT 290
ONLINE TROLLS 291
ENERGETIC BEAR 292
SCS 293
ROSENERGOATOM 294
APPENDIX B: GAME RULES 295
APPENDIX C: GAME SESSIONS 297

BIBLIOGRAPHY 308

List of Figures

FIGURE 1: A GAME OF [D0X3D!] IN ACTION 68
FIGURE 2: SCREENSHOT FROM SPOT THE RISKS, OFFICE VERSION 72
FIGURE 3: OPERATION DIGITAL CHAMELEON GAME BOARD 74
FIGURE 4: CTRL+ALT+HACK GAME BOX AND CONTENTS 79
FIGURE 5: MAELSTROM GAME BOARD 87
FIGURE 6: VERSION 1.0 OF THE GAME BOARD 97
FIGURE 7: FINAL VERSION OF THE GAME BOARD 97
FIGURE 8: THE IN-GAME BLACK MARKET 122
FIGURE 9: BLACK MARKET ASSET CARDS 123
FIGURE 10: VERSION 1.0 COMBAT RESULTS TABLE 131
FIGURE 11: FINAL VERSION COMBAT RESULTS TABLE 131
FIGURE 12: EVENT CARDS 135
FIGURE 13: NON-EVENT CARD 135
FIGURE 14: WARGAME OUTCOME PROBABILITY DISTRIBUTIONS. FROM SABIN (2012), P. 56 180
FIGURE 15: A ROLLING MOMENT, SHOWCASING THE EMOTIVE POWER OF DICE 220
FIGURE 16: THE FUN AND ENTERTAINING QUALITIES OF THE GAME EMBODIED IN PLAYERS 224
FIGURE 17: WIZARD WHEEZE EVENT CARD WRITTEN BY GERMAN MILITARY PLAYER 229
FIGURE 18: COMPARISON OF EARLY AND LATER FIELDNOTES 253
FIGURE 19: THE RESEARCHER EXPLAINING THE GAME RULES AT CYCON 2018 256

List of Tables

TABLE 1: GAMES ANALYSED IN THIS CHAPTER.....60
TABLE 2: GENDER BREAKDOWN OF GAME SESSION PARTICIPANTS 177
TABLE 3: RESOURCE AND VITALITY VALUES FOR ENERGETIC BEAR 182

Chapter 1: Introduction – why cyber wargaming?

Wargaming is an activity that at some level of abstraction attempts to model and simulate conflict. Jim Dunnigan, a giant of the wargaming community, has stated that wargaming is most simply understood as 'glorified chess.'[1] A more elaborate expression, from Peter Perla, another wargaming giant, defines a wargame as 'a warfare model or simulation whose operation does not involve the activities of actual military forces, and whose sequence of events affects and is, in turn, affected by the decisions made by players representing the opposing sides.'[2] Used in this way, wargaming is a study of humans that can help us to better understand events of the past, present, and future.

But wargaming is not limited to military use and has made its way to other contexts where conflict, perhaps better framed as competition, is prevalent, such as policymaking or business environments. This thesis explores all three of these contexts with regards to one specific topic: cyber security. The thesis has three key research objectives:

- *Create a wargame for cyber security education.*
- *Analyse the capacity for the game to create learning moments and enable players to share knowledge and ask the right questions.*
- *Reflect on the researcher's experience as a wargaming practitioner.*

In order to address these objectives, the researcher has developed an original tabletop wargame and deployed it to a variety of organisations to gather data about its pedagogic efficacy. The entire research process, from scoping and methodology through to game design and wargaming practice, is documented in this thesis.

[1] Dunnigan (1992), p. 13
[2] Curry (2011), p. 157

1.1 Motivation

This thesis is motivated in the first instance by the critical importance of cyber security. With computers, networks, and digital devices becoming near-ubiquitous for people and organisations, cyber threats have been recognised as one of the most prevalent and impactful risks facing society today. In the UK, the most recent National Security Strategy and Strategic Defence and Security Review (from 2015) ranked cyber threats as a Tier One risk – the highest – stating that 'cyber risks underpin many of the other treats we face.'[3] Outside the national security context, cyber security is also high on agendas. In a survey of treasury and finance professionals, the Association for Finance Professionals states that cyber security 'disproportionately occupy' concerns, with 52% of respondents ranking it as a top three risk.[4] Insurer Allianz, meanwhile, reports that cyber incidents are rated as the top business risk in 11 countries but that they are simultaneously the most underestimated risk.[5]

Despite recognition of its importance, knowledge and understanding of cyber security remains underdeveloped. In addition to a global skills shortage (discussed in Section 4.2.2), cyber security is often viewed as a niche technical subject requiring a computer science degree just to grapple with its impenetrable jargon. This view is severely mistaken. Cyber security is a multifaceted subject extending beyond technology into the realms of psychology, international relations, sociology, geography, ethics, and more. As a problem to solve, cyber security requires more than technical solutions, including processes enabling organisational responses, and well-trained people recognising risks.

The latter of these is of particular importance; people are often viewed as the weakest link in the security chain (see Section 4.5.1), yet with education and training they can be turned into the first line of defence. This thesis attempts to create and measure the effectiveness of a tool for such education in the form of a tabletop wargame. The theoretical target audience for the game are senior policy- and decision-makers who understand that cyber security is important but may not

[3] HM Government (2015), p. 85
[4] Association for Finance Professionals (2018), pp. 7, 10
[5] Allianz (2018), pp. 10-11

have had an opportunity to closely engage with key cyber concepts and terminology. This audience was targeted because buy-in and understanding at the top of an organisation is crucial to building a robust cyber security culture. Moreover, top executives are often the targets of cyber fraudsters, particularly spearphishing attacks.[6] However, although this was the theoretical target audience, in practice the game was played by a range of participants (see Appendix C).

In using wargames as educational tools, this thesis also answers a call to arms from wargaming academic Philip Sabin. Referring to his own success in using historical wargames to teach university students, Sabin encourages those with an interest in gaming to 'come out of the closet' and embrace wargaming for education.[7] Despite targeting a different audience, the present research is an attempt to use wargames in a way that is accessible, acceptable, and in no way "closeted."

1.2 A dearth of cyber games

As illustrated at multiple points throughout the thesis (notably Section 2.1 and the introduction to Chapter 3), wargaming has a rich history of use, especially in the military but also in various civilian contexts. Wargames, both professional and hobby, cover all of the four traditional military domains (land, sea, air, and space) at every level ranging from grand strategic games to operational games to squad-based tactical simulations. Meanwhile, the ideas of gamification and serious play have garnered significant traction with businesses as means for customer engagement and retention, and for employee training. Relatedly, games have been used in educational settings, both academic and professional, to teach a multitude of subjects. A systematic mapping study by Darina Dicheva et al found an exponential increase in the use of gamification in education between 2010 and 2014.[8] Anecdotal observations suggest this trend has continued in the intervening years.

[6] FireEye (2016), p. 2
[7] Sabin (2015), p. 346
[8] Dicheva et al (2015), p. 76

The authors of the mapping study also found that computer science and information technology educators were most likely to adopt gamified elements in their curricula, but evidence exists of games designed to teach a diverse range of subjects.[9] Consider the following non-exhaustive list:

- Games for environmental education[10], including climate change[11], sea ice[12], and glaciers.[13]
- Games for young children's education, including communication and social skills[14], and preschool reading and mathematics.[15]
- Games for biology and medical education, including sex education[16] and burn care.[17]
- Games for teaching the American Revolution.[18]
- Games for teaching homeland security.[19]
- Gamification in designing open governance platforms.[20]

Indeed, simply consulting leading journals in the field, such as *Simulation & Gaming*, reveals a myriad of academic endeavours presenting innovative games or gamified systems.

Amidst this wealth of examples and expertise is a notable omission: cyber security. NATO has declared cyberspace as the fifth domain of warfare, yet very few military wargames about cyber security exist, at least ones that are accessible to the public.[21] As Joseph Miranda has outlined, some military wargames have included cyber operations as tools available to commanders to achieve effects but did not focus exclusively on these.[22] In the hobby sphere, cyber *security* games

[9] Dicheva et al (2015)., p. 81
[10] Bedwell (1977)
[11] Eisenack (2012); Taylor (2017)
[12] Berry Bertram (2008)
[13] Knight (1994)
[14] Collins et al (2011)
[15] Weisberg et al (2015)
[16] Kashibuchi and Sakamoto (2001)
[17] Whittam and Chow (2017)
[18] Smith (2013)
[19] Cozine (2015)
[20] Kelley and Johnston (2012)
[21] Paganini (2016)
[22] Miranda (2016), pp. 673-678

have largely been subsumed in the cyber*punk* genre, which is related but concerned more with science fiction than contemporary security concepts. Some games for cyber security education do exist (see Chapter 3), and some of these are rather good too, but in the current state of affairs wargaming remains a woefully underutilised tool for cyber security education.

This thesis represents an attempt to ameliorate this situation by plugging the gap in cyber wargames.

1.3 Genesis of the thesis

Unlike many PhD theses, in which the central focus, perhaps even the core question, is closely defined before research commences, this thesis had more informal beginnings. The thesis started out as a summer project conducted in the first year – a training year – of the Centre for Doctoral Training in Cyber Security (CDT) programme at Royal Holloway, University of London. The project was to be equivalent to a Masters-level dissertation on any topic of the researcher's choosing. The CDT has a number of external partners, and projects could be conducted in conjunction with one of these, outside the confines of pure academia. One of the partners is a professional services firm providing audit, tax, and advisory services. The researcher decided to partner with the firm for their project, not with any particular research topic in mind, but simply to gain some experience collaborating with the private sector.

After receiving assent from the firm to collaborate, the researcher was tasked with coming up with some project ideas and the firm would then decide which idea it thought was most worthwhile and could provide support for. Amongst others, one of the ideas was cyber wargaming, though at this stage the idea was embryonic, and the researcher had only suggested it because they saw it briefly mentioned in a press release.[23] Despite being so unrefined, wargaming was the topic the firm elected to pursue and the researcher was given a point of contact who would assist with the project.

[23] Smelkovs (2015)

Crucially, and serendipitously (a theme returned to in Section 7.1.1), the contact person had previously been a senior UK civil servant, where they had commissioned a report on cyber wargaming called 'The Global Cyber Game' (see Chapter 3, Game 6). Moreover, the person was aware of the shortcomings of this report and was keen to see something more actionable created.[24] Actionability therefore became the key word which the project strived towards, resulting in a prototype tabletop wargame involving players navigating computer networks to capture digital loot. Ultimately, the project was well-received, and the researcher was encouraged by positive reactions to the prototype game at the Connections UK wargaming conference held in London in September 2015. On the back of this, it was decided to pursue the topic more thoroughly for the PhD thesis.

It is important to be cognisant of these origins because they have fundamentally shaped the thesis in two ways. Firstly, the actionability brief which drove the summer project echoed through to the thesis. Rather than create a purely academic endeavour, the researcher wanted to produce something with potential for real-world impact and the most direct method to do this was to develop a game for people to play. By design, the thesis would thereby interact with the real world in a very hands-on, actionable, way.

Secondly, although the prototype game was successful in demonstrating the possibility of wargaming cyber security, it was also limited in what it could achieve. Practically, the game was for two players and resource-intensive to facilitate. The game could therefore not scale to larger playing groups, limiting the amount of people that could be exposed to it. More theoretically, the game depicted a tactical cyber operation, but ample tools already existed for training network operators in simulated environments. It was therefore decided to realign the design approach to the national strategic level, for which no games exist, resulting in the game presented in Chapter 4.

This thesis therefore had less than orthodox origins, but the work presented herein holds both academic merit and represents impactful research.

[24] Author telephone conversation with firm contact, 26 May 2015

1.4 Thesis structure

Aside from the introduction and conclusion, the thesis contains six substantive chapters. Chapter 2 forms an initial literature review, the aim of which is to embrace the interdisciplinary nature of wargaming. Although there is an abundance of wargaming literature, wargaming is not by itself an academic discipline, but instead draws on a range of disciplines. In addition to references to standard wargaming texts from the likes of Dunnigan and Perla, the literature consulted in Chapter 2 includes works of history, philosophy, geography, and computer science. The chapter's originality stems from the intersection of all these disciplines, drawing out themes particular to cyber wargaming which have not hitherto been analysed in the existing literature.

Chapter 3 forms a second literature review, surveying the cyber wargaming landscape. Despite there being a dearth of such games, as previously outlined, there are nevertheless some games in the field and these must be taken into account, partly to position the thesis and partly to inform game design. The chapter identifies 25 games, spread across wargames, educational games, hobby or entertainment games, and some which fall into neither of these categories. Overall, it is found that several of the games contain components or mechanics which fulfil useful educational purposes and can be used for inspiration in future game design.

In Chapter 4, these inspirations are realised through the design of an original tabletop cyber wargame. The game is loosely based on the UK National Cyber Security Strategy (both 2011 and 2016 versions) and the purpose is to expose players to a wide range of cyber security concepts. The intention is that players learn lessons by engaging with these concepts through the game. As well as taking into account fundamental game design principles such as realism versus complexity, gameplay phases, and visibility, the chapter justifies the inclusion (and exclusion) of the cyber security elements of the game by relating their real-world importance.

The first three chapters having formed the theoretical components of the thesis, the next three are more practical in nature. Chapter 5 outlines the research methodology of the thesis, with particular attention paid to ethnographic practice and the role of positionality. Two types of positionality are defined: strategic positionality, encompassing the background of the researcher; and tactical positionality, referring to the researcher's behaviour during the research. Tactical positionality is further delineated into two strands with different tensions: one concerning the running of games, where there are tensions between the role of designer and facilitator/adjudicator; and one concerning data collection, where there are tensions between the role of facilitator/adjudicator and researcher. The chapter draws on ethnographic literature, wargaming literature, and the experience of other researchers to establish a robust research methodology.

In Chapter 6, findings from the fieldwork are presented. The original game was deployed in 33 game sessions across a variety of civilian and military organisations, both in the UK and overseas. The data collected from these sessions is analysed in three ways. First, quantitative data is interpreted using techniques which might be found in analytical wargames, although the intention here is to illustrate how such techniques can be used, rather than to draw any concrete conclusions. Second, directly addressing the central thesis objectives, qualitative data about player discussions is analysed, organised thematically by learning moments and aligning these with the purposes served by different game components. Finally, qualitative data about player engagement with the game is compared to the advantages of gaming found in Chapter 2, for example corroborating Peter Perla and Ed McGrady's assertion that games provide a 'story-living experience.'[25]

In the last substantive chapter, the researcher writes from a personal perspective, analysing their experiences as a wargaming practitioner. This covers the creation of research opportunities, particularly the role of serendipity, and the researcher's experience as a wargame facilitator, particularly the physically and mentally exhausting nature of facilitation. Some challenges of working on the edge of classified environments are also discussed, followed by an analysis of the

[25] Perla and McGrady (2011), p. 112

important role of humour during game sessions. These personal stories are important because they are largely lacking in extant wargaming literature yet are exceptionally useful for understanding the realities of wargaming in practice.

1.5 Key original contributions

The concluding section in each chapter summarises the original contributions made, and Chapter 8 reinforces these. However, by way of providing the bottom line up front, it is worth highlighting some of the key contributions this thesis makes to cyber wargaming.

- The creation of an original game in Chapter 4 represents a novel addition to cyber wargaming. The game is pioneering in that it tackles cyber security from a strategic level, yet also showcases the value of understanding the wargaming landscape and being able to transpose useful mechanics from other games (evaluated in Chapter 3).
- The researcher's experience as a wargaming practitioner, particularly in organising and facilitating game sessions, were of crucial importance. Extant wargaming literature is largely devoid of experiential accounts of wargamers, so by providing a candid reflection on the researcher's experience some of the seemingly unwritten assumptions about the practice of wargaming could be challenged (Chapter 7).
- Most crucially, the research positively addresses the central thesis objectives. As illustrated in Chapter 6, the game was successful in generating discussions around a multitude of cyber security topics ranging from key actors in cyberspace to attack and defence dynamics, thereby creating learning moments for players. The research illustrates that wargames can be an effective learning tool in cyber security education and awareness training.

Chapter 2: Uses, advantages, and limitations of wargaming

The literature that informs this thesis comes from a broad range of academic disciplines. The primary source is wargaming literature, but this is not a standalone discipline, nor does it belong exclusively in any other discipline, instead drawing on and straddling several fields. This is not to say that wargaming lacks academic merit on its own, but rather that it faces a number of challenges which prevent it from being confined within one discipline. With regards to the interdisciplinarity of wargaming, Robert Stemp writes of operations research 'integrating the conventional academic disciplines'[26], and Rudolph Darken and Curtis Blais state that modelling and simulation does not 'fit neatly into a traditional academic department.'[27] Another challenge is that of acceptance. Sabin notes that wargaming carries a 'stigma', especially among historians[28], and that 'one would scarcely know from academic literature that wargaming even existed,'[29] while Robert Rubel writes that wargaming 'is still more a craft than a discipline,' suggesting this as a hindrance to professionalisation.[30]

Rather than resist interdisciplinarity, this thesis seeks to embrace it by interrogating a multiplicity of sources with regards to their applicability to wargaming, creating a novel intersection where previously unrelated bodies of literature can meet and enhance one another.

This Chapter is broadly divided into three sections. Section 2.1 covers the uses of wargaming, firstly by constructing a high-level categorisation of the uses of wargaming, based on deficiencies identified in existing categorisations, notably by Garry Brewer and Martin Shubik. This is followed by close analysis around three

[26] Stemp (1991), p. 15
[27] Darken and Blais (2017), p. 152
[28] Sabin (2015), p. 344
[29] Ibid., p. 330
[30] Rubel (2006), p. 109

themes. Firstly, the theme of exploring futures and anticipation draws on diverse writers such as geographer Ben Anderson, philosopher Alexander Galloway, historian Sharon Ghamari-Tabrizi. Secondly, the theme of gaining skills draws on testimony from various participants in the 2010 Schriever Wargame as evidence for specific cyber security-related skills, and on material from wargamers such as Robert Specht and Graham Longley-Brown for the capacity of wargames to generate self-learning. Thirdly, the theme of play and playfulness uses arguments from John Gray and Johan Huizinga, among others, to elucidate the close links between war and play and the important role of playfulness in wargaming.

Section 2.2 outlines the advantages of wargaming, particularly the advantages of manual gaming over computer gaming, and wargaming vis-à-vis other methods of learning and training. Here, the wargaming literature is rich with analysis and evidence, and the section references many standard works from Jim Dunnigan, Peter Perla, and Ed McGrady, in addition to lesser-known writers like Sanu Kainikara.

The chapter is rounded off by Section 2.3, which continues to draw on much of the same wargaming literature to balance against the positives by providing an overview of some of the limitations of wargaming in how it can be used and what it can achieve. A concluding section summarises the main contributions of the chapter: the creation of a succinct categorisation of the uses wargaming, intersecting diverse literatures on futures, and using computer science literature to corroborate claims in wargaming literature about the advantages of paper over computers.

2.1 Uses of wargaming

The uses of wargaming are highly dependent on the context of the game, the players and the organisation. The history of wargaming shows us that at various times, different countries and sectors have used wargames in different ways, and with varying attitudes towards the activity. The German military, for example, having pioneered the use of *kriegsspiel* in the 19th century viewed wargaming as

indispensable to tactical, operational and strategic planning. Count Schlieffen, in architecting his eponymous plan for war with France, experimented with wargaming.[31] Similarly, the invasion of Poland in 1939, the invasion of France in 1940, the abandoned invasion of England in 1940, the invasion of Russia in 1941, and the Ardennes campaign in 1944 were all planned using wargames.[32] Additionally, in an extraordinary turn of events, as Allied forces were assaulting the Normandy beaches on D-Day in 1944, German high command were playing out a wargame of this very scenario. As the news of the landings reached the officers, 'reality had overtaken the game's hypothetical premise' and 'the German commander ordered the game to proceed, not as a game but a command tool.'[33]

As a contrasting example, take the declining fortunes of wargaming in the US in the 1950s and 60s. The industrial scale of the Second World War, combined with the destructive power of nuclear weapons, resulted in future war being envisaged not as battles involving intricate strategy, tactics and skills, but as contests of attrition in which efficient machinery of war would win the day. In this context, *kriegsspiel*, as practiced by the Germans, was foregone in favour of operations research, systems analysis and cost-benefit trade-offs, a 'new theology which buried wargaming beneath a deluge of mathematical analyses and computer simulations.'[34] One of the catalysts of this change was Robert McNamara who had been appointed US Secretary for Defense in 1961, after spending a number of years improving the operations of the Ford motorcar corporation. It is perhaps little wonder that the major conflict of this era, the Vietnam War, was 'fought as much with spreadsheets and statistics as bullets and bombs.'[35]

2.1.1 Categorising the uses of wargaming

The previous brief history of wargaming provides some idea of the context-dependent applications of wargames. This illustrates the difficulty of generalising

[31] Perla (1990), p. 41
[32] Brewer and Shubik (1979), p. 46
[33] Dunnigan (1992), p. 234
[34] Perla (1990)., p. 109
[35] Comments made by Ian Shaw at Royal Holloway University of London Geography Department seminar, 24 November 2015, referencing Gibson, James William (1986), *The Perfect War* (Atlantic Monthly Press: New York)

how they have been, are, and can be used. Nonetheless, perhaps the most the most concise attempt at a categorisation comes from Garry Brewer and Martin Shubik who summarise the uses of wargaming as:

> '...to attain a better balanced understanding of likely enemy reactions and actions; to determine beforehand how plans, procedures, and processes could fail; to pool expert knowledge from various areas of competence; to help make the abstract more concrete; to generate alternative courses of action and new information...; and to test alternatives in a simplified and well understood setting before trying to use them in a complex, poorly understood, and uncontrolled one.'[36]

Brewer and Shubik were writing primarily for a business audience, and this is evident in their use of forward-looking verbs: attain, determine, pool, help, generate, test. While none of what they suggest is incorrect, it is also not a wholly useful perspective. This is partly because their approach is too far removed from the military context which made wargames so successful to start with, and partly due to their omission of the utility of history. With this in mind, the researcher proposes the following short categorisation for the uses of wargames:

> *Wargaming can be used to understand events of the past, plan operations and organisations for the present, and explore envisaged futures.*

Although perhaps vaguer than Brewer and Shubik's definition, this reflects an attempt to draw on a wider variety of wargaming literature to encompass a broader scope. It is worth breaking the definition down and outlining its three major facets:

1 – *understand events of the past*

The vast majority of publicly available wargames, especially in the hobby sphere, concern historical battles and wars.[37] Every major epoch of warfare has been covered in gaming format, from ancient melee combat, to pike and shot, to interstate industrial conflict, to counterinsurgency. Aside from allowing those who

[36] Brewer and Shubik (1979), p. 52
[37] Sabin (2002), p. 199-200

have an interest in these settings to explore them in an interactive way, there is also something to be said for the value of learning from history. Although this thesis is not an appropriate place to debate the efficacy of historical studies, the oft-quoted George Santayana neatly sums up the sentiment: 'Those who cannot remember the past are condemned to repeat it.'[38] If you want to avoid mistakes in the future it is worth looking back to see if those mistakes have already been made by someone else and consequently how you might avoid them yourself.

To take an example, consider the Battle of Waterloo of 18 June 1815. According to gaming compendium website BoardGameGeek, some 58 different titles cover this battle, making it one of the most popular settings for wargames.[39] Players of these games can discover the dynamics of the battle and potentially experiment with counterfactual outcomes. Should Napoleon have committed more troops to overcome the British defences at Hougoumont? What would have happened if Blücher's Prussians entered the fray two hours later than they did? These are the sorts of questions that can potentially be explored with a wargame and enable players to identify where the commanders of the time may have made erroneous decisions. Although specific lessons pertinent to the warfare of the Napoleonic era do not translate to modern combat, classic concepts such as force-to-space ratios and *Schwerpunkt* transcend technological differences and are as applicable today as they were historically.[40]

In a non-military setting the utility of historical wargaming should not be discounted. Consider a situation where a large company wants to mount a merger or takeover of a rival. One potential tool of value here could be to conduct a game of a failed past merger, for example Kraft Heinz's aborted $143 billion takeover of Unilever in February 2017, to closely understand why that deal broke down.[41] Assuming there are enough similarities between the game scenario and real life (industry area, size of companies etc.), there are likely to be direct lessons which can be applied in the real-world situation. On a more general level, perhaps for

[38] Santayana (1906), p. 284
[39] BoardGameGeek website
[40] See, for example, the use of Lanchester's Laws in Adams and Mesterton-Gibbons (2003); or Taylor (1974)
[41] Buckley and David (2017)

business students, such a game might be used to explore overarching ideas and concepts – the corporate equivalents of force-to-space ratios and *Schwerpunkt*. George Kurian attests that Japanese businesses have used such ideas, specifically Lanchester's Laws, to study business competition and competitive advantage.[42]

2 – *plan operations and organisations*

The earlier mentioned historical examples, particularly from the Second World War, are illustrative of the uses of wargames for military operational planning. Wargames that are accurately modelled on real military units and operating environments can allow commanders to play through an envisaged manoeuvre and evaluate its success. Multiple iterations of this enable an optimal plan to be formulated based on which decision permutations produced desirable outcomes. Of course, the accuracy of the game is pivotal to the applicability of this method, because if the game inaccurately models the real world the in-game outcomes will not be replicable in real life (see Sections 2.3.1 and 2.3.3 for further discussion).

A notable example to demonstrate this tenet comes from the Gulf War. As news of Iraq's invasion of Kuwait broke, 'one of the first thing Pentagon officials did was to wargame out the unfolding situation.'[43] Based on their findings from this game, the officials could predict the disposition of Saddam's forces and consequently work out their subsequent reactions. Operations Desert Shield and Desert Storm resulted from this.

For organisational planning purposes we can again consider a non-military scenario. If a company is seeking to expand it may have a choice of investing money into research and development to create new products or reach out to new geographical territories to find new customers. The first option puts an emphasis on hiring scientists, engineers and designers, while the second option favours sales and marketing staff and office managers. It is entirely possible to conduct a game around this situation, perhaps exploring the consequences of making the opposite decision – i.e. hiring business staff while focusing on R&D or hiring product staff while focusing on new territories.

[42] Kurian (2013)
[43] Dunnigan (1992), p. 234

It is notable that the organisational planning principles apply equally in the military context. Commanders with limited budgets need to make decisions about their force composition. Should they procure new submarines at the expense of combat aircraft? What ratio of airborne to mechanised infantry brigades do they need? The answers to such questions will depend on the posture of the force and its current and future missions.[44]

3 – *explore envisaged futures*

The whole point of planning is that it is done for the future. You cannot plan for things that have already happened or are happening – this is reacting. Planning tackles events and situations that will or may happen. Wargames provide powerful tools for devising and exploring these futures. Put simply, a future-looking wargame would model the world as it is now, then remove or add one or more components depending on how the future is envisaged. As an example, a naval strategy game set in 2030 would model British forces in line with the expected commissioning and decommissioning schedules of current vessels. As such, several ships will have left Royal Navy service, but two new Queen Elizabeth Class aircraft carriers will be operational, significantly altering the makeup of the UK's naval forces – and, in the words of the 2015 Strategic Defence and Security review, 'transform[ing] the Royal Navy's ability to project our influence overseas'.[45]

An alternative use of wargaming futures is to ascertain how to get from where you are now to where you want to be. Continuing the business example from above, the company might decide that in ten years' time it wants to have launched four new products and gained a foothold in two new geographical markets. This is their desired future model of the world. The current model is represented by their present products and markets, as well as their organisational makeup. Getting from the current model to the future model will require a number of decisions along a timeline, each of which can have different consequences, opening up new decisions while shutting off others. In this

[44] Which is part of the rationale behind publications like the UK Ministry of Defence's *Global Strategic Trends* report (2014)
[45] HM Government (2015), p. 30

scenario the company will have to hire staff both for the product and business functions, but which should it do first? If it hires a load of engineers it will create new products but might miss a window of opportunity where a rival moves in and dominates a target market, closing this off. A game can be created based on a series of decision points that allows the company to play through and make decisions to see what the outcome is. If the outcome aligns with the desired final model, these decisions should probably be emulated in real life. If the outcome does not align with the desired model the company will have to either revisit some of the decisions or adjust their expectations in line with what the game suggests can be achieved.

2.1.2 Futures and anticipation

Continuing with the final facet of the definition developed above, the various ideas surrounding futures resonate through much of the relevant literature, even from disparate disciplines. This section ties some of these threads together to provide an overview of how wargaming, in its multitude of manifestations, concerns futures.

Imagining futures

The future is an uncertain time, and the further into the future we attempt to look the more uncertain it becomes. Where uncertainty reigns, imagination thrives, and several strands of literature pick up on the theme of imagining futures. In his study of competitive chess, Gary Fine asserts that 'the line' – the player's planned moves that constitute a strategy – is the core mechanic in chess, not the moves themselves.[46] Planning, of course, requires an ability to imagine the context in which future moves are made, which in chess (and other antagonistic games) includes anticipating the other player's strategy.[47] By contrast, in the context of emergency exercises which Ben Anderson writes about, the anticipated future is 'assumed to be "unimaginable" or "incalculable".'[48] This is of course hyperbole,

[46] Fine (2014), p. 323
[47] Ibid., pp. 328-329
[48] Anderson (2010), p. 229

because the future is indeed being imagined and calculated – it would not be possible to design and run an emergency crisis exercise without developing an idea of the potential causes and impact of an emergency. Anderson is concerned with exercises relating to events of terror, which are particularly detestable and deplorable, but not unimaginable. The moves on a chess board are innocent and harmless compared to the death and destruction associated with terrorism, but both the game of chess and emergency exercises require an imagined future to be constructed.

This is also the case in a broader political sense. Pericles of ancient Athens was an early master of constructing and communicating political futures. A Periclean future was 'drawn from existing reality but moved beyond it' and 'its plausibility derived from its practicability.'[49] By contrast, in a more modern context, a superb biographical essay by Alexander Galloway about Guy Debord and his later-life forays into wargaming concludes with the following passage:

> For the left, the 'historical present' is one of immediate justice won through the raw facts of struggle and sacrifice. In short, the historical present is always *true*, but forever at the same time *bloody*. But the future, the utopian imagination, is a time of complete liberation forged from the mould of the most profound injustice. In short, utopia is always *false*, but forever at the same time *free*. [Italics in original][50]

In his first wargames, Debord tried to capture this struggle, but eventually he became obsessed with 'the sublimation of antagonistic desire into an abstract rulebook.'[51] This rulebook was embodied in a chess-like wargame which had more to do with military logistics than it did with political strife. Therefore, in imagining futures for wargames, unattainable Debordian utopias are likely to be less successful than Periclean rhetoric.

[49] Freedman (2013), p. 37
[50] Galloway (2009), pp. 151-152
[51] Ibid.

Actioning futures

It is imperative to keep in mind that while wargames require an imagined future, this future is not constructed for its own sake, but as something which requires action. Professional wargames are not frivolous pastimes but are intended to derive lessons that help organisations realign their structure and behaviour in order to mitigate threats and exploit opportunities that not only may, but likely will materialise. Reports from the 'Schriever Wargame' played by the US Air Force in 2010 attest to this actionability as the key outcome of the wargame. 'The lessons identified...are not futuristic concepts,' says Hon. George Foresman – stressing the immediacy of the imagined future the game constructed.[52] Similarly, General Robert Chekan attests that his team 'gained insight into real issues that we confront now and will likely confront in the future.'[53] For both Foresman and Chekan it is clear that the wargame provided a greater understanding of how their organisations should position themselves to tackle the issues brought to bear by the imagined wargame scenario. Unlike the abstractness of Fine's chess or Debord's utopia, wargames require the lessons learned to be actionable as they relate to a potentially very real future.

Indeed, actionability was a key driver in the genesis of this thesis. As outlined in Section 1.3, the original idea to research cyber wargaming came from a project conducted in partnership with a professional services firm. The researcher's contact at the firm was, at the time, on secondment to the company from their role as a senior civil servant. In this role they had commissioned a study which resulted in The Global Cyber Game report (analysed in detail in Chapter 3, Game 6), but in initial conversations with the researcher they lamented that, although interesting, such reports had limited utility because they lacked actionability. From the researcher's efforts they were therefore exceptionally keen to see something tangible and actionable that people could get their hands on and use.[54] Although the firm did not play any role in the remainder of the thesis beyond the progenitor stages, the game design presented in Chapter 4 and results discussed in Chapter 6 hopefully fulfil the actionability brief.

[52] Foresman (2010), p. 8
[53] Chekan (2010), p. 16
[54] Author telephone conversation with firm contact, 26 May 2015

Anticipating futures

Where some literatures refer to imagining and actioning futures, others refer to anticipation. Anticipation can be considered a combination of imagination and action – envisaging the effects of a future and reacting appropriately. In a paper on using geodesign to model and simulate wildfires, David Hulse et al draw close links between anticipation and surprise.[55] They conclude that modelling can help address surprise in two ways:

> '1) when and where surprising departure from expectation is due to events, to actions, or to the unanticipated interplay of both;
> 2) when, where and how "reducible ignorance" can be most effectually reduced vis-à-vis anticipated surprises.'[56]

As established in Chapter 1, wargaming is fundamentally concerned with modelling and simulation, so these findings are entirely applicable to wargaming. Indeed, understanding or reducing surprise through anticipation can be considered a key use of wargames. Because wargames involve human participants experiencing events, players gain insight into the source of surprise similar to the first finding above (see Sections 2.2.1, 2.2.2 and 2.2.5 for further discussion). Furthermore, as an introspective learning activity, players can identify gaps in theirs and others' knowledge and seek ways to bridge these gaps. Vincanne Adams et al have even gone so far as to claim that 'anticipation is not only an epistemic orientation towards the future, it is also a moral imperative.'[57]

While this thesis makes no claims about the ethics of creating knowledge, it is clear that anticipation is closely related to subjectivity and emotion. In everyday parlance this is evident through how we often think of surprise as a positive or negative feeling – being pleasantly or unpleasantly surprised. Roy Baumeister et al provide the additional insight that 'anticipation of emotion is more important

[55] Hulse et al (2016), p. 27
[56] Ibid, p. 41
[57] Adams et al (2009), p. 254

than the actual emotion' for driving human behaviour.[58] These are findings which help inform the uses of wargaming because games are closely linked with competition and personal performance (see Section 2.2.4), so understanding the imperatives that cause people to act, or not act, provides foundations for analysing player behaviour.

Preventing vs. enabling futures

As related to this thesis, there seems to be some dissonance in the futures literature between pessimism and optimism, and a disjunction between tactics and strategy. Anderson, for example, focuses on pessimism and tactics. He writes: 'the aim of security is, supposedly, to control and manage the future, ensuring that an event does not come to pass.'[59] The focus here is on preventing a single negative event from occurring. The idea of prevention is pessimistic because it presupposes that something bad will happen, while narrowing the scope to an event is tactical because it does not take into account the bigger picture. The 2016 UK Cyber Security Strategy, on the other hand, is comparatively optimistic and strategic (as the name implies). It is optimistic because in its attempts to ensure security and prosperity it is enabling rather than preventative, and it is strategic because it draws upon a wide gamut of society to achieve its goals while being situated in a larger context.[60] This is not to say that either approach is more correct than the other, but merely to recognise that there are different approaches to the topic of futures.

Wargames can fall anywhere on this spectrum depending on how they are designed and the learning outcomes desired. It can be difficult to envisage a truly optimistic enabling game, as games usually have a set endpoint after which the future the game imagines effectively ceases to exist, and therefore any decisions and achievements made within the game are rendered moot. This is not representative of the real world which, of course, does not have a set endpoint but continues onward uninterrupted. To reflect this, a game would likewise have

[58] Baumeister et al (2007), p. 174
[59] Anderson (2010), p. 228
[60] HM Government (2016), p. 9

to continue ad infinitum. While this falls outside the scope of this thesis, organisations like the US Department of Defense have the resources and capability to run such games. The National Decisionmaking game, for example, uses players from Reserve Officers' Training Corps (ROTC) programmes to model 193 countries spanning a 50-year timeframe. Any time conflict arises, the situation is turned into a wargame, 'complete with a "history of the future."'[61] This is perhaps the ultimate wargame solution, combining prevention, enabling, strategy, and tactics to allow players to shape the future according to what they envisage, whether that is pessimistic or optimistic.

Cyber futures

Finally, although futures are imagined, they are not merely conjured from nothingness. Instead, knowledge and understanding of the present is used to extrapolate what the future might look like. Writing about wargaming during the Cold War, Sharon Ghamari-Tabrizi asserts that 'the technical horizon within which future wars would be fought would change constantly, albeit uncertainly.'[62] While this is true to an extent, a more accurate assessment (made with the infinite benefit of hindsight) is that Cold War wargaming was based on a future that had already arrived, and which would only evolve incrementally. Although the destructive power of nuclear weapons increased and their delivery mechanisms became more sophisticated, the overall character of these weapons remained unchanged (and does so to this day).

By comparison, the future of cyber weapons and cyber security is very much in an embryonic stage.[63] Although we have seen glimpses of what cyber capabilities might look like – for example the Russian attack on Estonia in 2007, the Stuxnet operation of 2010, or the NotPetya malware of 2017 – there is real difficulty in predicting the character of future cyber capabilities. It may be entirely possible that cyber capabilities have plateaued like nuclear ones and we will not see new technologies beyond incremental improvements in levels of destruction or

[61] Garretson (2015)
[62] Ghamari-Tabrizi (2000), p. 164
[63] Brangetto et al (2015), p. 18

sophistication of delivery mechanisms. On the other hand, it is also likely there are things to come which no one can foresee. Imagining the cyber future is therefore very difficult and represents a particularly thorny, if satisfying, challenge for wargame designers.

2.1.3 Skills

Much of the literature surrounding wargames points out the lessons learnt from games that have already been played, particularly cyber defence exercises. These can be categorised in terms of the takeaway skills that have been developed by participants in the game, or areas where skills are deficient and need to be cultivated. This section will explore these partly with a view to postulating what kind of lessons may be derivable from the wargames used in this thesis, and partly to determine where the focus has been so far, thereby demarcating where there is scope to make original contributions.

Networking and communication

Wargames in which players can collaborate to achieve goals allow players to forge connections they might not otherwise have, and transfer knowledge and ideas across departments and domains. On a theoretical level it has been postulated that massive multiplayer online games engender skills 'closely parallel those required by a military transforming itself to operating under the concept of network centric warfare.'[64] Although the hype around network-centricity has abated from its heydays in the 1990s, cyber may well provide an environment where this concept is worth revisiting. On a practical level, evidence from the Schriever Wargame and others suggests that the social aspects of wargames are fulfilling important functions. General Chekan attests that Schriever allowed his team to 'establish both connections and even friendships' that would allow them to progress with inter-departmental integration.[65]

[64] Bonk and Dennen (2005), p.
[65] Chekan (2010), p. 17

From another US Department of Defense wargame, two key lessons about communication were identified: firstly, a need for a 'common lexicon in relation to cyber', and secondly that there are 'barriers to cooperation...hampering information sharing.'[66] With regards to the latter, the experience of Chekan demonstrates that such barriers can be negated through further wargame participation. As to the former, the challenge appears to be a semantic one that can be ironed out through continued collaboration and communication. Networking (in the human sense), is the best way to overcome such challenges, and wargames provide structured environments in which to build these links and relationships. (See Chapter 6 for examples of participants in this thesis establishing personal connections through a game, particularly to enable peer-didacticism and knowledge exchange as in Sections 6.2.1 and 6.2.5)

Deterrence

Very much related to the need for inter-departmental networking and relationships is communication on an international level. Specifically, the Schriever Wargame demonstrated that traditional assumptions about deterrence do not translate to cyberspace.[67] Deterrence strategies are built on a combination of directed policy statements and signalling through force composition and posture. Effective deterrence relies on communicating one's intentions to a perceived adversary. The Schriever Wargame highlighted that these tools and methods are lacking in cyberspace.[68] If cyber intentions cannot be communicated, there exists a real risk of unrestricted escalation with the potential for conflict. International communication skills are therefore a paramount requirement in order to avoid major military cyber confrontations.

In recent years, the cyber deterrence debate has transitioned from theory to practice. In particular, the 2016 UK National Cyber Security Strategy contains an explicit focus on deterrence, with some eight pages (14 percent) of the content devoted to this concept.[69] Despite such lengthy treatment, the Strategy still seems

[66] Purvis and Forsythe (2013), p. 6
[67] Helms (2010), p. 12
[68] Dahm and Silkowski (2010), p. 38
[69] HM Government (2016), pp. 46-53

to suffer from the problems of communication highlighted in the Schriever wargame some six years prior. As an example, one of the pivotal problems of cyber deterrence is the problem of anonymity which creates uncertainty and undermines credibility. The Strategy states that one of its approaches to countering hostile foreign actors is to 'attribute specific cyber identities publicly when we judge it in the national interest to do so.'[70] This suggests that the UK has some sort of technical capability to identify actors in cyberspace, effectively overcoming the problem of anonymity. Although certainly positive, there are two key caveats which must be taken into account, both relating to the issue of transparency. First, because this technical capability is merely a conjecture publicly, there is no way for the UK to provide proof of their attribution without giving away the secrets of the technology. As long as attribution remains unsubstantiated it is little better than finger-pointing. Second, judging what is considered to be 'in the national interest' is highly transient and difficult for outsiders to predict. Using this as the criterion for disclosing attribution does not promote certainty nor credibility.[71]

Scale and speed of reaction

The ubiquity of computer networking and rate at which signals can travel along fibre optic cables makes scale and speed the hallmarks of the cyber domain. Humans managing cyber operations and equipment therefore need particular skillsets tailored to this expansive, fast-paced environment. Participants in both the wargames referred to above provide evidence that the effects of a cyber attack will not be constrained to a single geographical locale, but have a global impact.[72] Commanders faced with the decision to launch cyber attacks therefore need to be equipped with a broad understanding of geopolitical situations in order to fully comprehend the potential ramifications of their decisions. Simply understanding the tactical situation is not enough; the wider strategic picture must also be kept in mind.

[70] Ibid., p. 50
[71] This argument has previously been made in Haggman (2018)
[72] O'Shaughnessy et al (2010), p. 32; Purvis and Forsythe (2013), p. 6

The speed of reaction required to respond to events in cyberspace is often beyond human capabilities. A human cannot gather, interpret, and act on the data which constitutes a cyber attack as fast as a computer can. Even when the data is collated by a computer and presented to a human in the form of a decision-making point, this decision is likely to come too slowly. Owing to this, Werner Dahm and Eric Silkowski assert that the Schriever Wargame showed that 'cyberspace will demand increasingly autonomous capabilities.'[73] From the point of view of this thesis, the requirement for autonomy demonstrates that a board wargame which attempts to simulate a tactical cyber engagement is pretty moot, and it is instead better to focus on the higher strategic level, where human decisions still reign.

Self-learning

On a more general level, wargaming can enhance players' capacity for auto-pedagogy. This means that players identify their own learning outcomes and evaluate whether these were achieved, plus any remedial steps necessary. Nina Wilhelmson and Thomas Svensson say these skills can be embedded within the game design process by involving players from the outset.[74] This certainly seems to echo established norms in wargame design, where games are constructed bottom-up with the learning objectives as basis. One caveat to keep in mind with this approach is that players may be able to anticipate events during the course of the game because they had specifically requested them to be included, which can negate the impact these events were intended to have. The extent to which the design of the game is player-led is therefore a balance.

Perhaps the most glaring vindication of the usefulness of wargaming for self-learning comes from Robert Specht, who says that 'the player teaches himself in a manner more convincing than any lecture can possibly be.'[75] Wargames go beyond mere showing and telling, instead employing the idea of learning-through-doing. There are few more powerful pedagogical tools than the ones where

[73] Dahm and Silkowski (2010), p. 40
[74] Wilhelmson and Svensson (2013), p. 19
[75] Specht (1957), p. 12

participants actively engage with the material in a highly sensory way that provides instant feedback on their performance. In the words of Graham Longley-Brown: 'I hear I forget; I see I remember; I do I understand.' [76] In this sense, wargaming is not quite Pavlovian, but it is certainly very effective.

2.1.4 Play and playfulness

Despite, or perhaps because of, the capacity of wargaming to generate tangible benefits in the form of learned skills, the relationship between wargaming and ideas of play have historically been fraught. How different wargaming communities employ terminology is emblematic of this schism. Professionals tend to use the separated "war gaming" while hobbyists prefer the contracted "wargaming" (with the hyphenated "war-gaming" also occasionally making an appearance in both camps). The reasons for the dichotomy are not entirely evident, but Perla postulates that it may have something to do with professionals seeking to distance themselves from the jovial 'gaming' aspects of the activity.[77] Physically separation of the words leads to a logical separation the professional domain (war) from the playful domain (gaming). It would be a mistake, however, to wilfully introduce distance between wargaming and play, for two reasons.

Historical links between war and play

First, war, the activity at the heart of wargaming, has strong historical linkages to play. Philosopher John Gray, interpreting the writings of Homer, posits that in ancient Greece war was a sporting activity filled with rivalry and glory.[78] Similarly, historian John Lynn has pointed out that in medieval times, chivalric ethos dominated warfare and concepts of courage and honour were boasted in tourneys, organised – as a display of war – for this purpose.[79] Even Aristotle found need in his *Nicomachean Ethics* to address the question of frivolity in war, although he disagreed that is has playful content, concluding that war has no

[76] Comments made by Longley-Brown at Connections UK conference, 8-10 September 2015, King's College London
[77] Perla (1990), p. 2
[78] Gray (2003), p. 182
[79] Lynn (2003), p. 93

place for leisure because war is a means to an end, not an end in itself.[80] Gray tentatively supports this position, building on his earlier argument by concluding that 'wars are not fought to stave off boredom….but once it is underway, war is often embraced as a release.'[81] Gray's point is that although wars are started for serious purposes, their conduct 'has become another entertainment'[82], perhaps a reference to the Gulf War which because of its extensive television coverage has been called the 'first Nintendo war.'[83]

The point, then, is that while war is a very serious activity – quite literally a matter of life and death – it nonetheless contains elements of playfulness such as sporting or entertaining qualities. To deny the links between war and play therefore does a disservice to war, because it removes essential elements that help us better understand war as a phenomenon. The reader will note that this thesis uses the contracted "wargaming", partly as an attempt to maintain the close links between war and play.

Applicability of ludology to wargaming

Second, concepts of play can do much to inform wargaming practice. As established at other points in this thesis (Section 2.2.2), wargaming is fundamentally a study of human events. Scholars of play have long used ludological lenses to study the human condition, of which war and conflict are an intractable part, so it is prudent to draw on this material when analysing the uses of wargames. One of the earliest recognised pioneers was Dutch cultural historian Johan Huizinga, whose seminal *Homo Ludens* opens with the assertion that playing games has a '*significant* function' [italics in original] in shaping society and culture.[84] He proceeds to argue and illustrate how play has influenced many fundamental aspects of humanity, from epistemology to law to art. With regards to war, Huizinga finds it inexorably linked with play: 'Ever since words existed for fighting and playing, men have been wont to call war a game.'[85] This is not mere

[80] Aristotle (2004), p. 271
[81] Gray (2003), p. 183
[82] Ibid.
[83] Huntemann and Payne (2010), p. 6
[84] Huizinga (1949), p. 1
[85] Ibid., p. 89

linguistic gymnastics, however, as human behaviour in war has been shaped by ludological practices – notably in the idea of judicial duels which are rooted in the same chivalric ethos Lynn referred to.[86]

In these general senses, we can use Huizinga's writings to inform our understanding of player behaviour in wargaming. If wargames emulate war, players are likely to act in war-like manners while playing the games. Moreover, these behaviours stem from humanity's roots as a playing animal. Of particular relevance, Huizinga notes how competition, 'the innate desire to be first', drives people to conflict.[87] This directly ties in with modern ideas that seek to harness this competitive spirit to fuel creativity and innovation (see Section 2.2.4).

Another ludological practitioner and writer is Bernie de Koven, who is less celebrated – indeed largely unreferenced in wargaming literature – but no less relevant. A central figure in the New Games Movement which flourished in the US in the 1970s, de Koven made singularly effective use of games and play in his career as an educator, which he documented in *The Well-Played Game*.[88] In the book, de Koven draws on his extensive experience to analyse what prompts people to create, start or join games, to avoid games, to end games, and to change games for greater enjoyment.

A central theme to de Koven's book is that player participation in games is ultimately individualistic. Even in team games and sports, what prompts players to join and actively take part is that they see a way for themselves to play the game in a way they want to. Consider the (real) example of the girl who refused to play hide and seek until she had sufficiently acclimatised to the playing group through distant observation and decided it was safe to join[89], or the (hypothetical) example of a volleyball player who grows tired of following the rules and so changes them, with the permission of the other players, to suit their desires at that particular time.[90] What is being demonstrated here is closely aligns with the

[86] Ibid., pp. 91-95
[87] Huizinga (1949), p. 101
[88] de Koven (2013)
[89] Ibid., pp. 71-73
[90] Ibid., pp. 41-42

advantages of wargaming, particularly the principles of safety (Section 2.2.7) and flexibility (Section 2.2.6).

The intent of this discussion has been to illustrate that concepts of play and playfulness have received thorough treatment in disparate literatures, ranging from philosophy to history to cultural studies. These literatures show that the idea of play cannot be separated from war and therefore should not be separated from wargaming, and that treatises on play can provide new lenses by which to analyse aspects of wargaming.

2.2 Advantages of wargaming

The uses of wargaming, as specified with regards to futures and skills, are not necessarily unique to wargaming. Other analytic and pedagogical activities can potentially be used to achieve similar outcomes. However, the literature reveals that wargaming confers a number of advantages over alternative methods.

2.2.1 Advantages over computers

Given the growth in availability of computers and their processing and graphical power, astute commentators will question the choice to create a manual game as opposed to a computer game – particularly for this thesis where the topic of the game is cyber security. There are certain things computers are more capable of doing than humans, particularly complex calculations and computations. Computers are also more flexible when it comes to graphical display, being able to manipulate digital images to suit the needs of the game, as opposed to the relatively static display offered by paper. In the inaugural 1981 issue of *Computer Gaming World*, Chris Crawford presciently outlined five capabilities which distinguish computer wargames from board games: performing more extensive and realistic calculations, limited intelligence (visibility and knowledge), solitaire games against computer opponents, real-time play, and networked multiplayer

games.[91] Almost 40 years later, these capabilities have been realised many times over and can readily be seen in commercial computer wargames in various genres, from the grand strategy game *Hearts of Iron* to the first-person shooter *Call of Duty*. Despite some clear benefits, however, there are good reasons for choosing a manual game over a computer game, as elucidated in the following sections.

Inaccessible mechanics

Computers, though easy to access and use, are not simple mechanically. Getting to grips with the internal workings of computer hardware and software requires a significant degree of technical knowledge and understanding. To those without these skills, the operations of the computer remain shrouded in mystery. A manual wargame is built as a fully-accessible system, where all the information is available to the players, including rules, procedures, numbers and probabilities.[92] In a computer wargame this is largely hidden from the player. The downside of this is that the player does not know why the game behaves as it does, which in turns limits the learning potential of the game. This is especially true of 'pre-play analysis' where the players scope out the game's various aspects in order to understand how it works before actually playing the game.[93] In order to fully utilise the pedagogical dimensions of wargaming, it is therefore often better to design and play a manual game rather than a computer game.

Modifiability

Following on from this, without easily accessible mechanics, computer wargames become very difficult to modify. Once the game has been created its rules, procedures, numbers and probabilities will remain constant as determined by the game developers. The players have no opportunity to make their own changes to fit their needs. Changes might be needed to reflect changes in the real world, or

[91] Crawford (1981), p. 4
[92] Dunnigan (1992), pp. 64 and 174
[93] Ibid., p. 63

to adapt the game to different training needs.[94] Part of the allure of manual wargames is that players can adapt game parameters as required, even mid-game. With a computer game this would have to be done by the developer on request of the players, incurring both time and monetary costs.

Alternatively, a developer might anticipate, or the customer requests, that parameters need to be changeable and build this function into the game's interface. However, as Sabin points out, the computer game developer thereby becomes a gatekeeper to the game mechanics, preventing modifications 'beyond those explicitly allowed for by the designer.'[95] It could also be contended that such solutions suffer from problems of scalability. Changing a few parameters may be simple (for example the amount of starting resources or the destructive capacity of a weapon), but to be truly modifiable, every parameter and every algorithm needs to be changeable. With a board wargame this is as simple as grabbing a pen and making edits to the rule sheet. With a computer game, however, even if the interface is designed to enable modifiable algorithms, the user would likely need to understand the principles of constructing an SQL query to utilise it.

Affordability

In this way, manual wargames are also more affordable than computer games. The initial development of a computer wargame, involving extensive consultations with a professional game design and programming team, can drive costs to six-figure sums and beyond, to which must be added the costs of 'constant fine-tuning to make it relevant to emerging scenarios.'[96] A manual wargame, on the other hand, while it might require the consultation of a professional to create it, does not come with the same attendant costs, either in initial production or subsequent adjustments. Another aspect to this is of course that manual games are played on paper game boards using paper or plastic game markers and dice. These are orders of magnitude cheaper than computers, even low-specification

[94] Curry and Price (2013), p. 12
[95] Sabin (2012), p. 27
[96] Kainikara (2003), p. 16

ones. The investment required to get a working wargame is therefore much less with manual games than computer games.

Compatibility

In the same vein, manual wargames do not suffer from any compatibility issues, as a computer wargame might.[97] A wargame created for a particular computer configuration is not necessarily transferrable to other computers or may cease to function if the configuration changes. The repercussions of this is that a computer wargame can potentially have limited applicability, only being usable by the organisation which originally commissioned it and this only being the case for a finite amount of time. For example, a game created for the Air Force might not be usable by the Navy because they have different computer specifications, and the Air Force can only use it until such time that they perform a system update which relegates the game to legacy software. Paper and dice are unaffected by this, being self-contained and not reliant on any additional hardware. With computer games having such short shelf-lives compared to the indefinite lifespan of manual games, Sabin estimates that 'the entire corpus of board wargames outnumbers currently accessible computer game titles by at least a factor of ten.'[98]

Human expertise

Finally, in the process of replacing human ingenuity with computer processing power as the adversary in a wargame, a lot of the finesse of wargaming is lost. Conflict is, at heart, a human activity, replete with quirks and foibles which are beyond the grasp of a computer game. In the past three decades computers have bested humans at certain conflict games like chess – notably IBM's Deep Blue versus Garry Kasparov in 1997[99] – and more recently Go – Google's AlphaGo versus Lee Sedol in 2016.[100] However, a well-designed wargame does not lend itself to being playable by an algorithm, no matter how complex or powerful. Jim

[97] Curry and Price (2013), p. 12
[98] Sabin (2012), p. 25
[99] See, for example, Marshall (2014)
[100] For example, Ormerod (2016)

Dunnigan writes that despite advances in artificial intelligence, these 'routines usually have problems with strategy and are not quick to catch on to changes in the big picture.'[101] This observation precedes the feats achieved by Deep Blue and AlphaGo, yet is not invalidated by these events, even if the terminology "routines" is somewhat outdated. In a tactical engagement the computer may be able to crunch numbers better than humans, a point emphasised in James Somers' explanation of Kasparov's defeat, but it still has a hard time planning a long-term strategy and dealing with unexpected variables.[102] It is in these situations the power of the human brain becomes evident – the ability to create and innovate. With computer wargames, the creativity and innovation which underpins game design and play can be diminished or lost, yet it is these facets which provide the most striking learning opportunities.[103] In adversarial settings, a manual wargame is therefore preferred to a computer one, because we still rely on human expertise computers simply cannot match.[104]

With regards to the limitations of computers, a singularly insightful and provocative remark which neatly summarises this section comes from an unlikely source: Pablo Picasso. In conversation with William Fifield, Picasso reportedly said of computers: 'But they are useless. They can only give you answers.'[105] This is an important point which will be returned to later (Section 2.3.3).

2.2.2 The human factor

The point about human expertise is significant because it indicates the very core of what wargaming is about. The optimal use for a wargame is not to test a specific strategy or tool, but to test the people in charge of implementing the strategies and tools. Whatever the granularity of a wargame, it can never simulate the real world with complete accuracy, yet the people who partake in the game are the same as they are in the real world. In this way, wargaming is, what Perla calls 'an imperfect mirror of reality, reflecting it best in the decision-making

[101] Dunnigan (1992), p. 65
[102] Somers (2013)
[103] Brewer and Shubik (1979), p. 52
[104] Herr (2015)
[105] Fifield (1982), p. 145

processes of its players.'[106] Wargaming is about exploring different paths through scenarios, but the final outcome of a game is perhaps less important than the process of getting there. Wargaming is a participatory activity where human action and interaction is central to the experience, and it is this experience which is one of the most important things a wargame can offer.[107]

Interactions between humans provide some of the most dynamic and unpredictable situations in life and ensure that no two iterations of a wargame are alike.[108] In Go, for example, the number of possible moves famously exceeds the number of atoms in the universe.[109] Through the course of a wargame, players make decisions that affect other players, creating a complex chain of interdependent decision-making cycles. Though this can result in a confusing web of interactions, wargaming 'forces participants to think hard about a problem – hard enough...to make the elements of the problem explicit and logically consistent.'[110] Wargaming challenges players to think clearly about issues and provides insights into that which was previously obfuscated. Few other activities can have this effect, especially not at the same time as allowing the people making decisions to play them out and live the experience.

Here we see the limitations of an alternative approach to problem solving: game theory. Game theory breaks constituent parts of a problem down into mathematically definable elements, and then crunches the numbers to arrive at an optimal solution. Such an approach removes the unquantifiable human elements which introduce uncertainty, instead supposedly providing robust scientific answers backed up by rigorous numerical reasoning. Where game theory falls short, however, is precisely in its removal of the human element, which, as Brewer and Shubik assert, 'real experience has forcefully and repeatedly proven' to be a 'critical feature of actual operations.'[111] Scenarios involving human action, interaction, and decisions cannot be reduced to just the objective data. The subjective experience of each participant is critical in determining how events

[106] Perla (1990), p. 11
[107] Dunnigan (1992), p. 87
[108] Perla (1990)., p. 164
[109] Lei (2013), p. 2; Walraet (2016), p. 19
[110] Brewer and Shubik (1979)., p. 51
[111] Ibid., p. 57

unfold, and wargaming provides a method of integrating these when exploring scenarios and solving problems.

Indeed, historical experience has shown that pure number crunching yields only impartial or even counterproductive results. In the 1960s, the United States Joint Chiefs of Staff's 'push to reduce the role of human players in so-called "analytical" games, undoubtedly contributed to the self-deluding tendencies exhibited by many of the games played about the conflict in Vietnam and other potential trouble spots even today.'[112] Humans are at the centre of every conflict and attempts to examine and analyse these activities need to take this into account. For wargaming to be effective it should include and embrace the human element, and players should, as Dunnigan phrases it, 'get the feeling that they are participating in a study of human events, which is exactly what they are doing.'[113]

2.2.3 Cost

Perhaps the most obvious benefit of using wargaming to gain experience as opposed to mounting actual combat operations (or launching a business venture) is that it is significantly cheaper. This is in terms of money, manpower, and political investment. When testing new equipment, strategies or tactics, rigorous scientific analysis will always be costlier than a wargaming implementation. When testing new hardware, for example, the great expense with such 'realistic experimentation,' says Sanu Kainikara, stems from the need for 'building up multiple copies of devices using emerging and unproven technologies.'[114] This is perhaps especially true of the cyber domain, where the pace of technological advancement is particularly swift.

The cost-saving aspects of wargaming were enshrined in US Deputy Secretary of Defense Robert O. Work's memorandum of February 2015, in which he asserted a 'need to reinvigorate, institutionalize, and systematize wargaming across the Department [sic]' in order to, amongst other things, 'make the best use of limited

[112] Perla (1990), p. 126
[113] Dunnigan (1992), p. 54
[114] Kainakara (2003), p. 6

resources.'[115] This is ample evidence that the cost benefits of wargaming have been recognised at the highest level of policy-making.

2.2.4 Creativity

In being a participatory activity, wargaming has an immense capacity for exercising the uniquely human capability to create and innovate. In part this is because 'wargaming forces participants to look at reality from a different angle,'[116] an angle the game designer can impose, but also because 'great games capture meanings that have never been said.'[117] This leaves games open to interpretation by the players, allowing them to exercise their creative capabilities. In this way, a wargame actively forces players to escape from their comfortable reality, yet it does not necessarily provide an alternative view, instead encouraging players to imagine their own alternate realities.

The benefit of this is that players construct the reality of the game according to their particular needs, which not only helps serve the learning outcomes of the game, but also challenges stagnant visions of operations and procedures. In the words of Alfred H. Hausrath, 'Gaming challenges the competitive spirit and spurs the contenders to do their best in any given situation. It stimulates the search for new and more effective ways of meeting situations and encourages innovation.'[118] It has also been highlighted that this is particularly the case when players are drawn from decision-making echelons of organisations: 'The genius of modern professional wargaming,' says Mark Herman et. al., 'is that it...provides a methodology to get at the things that one leader, no matter how visionary, cannot grasp on his or her own.'[119] Wargaming provides an effective tool for inspiring the flow of creative juices and, importantly, provides an outlet where these juices can fuel planning, training and learning.

[115] Work (2015), p. 1
[116] Perla (1990), p. 181
[117] Perla and McGrady (2011), p. 122
[118] Quoted in Brewer and Shubik (1979), p. 52
[119] Herman et al (2009), p. 3

Other writers have noted that this also extends to the game developer. In the process of designing a game, the creator inevitably experiences many of the same things the eventual players do. According to John Curry and Tim Price, this can result in 'unexpected real world insights', which can be passed on to the players either indirectly through the game or directly through communication.[120]

2.2.5 Experience and simulation

One of the key benefits of wargaming as opposed to other forms of learning or training is that it provides a manner of *ersatz* experience of the real thing. By actively participating in the game, say Perla and McGrady in a seminal 2011 paper on the topic, players are provided with a 'story-*living* experience...more akin to real-life experience than to reading a novel or watching a video. [Italics in original]'[121] Simply having a scenario, and its outcomes, relayed to you, whether it is by text or imagery, through a second-party is never as engaging or effective as the first-hand experience.[122] Additionally, traditional learning materials such as textbooks and instructional videos are relatively static, having been created at a certain point in time for a certain purpose. Wargames are updateable in real time as they are played and, because they centre on human participation, no two games are the same. Because of this, wargames 'can help enlighten players about that fact that unexpected and unpredictable events, including embarrassing ones, do happen and that there are real consequences when they do.'[123]

Making wargames come to life in this way turns them from models into simulations. Most simply defined, simulations are models exposed to time.[124] Whereas a model is a static representation of a system, a simulation represents the moving operations of the system and how it changes as it is exposed to conditions. An Airfix plane is a model; placed in a wind tunnel it becomes a simulation. Wargames, of course, are potentially more complex simulations than pure scientific experiments (such as wind tunnels) because they involve human

[120] Curry and Price (2013), p. 15
[121] Perla and McGrady (2011), p. 112
[122] Sabin (2016), p. 424
[123] Perla and McGrady, op cit., p. 122
[124] Halter (2006), p. 9

participants whose behaviour is not predictable in the same way physical objects are.

Because humans are the agents of change in a wargame, it makes sense for the focus of study to be the participants rather than the game itself. As established in Section 2.2.2, the human is the magic ingredient to a successful wargame so it would be a mistake to relegate them to mere input into the system, only for their part to be churned over and a game outcome produced (although sometimes the outcome is also important). That churn is the key function where players derive value from a game because they experience the process in a lifelike way, with attendant unpredictable events and consequences.

The point about consequences is important because consequences are the results of decisions. If the world was entirely predictable there would be no need to make decisions as the path of experience is known *a priori*. This is, of course, an absurd logical inconsistency and much of our experience of the world is entirely unpredictable. The burden of decision-making thrust on people thereby becomes a heavy one, for they cannot necessarily see what path the decision will lead down. A very accurate wargame may help illuminate some of these paths, but more importantly, a wargame will allow the player to actually make decisions, not merely imagine them. As such, 'games give players active responsibility for their decisions, similar to what they would experience in the real world, and force them to bear many of the same consequences of those decisions, both positive and negative.'[125] Through exploring, repeating and reflecting on decisions, players gain actual experience that cannot be attained by reading a book or watching a video.[126] It is here that one of the key benefits of wargaming is revealed.

2.2.6 Flexibility

Following on from the preceding paragraph, wargaming is an ideal way to tackle the complexity of the real world. Without belabouring the point, it must be emphasised that the human experience is only consistent in that it is inconsistent.

[125] Perla and McGrady (2011)., p. 113
[126] Ibid., p. 112

No two lives lived are the same, nor are any two given days, and varying contexts provide width and depth to the complexity of the world. That wargaming is the right tool to meet this challenging environment has been frequently reiterated.[127]

It has already been argued that attempts to reduce the world to mathematically rigorous components are futile, and wargaming should be recognised as a superior method for analysing events, processes and people. This is because, unlike strictly scientific approaches, wargaming affords a great degree of flexibility in how it is applied. Wargames come in a huge variety of shapes, sizes, and configurations, all of which can be adapted as the situation requires. In his wholehearted endorsement of wargaming, Work makes this point very well: 'When done right, wargames spur innovation and provide mechanisms for addressing emerging challenges, exploiting new technologies, and shaping the future security environment.'[128] The key words here are "innovation", "emerging", "new" and "future", all of which indicate the complexity of the modern world. At the same time, however, the verbs "spur", "addressing", "exploiting" and "shaping" all show how wargaming is ably equipped to deal with this complexity, even taking advantage of it. No other learning tool has this capability.

2.2.7 Safety

The final benefit of wargaming analysed here is that of safety. Wargaming can take place almost anywhere, from business boardrooms to the hobbyist basements. The one place it does not take place, however, is on the actual battlefield. As such, wargaming is devoid of the actual dangers of conflict. Though initially counterintuitive, on reflection it is perhaps little wonder that H. G. Wells, an ardent pacifist, was the progenitor of the wargaming hobby. After all, only wargaming could provide 'a harmless setting in which human beings could face some of war's challenges without destroying lives, property, or nature, but also taught something of the reality of Great War to those not familiar with its

[127] For example Kainakara (2003), p. 17; Work (2015), p. 1; Perla and McGrady, ibid., p. 125
[128] Work, ibid.

practice.'[129] In the business world the benefits are very much the same, allowing players to '"experience" the future in a risk-free environment.'[130]

Wargaming is an activity which provides safety not only from mental and physical trauma, but also from the adverse effects of a wrong decision. Without the attendant real-world repercussions, players can be encouraged to explore paths they may otherwise have been loath to go down, enabling 'behaviours that might not occur in the real world – after all, "it's only a game."'[131] This attitude, if taken in a serious vein, is key to getting the most out of the learning experience of a wargame. The thrill of a reckless charge ending in bloodbath or the exhilaration of a wild investment gone awry can be acted out without costing the lives of the Light Brigade or a plummeting stock price followed by summarily joblessness. In short, to borrow the Perla's phrasing, wargaming 'provides an opportunity for glory without gore and defeat without destruction.'[132]

2.3 Limitations of wargaming

For all the advantages contained within wargaming, the activity is not without limitations. Outlined below are a number of facets that should be taken into account when evaluating the utility of a wargame as an educational tool.

2.3.1 Abstraction

Wargames are imperfect reflections of reality. If they were perfect reflections they would *be* reality, thereby negating many of the benefits analysed above. Depending on the accuracy of the reflection, the games become more or less abstract. Abstraction can make a game more accessible, but there are also repercussions, particularly when it comes to post-game analysis. The complexity of analysis is in fact proportionally related to the amount of abstraction in the

[129] Perla (1990), p. 179
[130] Herman et. al. (2009), p. 4
[131] Perla and McGrady (2011), p. 120
[132] Perla, op. cit., p. 4

game, and as the amount of abstraction increases so does the difficulty of learning the desired lessons from the game.[133]

There is also a stringent need to ensure that players understand that the game is an abstraction. There are dangers contained in conflating the game and reality, especially for players who have limited experience of the activity the game represents. In this way, attests Perla, the 'illusion can be a powerful and sometimes insidious influence' and it is imperative to offset the realism of the game with realistic appreciations of what the game both is and is not.[134]

The lack of actual experience can become a problem especially regarding cyber. Given that there are a limited number of publicly analysable cyber operations on which to base wargames, cyber games are to a larger than normal degree based on conjecture and extrapolation. This lack of a 'solid foundation of metrics gained from actual combat operations' will likely result in cyber wargames being quite far removed from the 'reality of a future major international cyber crisis.'[135]

Medium and fidelity

An extension of the debate surrounding computer versus manual games (Section 2.1.1) is what level of fidelity is desired in wargames, by which it is meant to what degree the game accurately represents the real world. Low-fidelity games are usually less complex and therefore easier to play, but are further abstracted from the real world, whereas high-fidelity games decrease abstraction through increased complexity, which also sacrifices playability.

There is no shortage of literature within wargaming extolling the virtues of manual board games over digital computer games. It is refreshing, therefore, to see that the computer science literature, contrary to what might be supposed of this field, also contains works that reinforce this notion. For instance, a study on fidelity in prototyping found 'paper and computer media equally valid for testing

[133] Kainakara (2003), p. 19
[134] Perla (1990), p. 182
[135] Curry and Price (2013), p. 23

prototypes,' and concludes that 'prototyping on paper eases participatory design and enables testing in a more exploratory, dynamic way.'[136] The ideas of participation and exploration are particularly interesting here, as they resonate with the goals of this thesis. Further computer science work in the area of interface design supports these findings. A 2007 study found that computer prototypes 'did not facilitate discussions on the overarching concept of the design, but did facilitate discussions on operational issues,'[137] while scenarios 'promoted discussion concerning structure, and function at a general level including social and organizational aspects. [sic]'[138] Strategy, which is at the core of this thesis, can be seen as an overarching design concept that emphasises social and organisational aspects, vindicating the move away from computer-based tools.

Some potential problems in this field have been recognised. Jagoda Walny, for example, points out that 'one challenge is in knowing how to create interfaces that do not interfere with thought processes.'[139] With regards to wargames, whatever the game board design, it will always limit – insofar as it guides – thought. However, as long as designers and players are aware of these limits and they are discussed, the learning objectives of the game can still be achieved. On this note, it should also be remembered that wargames are educational, not instructive. Games are great for promoting awareness about a topic, but less good for training people in processes. Steve Jackson, a prolific game designer whose work premises were raided by the US Secret Service in 1990 for alleged links to intrusion of federal computer networks (which were later proven false), included the following notice in the rulebook for *Hacker – The Computer Crime Card Game*:

> 'Important Notice To Secret Service! This Is Only A Game! These Are Not Real Hacking Instructions! You Cannot Hack Into Real Computers By Rolling Little Dice!'[140]

[136] Walker et al (2002), p. 665
[137] Johansson and Arvola (2007), p. 6
[138] Ibid., p. 7
[139] Walny (2014), p. 483
[140] Jackson (1992), p. 5

The point here is that games have a limited fidelity to the real world and are therefore limited in the lessons they can impart on players. It is important to recognise this, but not take it as an indictment of the usefulness of manual board wargames. The computer science literature highlighted above demonstrates that low-fidelity tools are particularly effective in promoting high-level thinking, which is exactly what this thesis is attempting to achieve.

2.3.2 Opponents

It takes two sides to make a wargame. Though hobbyists have a strange penchant for playing wargames solitaire, the games must nevertheless involve two or more opposing factions engaged in some manner of conflict.[141] In professional wargames the "protagonist" team will be played by the people whom the desired learning outcomes are primarily targeted at. The opposition, meanwhile, will be made up of people, potentially from the same organisation, whose job it is to adopt the mindset of the "antagonists" and play the game as if they were the enemy. The success of a game hinges heavily on the ability of these players to fulfil their role well. If the wrong people are used the value of the game will significantly drop because the accuracy of the game will be severely compromised.[142]

This places some great stresses on selection of these players who require 'in-depth knowledge of the adversary strategy, operational art and tactics.'[143] It is not always possible to find people with the necessary knowledge and understanding to fulfil the role, so ideally the game designer will restrict actions of the enemy to reflect these. However, in the case of free *Kriegsspiel* where rules are very few, evaluation of how realistic a player action is falls to the umpire. In these cases, the stresses of opponent player selection are instead transferred to selection of the umpire, whose 'judgement enters and colors the gaming process. [sic]'[144] Player and umpire selection is a problematic issue which is not easily resolved, and it will

[141] Dunnigan (1992), p. 59
[142] Kainakara (2003), p. 28
[143] Ibid.
[144] Brewer and Shubik (1979), p. 57

never be possible to completely rid a game of personal opinion. As Perla and McGrady summarise: 'Even expert military Red Teams [opponents] are slaves to their own worldviews – and all players are subject to the sometimes insidious preconceptions of the controllers and assessors.'[145]

This is particularly a problem with cyber wargames because knowledge and understanding of enemy plans and behaviours are very hard to come by. This is partly a feature of the cyber domain as one of heightened secrecy and inaccessibility (see Section 5.2.2 for further commentary on methodological constraints) but is also due to the lack of real-world examples from which to derive any information. Because of this, according to Curry and Price, 'games must rely on "experts" in name only, anointed in some way by background or media exposure. The danger of agenda driven self-fulfilling prophecy is obvious.'[146]

2.3.3 Outcome

Players of wargames, as with any games, can become too fixated on the final outcome of the game – victory or defeat – and lose sight of the subtler lessons learned along the way with regards to the thematic content. In rousing the competitive, spirit which has previously been listed as a benefit of wargaming, the very same spirit can potentially cause the game to misfire if players attach too much importance to the result of the game. There are three facets to this, as outlined by Kainikara:

> 'The first is a flaw in the design process of the game itself wherein a predetermined outcome is factored in and the rest of the game is tailored around it....The second is to view the outcome of a game as an infallible indicator to real life situations....The third, less serious, pitfall is for the participants to think that the design of the game itself is at fault when it is not going the way they perceived a situation to develop.'[147]

[145] Perla and McGrady (2011)., p. 124
[146] Curry and Price (2013), p. 22
[147] Kainakara (2003), p. 36

With the first two problems, if players begin to believe that either of these are the case, the game will cease to be valuable. In the first instance, players will become disillusioned with the game and consequently disengaged, which will counteract any of the benefits from experience discussed previously. In the second instance players will attach too much value to the game's realism and shy away from adventuring into the unknown territory previously made possible by the safety benefits.

It is also important to not be overzealous in promoting the realism of a game. If players buy into the game and immerse themselves completely, the game can be too powerful. Players can be manipulated into 'false beliefs and assumptions' creating a belief that the 'game has lied to the players, which will result either in their learning incorrect lessons or in their disbelieving the outcomes and recommendations that flow from the game.'[148] Right from the outset it is imperative that the game designer is aware both of their position as marketer of the game and how the game is received, because 'the difference between a false prophet and a real one is usually detectable only after it's too late.'[149]

Given the perils associated with game outcomes, it pays to recall the Picasso citation about computers being useless because they can only give you answers. Game designers can, and possibly should, adopt this attitude and insist that the game is approached with a mindset of 'We may never know the right answers, but gaming can sometimes help us learn to ask the right questions.'[150] If players are aware of this critical limitation from the outset they are less likely to get hung up on the results of the game and instead better absorb the pedagogical elements of the activity.

2.3.4 Politics of representation

An aspect of wargaming that ties together many elements from previous sections is the politics of representation in games. Because games are abstractly simplified,

[148] Perla and McGrady (2011), p. 123
[149] Dunnigan (1992), p. 110
[150] Perla (1990), p. 34

set up with overly opposing sides, and hinge on a win-or-lose outcome, they are fraught with representations that carry political connotations. It is important to be cognisant of these because they may impose limitations on what a wargame can achieve.

In modelling and simulating conflict, wargames by their nature set up scenarios with opposing sides. Unlike cooperative games (such as *[d0x3d]* analysed in Chapter 3, or the card game *Hanabi*) where players work together towards a common goal, wargames have players working against each other, not only to succeed themselves (as a player might in a game of *Cluedo* or *Snakes and Ladders*) but to actively see the enemy defeated. There are of course wargames where players form alliances, but the ultimate objective remains the demise of the enemy, whether that be a single player or an opposing alliance. In this sense, wargames represent a bellicose world of 'us versus them', perhaps expressed more strongly as 'us or them.' In setting up such zero-sum worlds, wargames do not necessarily represent the real world, which contains complex mixtures of positive-sum, negative-sum, and zero-sum situations.

More revealing, politically, is how the factions in such antagonistic scenarios are labelled. In standard wargaming terminology, friendly forces are blue and hostile forces are red – notation which has its roots with Helmuth Moltke the Elder.[151] This dichotomy is really only a chromatic advancement on the original juxtaposed black and white found in progenitor wargames Go and chess. In practical terms, different colours can help easily identify pieces on a game board, for example by using colours of national flags. Michael Vlahos has described how US naval interwar gaming used orange for Japan, red for the Soviet Union, and black-silver for Germany and Italy.[152]

The politically-charged implications of such colourisation become clear when we consider the default position of red as the enemy. Red has traditionally been the colour of the political left and was synonymous with Communist movements across the globe in the 20th century. During the Cold War, "the Reds" became a

[151] Simpson (2017), p. 15
[152] Vlahos (1986), pp. 17-18

byword, often used derogatively, to identify the Soviet Union, China, and other Communist factions.[153] In the wargaming mindset, those who assume the red mantle automatically slot into the enemy category and become someone who must be defeated. Cooperation with a Communist country can thereby be seen as an impossibility, setting up the existential struggle between Communism and capitalism, and East versus West, which dominated the latter half of the 20th century.

It is intriguing to note that such a worldview is entirely Western. William Simpson writes that 'when Russia and China adopted modern wargaming they chose their national color of Red as friendly reversing the colors.[sic]'[154] It could therefore be argued that wargamers, especially those in the West, need to be aware of the politicisation of aspects of gaming, because the conventions such as the colours used by teams can come to represent a narrow worldview. In general we want to avoid war and conflict, but if representations in games create political worlds with default enemies that must be defeated, it may be that players are left with the impression that war is a problem to be solved (or indeed a solution in itself) rather than one to be avoided.

Chapter 2 Conclusion

The literature that informs this thesis comes from a range of academic disciplines. Wargaming itself is highly interdisciplinary, and this thesis, combining wargaming with cyber security, is even more so. In addition to key texts in wargaming, this chapter has critically analysed works from fields including history, geography, philosophy, and computer science, while references to literature, mathematics, and business studies can also be found. Furthermore, a plethora of non-academic reports and government documents have been consulted, which, despite their lack of academic merit, are nonetheless crucial components of the corpus this thesis draws on.

[153] Mao (2013), p. 617
[154] Simpson, ibid.

The chapter has made three significant original contributions to our understanding of the uses, advantages, and limitations of wargaming. The first, as discussed in Section 2.1.1, is the creation of a new, succinct categorisation of the uses of wargames. In existing wargaming literature, there are many efforts to succinctly define what wargames *are*, and the most widely accepted seems to be Perla's definition: 'a warfare model or simulation whose operation does not involve the activities of actual military forces, and whose sequence of events affects and is, in turn, affected by the decisions made by players representing the opposing sides.'[155] To find out what wargames are *used for*, however, one must peruse lengthy chapters from disparate sources, in part because wargames have such a wide field of applicability, from military operations to crisis exercises to business ventures. The categorisation in Section 2.1.1 brings all of these uses together under a generalised umbrella: Wargaming can be used to understand events of the past, plan operations and organisations for the present, and explore envisaged futures. This neatly captures what wargaming can be used for and readers who are interested in one or more of these strands can consult the additional paragraphs in Section 2.1.1 for practical examples and suggestions for further reading.

The second contribution, found in Section 2.1.2 (and subsections), is intersecting diverse literatures around the theme of futures. Although much wargaming, as driven by hobbyists, concerns historical conflict, professional use of wargames often concerns the future. The literature, however, is replete with contrasts about futures. Where Fine found chess players employing 'lines' to imagine potential futures, Anderson considered the futures of emergency exercises 'unimaginable.' At the same time, these exercises were both pessimistic (preventative) and tactical, contrasting with the UK Government's approach to cyber security which is optimistic (enabling) and strategic. Moreover, potential contrasts exist between Ghamari-Tabrizi's assertions of technological progress setting the context for Cold War wargaming, while it could be said that in reality there was a lack of technological progress during this period – nuclear weapons became bigger, but they did not fundamentally change. It is unclear whether such a plateauing of technology has happened, or will happen, with regards to cyber security. To the

[155] Curry (2011), p. 157

researcher's best knowledge, no current work exists which brings together these divergent strands of literature, so the analysis in Section 2.1.2 should be considered a valuable and original contribution.

Finally, in drawing on computer science literature, Section 2.3.1 concerning medium and fidelity is a novel contribution to wargaming. Extant wargaming literature recognises both the problem of abstraction and its implications for wargame deployment and analysis, as well as design (see Section 4.1). Having acknowledged the problem, the literature is also keen to highlight why abstract (board) games are still entirely useful, even advantageous over less abstract (computer) games (see Section 2.2.1). However, rather than rely on this literature itself as evidence for these assertions, Section 2.3.1 utilises studies from the computer science fields interface design and human-computer interaction to corroborate the claims. Contributions from Walker et al and Johansson and Arvola show that using paper over computers encourages participation and exploration, while scenarios are better than computer prototypes at prompting strategic thought. These are conclusions any wargamer would agree with but have hitherto not been backed by evidence from "hard" science.

By embracing the interdisciplinarity of wargaming and amplifying this by consulting diverse strands of literature, this chapter has made original contributions which enhance our understanding of the uses, advantages, and limitations of wargaming.

Chapter 3: The state of play – existing cyber wargames

Though this thesis is born out of an identified gap in existing wargaming products, there is nonetheless a smattering of games that tackle cyber in one way or another. It is essential to conduct a review of these games in order to analyse their strengths and weaknesses, which can then be used to inform the design of the original game of this thesis, as well as to help position the thesis in the wargaming landscape.

This chapter draws on analysis of 25 games which are based around cyber security and/or cyberspace (see Table 1). Miranda has stated that with regards to cyber gaming, 'it's a matter of applying proven systems with radical new ideas.'[156] Going forward in this spirit, this chapter is structured according to five aspects or features of games which have been deemed successful, either for their effectiveness at conveying a particular cyber security topic – thereby enhancing the potential for creating learning moments – or their contribution to gameplay. The aspects are: ludic components, adversarial nature, cards, simulating unpredictability, and marketplace. These features not only inform the design of the original game in this thesis (Chapter 4), but also serve as guidance for other wargame designers seeking to tackle the topic of cyber security.

Table 1: Games analysed in this chapter

	Game Title	Type	Year	Medium	Availability[157]
1	Enterprise Defender	Wargame	2013	Manual	Open
2	All Your Secrets Are Belong To Us	Wargame	2013	Manual	Open
3	Conspiracy!	Wargame	2013	Manual	Open

[156] Miranda (2016), p. 680

[157] Open availability means all the game components (rules, boards, pieces etc.) can be acquired, either for free or to purchase. Closed availability means the game offers limited access to working components.

4	Media Wars	Wargame	2013	Manual	Open
5	Tallinn Soldier	Wargame	2013	Manual	Open
6	Global Cyber Game	Other	2013	Manual	Open
7	CyberCIEGE	Education	2014	Computer	Open
8	LOCKED SHIELDS	Other	2010-	Computer	Closed
9	[d0x3d!]	Education	2013	Manual	Open
10	Ctrl+Alt+Hack	Education	2013	Manual	Open
11	Operation Digital Chameleon	Wargame	2016	Manual	Closed
12	Cybernauts	Hobby	1996	Manual	Open
13	Cryptomancer	Hobby	2016	Manual	Open
14	Game of Threats	Other	?	Mixed	Closed
15	Cyber Strike	Wargame	2016	Manual	Closed
16	OWASP Snakes and Ladders	Education	2014	Manual	Open
17	Top Threats	Other	?	Manual	Open
18	Privacy	Education	2012	Manual	Open
19	Maelstrom	Education	2016	Manual	Open
20	Anti-Hack!	Education	2016	Manual	?
21	Security Cards	Education	2013	Manual	Open
22	Spot the Risks	Education	2016	Computer	Closed
23	Secure Workspaces	Education	2016	Computer	Closed
24	SyHacked	Education	2016	Computer	Closed
25	Decisions & Disruptions	Education	2016	Manual	Open

Of the 25 games, seven can be classified as wargames, twelve as educational games, two as hobby or entertainment games and four as other. Nineteen of the games surveyed are manual tabletop games, five are computer-based, and one is a hybrid solution. The reason for reaching out to a wide breadth of games is partially due to the dearth of pure cyber wargames – at least in the public domain (see Section 5.2.2 for further discussion of secrecy and classification problems). However, there are more than superficial reasons for analysing a variety of game types: these types are liable to inform and influence each other.

A potted history of 20th century wargaming serves to demonstrate how the hobby and professional sides of the activity have been mutually influential. Hobby wargaming was popularised by H.G. Wells' *Little Wars* in 1913 and grew steadily in the following decades.[158] In the 1960s wargaming suffered a downturn in popularity, owing to the rise of operational research, systems analysis and cost-benefit trade-offs on the professional side[159], while hobbyists struggled to 'reconcile playing at war when so many of their contemporaries and friends were dying in the reality of Vietnam.'[160] In the 1970s two developments on the hobby side served to reinvigorate professional wargaming. First was the widespread introduction of science-fiction and fantasy games, led by *Dungeons & Dragons* in 1973.[161] Second were the efforts of wargames publisher Simulations Publications International whose "future history" games helped 'civilians better understand the potentially violent world in which they lived.'[162] In the US, military officers who had been playing these games recreationally brought their experiences into their professional lives as they moved up the ranks, thereby reviving the fortunes of wargaming by the 1980s.[163] When the Pentagon wargamed the Gulf War within hours of receiving the news of Saddam Hussein's invasion of Kuwait in 1990 (see Section 2.1.1), they used commercial off-the-shelf wargame *Gulf Strike*. This mutually influential relationship endured into the 1990s and the first years of the 21st century as video gaming gained popularity. The United States Marine Corps modified first-person video game *Doom*, released in 1993, into a training simulator.[164] Going the other way, *Full Spectrum Warrior* was a direct derivative of a tactical infantry simulator, released as a video game in 2004.[165] With such synergism between the hobby and professional sides of wargaming, it would therefore seem imprudent to ignore developments in one sphere or the other. Indeed, the analysis provided in this chapter may serve as a catalyst for further synergism with regards to modern cyber wargaming.

[158] Perla (1990), pp. 35-36
[159] Ibid., p. 109
[160] Ibid., p. 127
[161] Dunnigan (1992), p. 153
[162] Perla, op. cit., p. 131
[163] Dunnigan, op. cit., p. 246
[164] Halter (2006), p. 169
[165] Adair (2005)

Broadening the types of games under consideration resulted in an increase in the number of games which could be analysed in the context of this thesis. Katrin Becker makes the point that as academic study of games has matured, it has become imperative to justify why we choose to analyse certain games over others, because proving their relevance enables us to ascribe them with wider impact.[166] She further begrudges that in her survey of 89 ludic scholarly articles, only one applied a systematic technique to identify games, only one had described an exclusion rationale, and only one described the methodology used to select the game for the study.[167] Although Becker's study is now dated (in that the sample of eligible articles has grown), the sentiment remains valid – studying games without validating their purpose in the study undermines the value of the analysis. Therefore, as to not repeat these mistakes, the games in this chapter represent a final selection based on the following, admittedly simple, criteria.

First, the primary theme of the game had to be cyber security, or a subtopic thereof (such as privacy or encryption). Games which contained a cyber security component, but which focused on some other aspect, were therefore not included. Megagames such as those run by the KCL Crisis Team in 2016 or at the Connection UK 2017 conference included cyber attacks as part of players' offensive arsenals, but these were merely small features in larger games, therefore precluding them from analysis in this chapter.[168] The cyber security theme was also considered distinct from cyberpunk, which is a popular board game setting heavily influenced by science fiction such as William Gibson's *Neuromancer*.[169] Website boardgamegeek.com lists nearly one hundred games in this genre.[170] The criterion excluded games like *Android: Netrunner*, which contains many cyber-themed elements, but draws more on science fiction than security practices.[171]

---

[166] Becker (2011), p. 49
[167] Ibid., pp. 51-52
[168] Author's personal experiences at KCL Crisis Team South China Seas event 26-28 February 2016 and Connections UK 2017 conference 5 September 2017
[169] Gibson (1995)
[170] BoardGameGeek website
[171] It could be argued that *Android: Netrunner* is indistinct from *Cybernauts* or *Cryptomancer* in this regard, but *Cybernauts* passes the criterion because of the voluminous explanatory notes which are cyber security-focused, whilst *Cryptomancer* is included because of its core focus on cryptography.

Second, information about the game had to exist in the public domain. This thesis is written entirely at an unclassified level, so any games encountered behind closed doors could not be included. Public domain information includes published games, peer-reviewed publications, game reviews, publicity material, and, in the case of *Cyber Strike*, hands-on time with the game in a public forum. If no combination of these could be obtained, the game could not be included.

To be clear, although all 25 games were reviewed as part of the process for deriving the themes for this chapter, not all 25 are explicitly referenced in the following sections. Readers interested in finding out more about a non-referenced game can find relevant entries in the bibliography.

3.1 Ludic components

The first aspect of note is that the games from the list which are most engaging to play – and therefore have a greater chance of capturing players' attention – have strong ludic components. That is to say, they contain many of the accoutrements usually associated with games (game board, playing pieces, dice etc.) and employ gamified mechanics to challenge players and drive progress in the game.

3.1.1 Games that are playable and enjoyable

Many games on the list aspire to be fully-fledged games, but only a few succeed in providing sufficient ludic components and mechanisms to be both playable and enjoyable.

Cybernauts

Cybernauts, one of the most complex games analysed in this chapter in terms of number of game components, was designed by Joseph Miranda. Released as part of an issue of wargaming magazine *Competitive Edge* in 1996, *Cybernauts* takes advantage of a number of contemporary nascent cyber themes to create a future game world replete with political intrigue and technical terminology. The game's

setting is heavily influenced by the Key Escrow/Clipper Chip conflict which was ongoing at the time[172], as well as the recently transpired legal case against Philip Zimmerman's PGP email encryption[173], but is equally aware of wider geopolitical trends and strategic concepts.

The game's introduction provides a perfect summary of the setting:

> 'In the early 21st century, a global computer network called the Net is openly used by the STATQUO (government, corporations, organized crime, "the system") to maintain global domination. STATQUO's power is challenged by computer hackers called Cybernauts. The game revolves around the struggle between Cybernauts and STATQUO for control of the Net. One side, called the Netrunner, represents a group of active Cybernauts. The other side is the NSA, STATQUO's Net Security Agency. The objective of the game is for the Netrunner to destroy or take control of as many electronic files on the Net as possible. The NSA uses its computer resources and agents to preserve the Net's integrity by blocking Netrunner activities and by discovering the whereabouts of the Cybernauts and eliminating them through execution.'[174]

Taken as political commentary, this passage clearly identifies the US National Security Agency (NSA) as a malevolent actor, while the proponents of encryption and internet freedom are a force for good. Indeed, the in-game NSA has a number of Security Service teams, referred to as SS units and whose icon resembles two red lightning bolts – a thinly veiled reference to the Nazi Schutzstaffel. We should recall that the target audience for the game were hobbyist wargamers, who more often than not are also avid historians. Additional aspects of audience-pleasing are several nods to popular culture science-fiction. For instance, two of the Cybernaut characters are called Decker and Gibson – the former referencing Harrison Ford's character in 1982 movie *Bladerunner*[175], and the latter being the author of seminal 1984 cyberpunk novel *Neuromancer*.[176]

[172] Miranda (1996), pp. 9-10
[173] Ibid., p. 12
[174] Miranda (1996), p. 13
[175] Scott (1982)
[176] Gibson (1995)

The game board is divided into two arenas: the real world (a geographical map) and the Net (a 10x10 square grid). The Netrunner player controls up to five Cybernauts selected from a list of ten, each of which has different attributes, while the NSA player has at their disposal a number of defensive 'Cyberchits' and aforementioned SS units. The game lasts ten turns, during each of which the Netrunner first conducts interaction and movement in the real world, followed by an optional 'Netrun' involving movement on the Net and 'cyberstrikes', which the NSA player has a chance to react to. A turn is then finished by NSA interacting and moving in the real world.[177] The game is won by victory points, calculated by comparing how many files the Netrunners have destroyed or captured versus the number of Cybernauts the NSA player has eliminated.[178]

Interestingly, the final five pages of the game are dedicated to an NSA strategy guide, while no such help is afforded the Netrunner player. Miranda justifies this by saying that 'the NSA player has the more challenging task ahead of him, and it is the successful accomplishment of a challenging task that is the most satisfying.'[179] Aside from the gendered language (remembering the target demographic for the game), it appears that the game is balanced in favour of the Netrunner, perhaps reflecting the political commentary from earlier.

Although not designed as an educational tool, it is readily evident how *Cybernauts* may be a useful entry point for someone interesting in learning more about cyberspace and cyber security. A glossary, for example, provides a good overview of key cyber security terminology.[180] As a caveat, however, certain parts of the game have not aged very well with references becoming outdated. The crypto wars debate, for example, has moved on from the Clipper Chip to post-Snowden. A 1990s audience would therefore probably have derived more educational value from the game than a 2010s audience might. Despite this shortcoming, *Cybernauts* retains immense value as a playable piece of astute strategic and political commentary.

[177] Miranda (1996), pp. 14-15
[178] Ibid., p. 20
[179] Ibid., p. 25
[180] Ibid., p. 11

Cybernauts and *[d0x3d!]*, on the other hand, are fully-fledged games with intricate, well-designed accoutrements and mechanics that force players to cognitively engage and make decisions about courses of action which in turn have repercussions on gameplay going forward. In order to make a meaningful contribution to the wargaming corpus, it is therefore important that a product which calls itself a game must actually be a game.

[d0x3d!]

Foremost among the educational games analysed in this chapter, *[d0x3d!]* is a card game designed by Zachary Peterson and Mark Gondree.[181] The game has 'modest pedagogical objectives intended to expose young people to topics in computer security' – a goal the designers motivate by identifying lacklustre participation rates in high school and university computer science courses, and 'curricular deficiencies' across K-12 education.[182] Players assume the role of white hat hackers who must infiltrate a network, locate assets (Personally Identifiable Information, Authentication Credentials, Financial Data and Intellectual Property) and recover these while remaining undetected.[183] Gameplay is entirely collaborative, with players using limited actions represented by cards in their hand to navigate the network game board, perform actions, or trade cards with other players. The players win, as a team, if they recover all assets and lose if they are discovered and locked out of the network.

[181] The name of the game is a stylised version of the word 'doxed', which is the practice of maliciously releasing someone's personal information (for example address and phone number) online.
[182] Gondree and Peterson (2013), pp. 1-2
[183] Ibid., p. 3

Figure 1: A game of [d0x3d!] in action. Image courtesy of TableTopSecurity Flickr (https://www.flickr.com/photos/tabletopsecurity/8295763634/)

[d0x3d!] is not a game designed from scratch, but instead based on the existing board game *Forbidden Island*.[184] In effect, *[d0x3d!]* is simply a reskinned version of *Forbidden Island*, borrowing its highly-regarded gameplay mechanics while updating the graphical assets to reflect a cyber security theme. In a 2016 seminar at Royal Holloway University of London, one of the designers, Zachary Peterson, was asked about his experiences with this approach, to which the answer was twofold.[185] Firstly, as a benefit, using an existing game significantly cut down playtesting time. *Forbidden Island* will have gone through a long process of testing and refinement by that game's designer (Matt Leacock), meaning any derivative games which share the rules and mechanics inherit this testing process. On the other hand, as Peterson pointed out, this also meant that any tweaks they made to their game could have drastic effects, because the original was so finely tuned. Unless they wanted to invoke additional playtesting, they therefore had to keep changes in game mechanics to a minimum.

[184] Gondree and Peterson (2013), p. 3
[185] Author conversation with Zachary Peterson, Royal Holloway University of London, 11 October 2016

Secondly, as a potential pitfall, Peterson was aware of intellectual property issues that may arise from copying other material. In practice, it is not possible to claim copyright or file a patent on game mechanics, only game graphics.[186] However, there is an unwritten code of conduct among game designers that when gameplay elements are borrowed or inspired by other games, these games should be given an acknowledgement, for example in design notes or promotional material.[187] This does not quite have the rigour of academic referencing, but should nonetheless be observed lest the designers, and by extension their game, come at odds with the gaming community. It is important to retain the support of this community, not only as a source of influence, but also as players and customers.

Benefits and drawbacks notwithstanding, by repurposing *Forbidden Island*, *[d0x3d!]* inherits the eminent playability of the former game, making it relatively easy to pick up and play, which is important when targeting a demographic with limited attention spans. Although the game does not have a lot of different components compared to something like *Cybernauts*, it contains robust mechanics to capture players' attention long enough to get them interested in the thematic cyber security content.

3.1.2 Games that are not quite games

A number of the games in Table 1 are marketed as games but contain much fewer ludic components and mechanics than other titles on the list.

Matrix games

The first five games in the list come from John Curry and Tim Price's *Dark Guest* book.[188] A common criticism that applies to all five games is that they are matrix games (also known as seminar games) – a subset of wargames focused on player discussion with limited game accoutrements and gameplay. In essence, the core gameplay of matrix games is that players verbally describe an action they would

[186] U.S. Copyright Office (2016)
[187] Which Gondree and Peterson do in their 2013 paper, op. cit., p. 3 and on the *[d0x3d!]* website
[188] Curry and Price (2013)

take, other players may get an opportunity to argue how they would mitigate or counter that action, and the umpire decides – sometimes using dice – whether the action is successful. Such games are recognised for their simplicity and accessibility, but at the same time lack much of what Perla considers 'a good wargame needs': a data base, models, and (to some extent) rules.[189] In most of the *Dark Guest* games, especially *Enterprise Defender*, *All Your Secrets Are Belong to Us* and *Media Wars*, the umpire plays a pivotal role and dice rolls serve no real purpose, as the numbers and outcome are assigned by the umpire anyway. Insofar as having any elements of chance or probability, this game fails to provide independent variables which can affect the outcome.

The authors do recognise these limitations and stress that 'the training value of [*Enterprise Defender*] comes from evaluating the familiarity of the managers with the organisation's existing policies.'[190] Despite this acknowledgement, the authors only offer the vague statement that their 'experience' evidences the game's efficacy.[191] It would have been beneficial for the authors to provide concrete examples of how the game has been used, or a list of suggested discussion points that their experience has shown generates useful outcomes. Without these it is difficult to evaluate the educational value of the game.

Intriguingly, in their introduction to *Dark Guest*, Curry and Price state that the first edition of the book (which the researcher was unable to acquire) contained a card-based game, but for the second edition they decided the wargaming community needed more 'generic ideas with wider application.'[192] As a counterpoint, the analysis presented in this chapter, and the game design and results in Chapters V and VI, make it clear that more intricate games for narrower purposes have great value and should not be discounted.

[189] Curry (2011), p. 158
[190] Curry and Price (2013)., p. 39
[191] Ibid.
[192] Curry and Price (2013), p. 5

The Global Cyber Game

The central focus of *The Global Cyber Game* is a 'Cyber Gameboard' which aims to endow players with 'the ability to determine an optimal strategic approach to cyber security concerns.'[193] The Gameboard is divided into nine rectangles, representing intersections between power and information. Cells are grouped in three zones (along the power plane), denoting, in turn, 'destructive power against information assets', 'information assets to produce economic exchange power', and 'social power of freely shared information assets.'[194] The intention is that an actor's real-world actions can be mapped onto this Gameboard, thereby exploring how that actor is traversing and exploiting different aspects of cyberspace.

While the goal is a noble one, it is very hard to see how this can be classified as a playable game, let alone a wargame. Though all the right components are nominally there, no actual information for how the game might be played is supplied. Instead, the report outlines historical exchanges such as US versus Iran, US versus China, and US versus Kim Dotcom to analyse how the different players' actions can be described in terms of the framework provided by the Gameboard. While certainly an interesting and potentially useful exercise, there is nothing here which a wargamer can actually play for specific educational purposes. In short, the report provides nothing actionable, which is the keyword this thesis is keeping in mind at all times.

Spot the Risks and *Secure Workspaces*

Meanwhile, *Spot the Risks* and *Secure Workspaces* are two computer-based games produced by legal expert Daniel Solove, intended to be used for training in aspects of privacy and data security. In both games, players are presented with a stylised image of a workplace (see Figure 2) and tasked with clicking on situations where personal information is at risk of being exposed. Players receive points for correctly identifying risks and penalties for incorrectly identifying risks, all of which adds up to a total score at the end.

[193] Ibid., p. 13
[194] Ibid., pp. 37-40

Figure 2: Screenshot from Spot the Risks, office version (image author's own)

Each game takes only a few minutes to play and the graphical presentation is simple and intuitive, so they are very accessible. Solove himself provides a voiceover that reads all the text in the games, but his voice is rather monotonous and does not enhance the engagement quality. Indeed, the games self-styling as 'highly-engaging and fun' is overly ambitious because the gameplay is fairly boring and attempts at humour in the games fall flat.[195] To classify these activities as games is tenuous owing to their linearity and lack of competition, and there are no repercussions for making an incorrect decision, which as we have seen in Section 2.2.5 is central to the effectiveness of wargames. A better term would be to call these products 'interactive tools', which more accurately reflects what they are.

3.2. Adversarial nature

The second aspect which many of the most engaging games have in common is their adversarial nature. As illustrated in Section 2.2.2, one of the primary benefits of wargaming is that it pits humans against humans, creating a dynamic

[195] *Spot the Risks* website

environment where unpredictability is not just the result of chance through dice rolls, but also the uncertainty of human decision-making processes. In other games where players battle against the game system there is still some representation of human decision-making foibles, but only on one side. For a physical metaphor, compare hitting a tennis ball against a wall with playing against a human opponent: both present a challenge, but only one has a thinking adversary.

3.2.1 Player versus player

Among the 25 games analysed, there were some which implemented adversarial player mechanics to great effect.

Operation Digital Chameleon

Perhaps one of the most intriguing developments in cyber wargaming is *Operation Digital Chameleon*. Designed by Andres Rieb and Ulrike Lechner from Universität der Bundeswehr in Munich, the game is intriguing because the academic paper which accompanies it reads like a miniature version of this thesis.[196] It begins with motivations that extoll the virtues of wargaming for education, provides an overview of current efforts (although the focus here is squarely on exercises rather than games), outlines their methodological approach and game design, and concludes by offering insights into player experiences.

The game itself is played on a game board representing 'the IT-infrastructure of a Critical Infrastructure – without any IT-security instruments.'[197] (See Figure 3.[198]) The game uses an adversarial setting where players are divided into red and blue teams, respectively tasked with attacking and defending this network. The teams are set up in separate rooms, so they cannot see what the other team is doing but must react to each other's actions as they become known. Gameplay consists of the teams describing their attacking and defensive measures in terms of 'attack

[196] Rieb and Lechner (2016)
[197] Rieb and Lechner (2016), p. 4
[198] Rieb has denied requests for a higher-resolution image of the game board, owing to him using it for consultancy purposes and not wanting others to steal his idea.

trees', and the actions taken must be consistent with the role the team is playing – for instance if the red team are playing script kiddies they cannot develop and use zero-day attacks.[199]

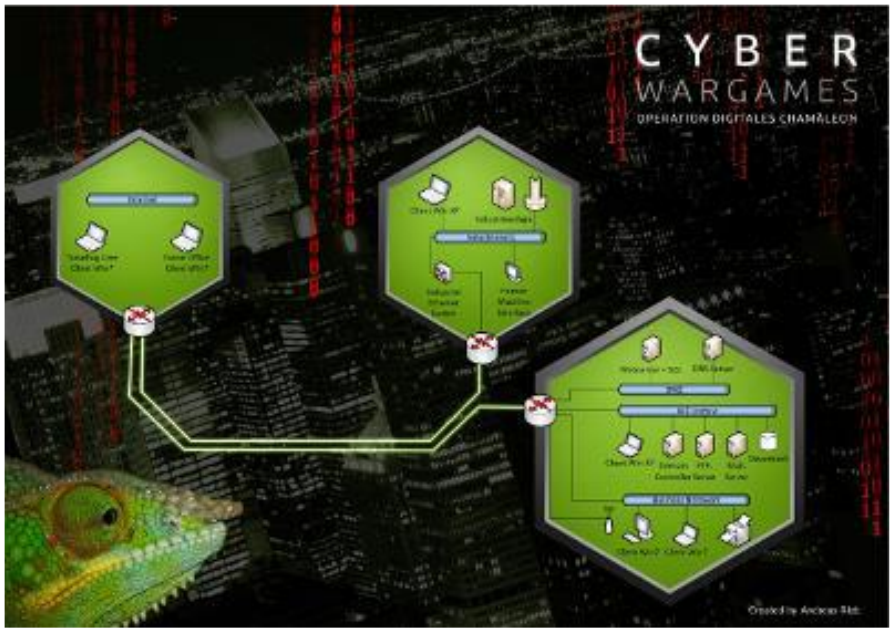

Figure 3: Operation Digital Chameleon game board (image from Rieb and Lechner (2016), p. 4)

In order to enable the double-blind gameplay mechanics, the game is overseen by a white cell 'Games Master' who not only ensures the rules of the game are adhered to, but also determines the winner.[200] In this sense, *Operation Digital Chameleon* Closely resembles some of the matrix games analysed earlier in this chapter. The designers do recognise the potential shortcomings of this approach, particularly the critical need for open discussion and evaluation of results, because 'without transparency, it is highly likely, that participants will be frustrated and blame the Game Master to manipulate and to decide in an arbitrary manner. [sic]'[201]

Rieb and Lechner's paper is positive about the outcomes of the game, though this appraisal is conducted on the back of only one play session.[202] Despite such a limited dataset, *Operation Digital Chameleon* is a valuable addition to the cyber

[199] Rieb and Lechner, op. cit., p. 5
[200] Rieb and Lechner (2016), p. 4
[201] Ibid., p. 5
[202] Ibid., p. 8

wargaming corpus, especially if viewed as an early indication reaffirming the utility of wargaming for education. Moreover, these outcomes were achieved in an adversarial game setting, reaffirming this approach as one that can foster high levels of engagement and create opportunities for players to learn about cyber security. As a drawback, *Operation Digital Chameleon* illustrates some of the overhead associated with facilitating the blind gameplay which enables a rich adversarial setting.

Game of Threats

One business that has adopted wargaming is PricewaterhouseCoopers (PwC), who have created *Game of Threats* to be used as part of their consultancy services. The game is loosely based on the Lockheed Martin Kill Chain[203] and 'simulates the experience of executives when their company is targeted by cyber attack.'[204] The game is for two teams of five to ten players, competing in an adversarial setting: one team plays attackers who must attempt to penetrate a company network and access valuable data or hinder the company from operating, whilst the other team play as company representatives who must defend their network, mitigate any intrusions, and manage public relations. Gameplay involves the teams investing limited resources in cards that enhance attacking or defensive capabilities and deploying these. The presentation of the game is technology-assisted, with each team viewing the game situation from their point of view on a screen while controlling their moves via an iPad. There is also a central screen visible to both teams which shows an overarching picture of the state of play. Points are scored for successful attacking and defensive moves, and at the end of the game moderators use these for 'reviewing both teams' strategy, actions and missed opportunities.'[205]

Aside from the flashy technological presentation, the setup and gameplay of *Game of Threats* appears very similar to the game created for this thesis, as outlined in Chapter 4. Unfortunately, it has not been possible to verify this as the

[203] Author discussion with PwC representative, London, 16 February 2017; Lockheed Martin website
[204] *Game of Threats* website
[205] Ibid.

company has not been willing to show a working demonstration or provide any hands-on time with the game. It was possible to garner some further information about the game in a meeting with a senior PwC representative, but most details were shared on a commercial-in-confidence basis (more on this in Section 5.2.2). However, one crucial insight, which is entirely shareable, is that according to the representative, *Game of Threats* 'helps the board ask the right questions.'[206] Whether they were wittingly channelling Peter Perla's citation from Section 2.3.3 or had arrived at this conclusion independently is unknown. Either way, Perla's sage wisdom appears to withstand the test of reality.

3.2.2 Player versus system

A less common approach in the analysed games was for players to compete against the game itself rather than other players.

[d0x3d!]

One limitation of *[d0x3d!]* (see Section 3.1.1) is its purely collaborative nature. Players do not compete against each other and the game's adversary (the network administrator) is 'encoded in the game's mechanics.'[207] This may serve the social function the game designers emphasise, as players have to communicate to achieve their goals.[208] The designers also point to a 'myth that human opponents are more dynamic, less predictable, and more skilled than the non-player adversaries encoded in challenges' and that 'player adversaries can be considered "poorly designed": they can become distracted, become disengaged, be offline for significant portions of the competition, [and] be over-skilled (or under-skilled) compared to other players.'[209] Whilst these are certainly defensible objections, we would also do well to recall many of the human-centric benefits outlined in Chapter 2 (Section 2.2.2), and the Alfred H. Hausrath quote that 'gaming challenges the competitive spirit.' A players-versus-system setup, such as

[206] Author discussion with PwC representative, London, 16 February 2017
[207] Gondree et al (2013), p. 65
[208] Ibid.
[209] Gondree et al (2016), p. 38

the one in *[d0x3d!]*, seems to be at odds with these benefits, or at least not realise them to their full potential.

SyHacked

As an antithesis to the Solove games (see Section 3.1.2), *SyHacked* is an excellent example of an interactive online tool with strong gamic elements. Produced by Transmedia Storyteller for Al Jazeera news network, *SyHacked* is a game intended to educate players about cyber security aspects of the ongoing conflict in Syria. Players are placed in the shoes of a newly-hired investigative reporter tasked with producing a report on the Syria cyber conflict.[210] Players make contact with sources to gather information but must be careful to not get hacked themselves.

Gameplay revolves around players making decisions about which potential sources to pursue and how to approach them. Sources range from hackers and activists to analysis and journalists, both on the ground in Syria and elsewhere. Once a player decides to pursue a lead they must establish a medium for contacting that source, whether via email, instant messaging, text message, telephone, or face-to-face meeting. Each decision can have ramifications as some sources prefer certain modes of communication and will only give you the information you need if contacted in the correct way, for example with pre-agreed codewords. The player is also exposed to hostile actors who try to derail the investigation through devious misinformation or outright hacking activities.

The presentation of the game is very polished, with a central interface containing an amalgamated inbox of communications. When the player interviews a source, it is presented via a video or voice vignette with details about cyber operations in Syria or more general cyber security lessons. The educational elements of the game are contained in these vignettes as the player learns more about how cyber has played a role in the Syrian conflict. Players not already familiar with cyber security concepts are also made aware of things like passwords, encryption and phishing – the latter of which is particularly powerfully presented when a player clicks on a link in an email resulting in them being hacked and game over. The

[210] *SyHacked* website

game even offers a way for players to link their own real-world Facebook accounts to the game, although this seems somewhat contrary to many of the lessons the game tries to teach.

Overall, the presentation value and design of *SyHacked* makes it emblematic of how interactive educational games should be done. The game is not linear, and player-decisions have a real impact on how the game progresses, so there is a strong sense of challenge and high replay value. However, as a single-player game, SyHacked does not contain any multiplayer adversarial elements. The challenge therefore comes only from the game itself, which is a less dynamic opponent than other humans would be.

3.3 Cards

The third aspect worth highlighting is the prevalence of cards among these games. There is only a handful of games which do not have any card components, and several are entirely card-based. Cards are a useful mechanic to simulate the fog of war, both in terms of capabilities and intentions. For these reasons, Clausewitz asserted that 'in the whole range of human activities, war most closely resembles a game of cards.'[211] Cards can be used to hide information from other players, yet their presence suggests the existence of information, just not the content – in effect creating known unknowns.[212] (More on this in Section 4.6.) Cards are flexible and powerful game components because they can be implemented in a variety of ways, and, as Miranda asserts, 'the physicality of the cards does much to enhance player experience.'[213] A notable limitation, however, is that cards are usually a relatively small size, restricting the amount of information and data that can be legibly printed on them.

[211] Clausewitz (1997), p. 27
[212] A term popularly attributed to former US Secretary of Defense Donald Rumsfeld, though it predates his 2002 use, particularly within scientific inquiry, see Logan (2009), p. 712
[213] Miranda (2016), p. 675

Ctrl+Alt+Hack

Similar to *[d0x3d!]* in motivation and design, *Ctrl+Alt+Hack* is a card game with educational purposes designed by a team led by Tamara Denning. The game is intended to 'help increase awareness and understanding of high-level security concepts', but the designers emphasise that they 'focused on making it fun to play so that people would come back and play again.'[214] Players take on the role of white hat hackers working for a security consulting firm tasked with penetration testing other organisations. The end goal is to become CEO of the company by gaining 'Hacker Cred' (credibility) which are earned by completing missions.[215] Gameplay consists of initial phases of drawing, playing and swapping cards followed by players attempting to complete missions by throwing dice, after which the round is completed by awarding or subtracting Hacker Cred depending on mission successes and failures. Rounds are played until the winning conditions have been met and one player can declare themselves CEO.[216]

Figure 4: Ctrl+Alt+Hack game box and contents. Image from game website.

[214] *Ctrl+Alt+Hack* website
[215] *Ctrl+Alt+Hack* game rules, p. 2
[216] Ibid., pp. 4-6

As with *[d0x3d!]*, *Ctrl+Alt+Hack* uses an existing game for its gameplay mechanics, in this case Ninja Burger (designed by Steve Jackson).[217] The attendant benefits of this, as outlined previously, are recognised by the designers, and instead allowed them to concentrate testing time on the thematic game content.[218] The designers are keen to acknowledge their reliance on an existing product, with Steve Jackson's name and logo liberally advertised both on the *Ctrl+Alt+Hack* website and in the game's rule book.

Although not a wargame, *Ctrl+Alt+Hack* does recreate some of the mechanisms which engender positive learning outcomes from such games. It fosters a competitive environment, and because it gives players the ability to conceal information from each other using cards, this environment resembles one that might be found in cyber security, which is replete with hidden data and intentions. It also gives a role to luck through the use of dice, which forces players to make risk assessments on each of their decisions. Clausewitzian fog and friction and are therefore amply represented in *Ctrl+Alt+Hack* (see Section 4.6 for further discussion).

Cyber Strike

Another company with a cyber wargaming product is Roke Manor Research, who have developed *Cyber Strike* – formerly known as *CEMA*, borrowing the title from the acronym for Cyber Electromagnetic Activities.[219] Although not security classified, no information about *Cyber Strike* exists in the public domain, for example promotional material. The account of the game below is therefore entirely based a brief experience of the game during a personal demonstration at the Connections UK 2016 wargaming conference.[220]

Cyber Strike is a game for four to twelve players divided into two teams. The game board consists of a satellite photo of a city (fictionalised for the game scenario, but the image is of Beirut) divided into zones. The scenario imagines the blue

[217] Denning et al (2013), p. 917
[218] Denning et al (2013), p. 917
[219] FM 3-38 (2014)
[220] Author discussion with Roke Manor representative, London, 8 September 2016

team deploying into the city as an intervention/peacekeeping force in response to a dramatic decline in state stability. The objective of the game is for the attacking team to gain control of key zones of the city while the defending team seeks to frustrate these efforts. Players have at their disposal a deck of cards, each representing different cyber capabilities that would help with controlling zones, such as manipulating traffic lights to affect flow of transport or disrupting television and radio broadcasts to win the support of the populace.

The game is intended foremost as an educational tool, with learning outcomes being achieved in the discussions players have around the capability cards. Players must make decisions, as a team, about which cards they should play and why, prompting debate about the potential effectiveness of the capabilities the cards represent. Furthermore, the game facilitators encourage discussion that relates the cards to the real world, allowing players to contribute with their personal knowledge and expertise, and learn from others where such is lacking.

Insofar as it exposes players to a wide gamut of cyber terminology, *Cyber Strike* certainly seems like it has a lot of potential for creating learning moments along the lines sought in this thesis. With the right mix of players in a game session, the format of the game lends itself to constructive discussions. It is only a shame that more information about the game is not available for closer evaluation, as this limits its impact on the catalogue of cyber wargames.

3.4 Simulating unpredictability

Following on directly from the idea of using cards, the fourth aspect of note is the type of card which simulates unpredictable events. Unlike the world represented in games like chess, where the entire range of actions are known in a closed system, the real world contains elements outside human control and sometimes things do not perform as they should. The weather, for example, can be forecast but not prescribed. Two of the games analysed were particularly noteworthy for their use of cards simulating events outside the players' control.

Anti-Hack!

Anti-Hack! is a board game in which players attack and defend their computer networks. The game is for two to four players who take turns drawing four cards from a main deck, of which they may play two. There are four types of cards: attack cards representing hacking methods, defence cards representing anti-hacking tools, situation cards representing real-life events, and chance cards which inject gameplay differentiators. The objective of the game is to be the last surviving player, represented by a security level gauge which is depleted each time players are attacked and unable to defend.

Anti-Hack! is a mysterious wildcard in this list of games because no information about it is available beyond a short video demonstration.[221] There is no explanation of the game's origin, purpose or design methodology, nor do we know who should be credited with its development. Judging from the video the most likely use for the game is as an educational tool to introduce players to network defence concepts, but without access to the game material it is not possible to evaluate the game's pedagogical efficacy. Nonetheless, the appearance of event cards is noteworthy and it would be beneficial for more game material to be made public to see what kinds of events the game designers have included.

Privacy

One of the oldest games analysed in this chapter is *Privacy*, an educational card game coming out of the Visualisation and Other Methods of Expression (VOME) collaborative research project between Royal Holloway University of London, Salford and Cranfield Universities, along with Consult Hyperion and Sunderland City Council, which ran from 2009 to 2012.[222] Developed during this time, *Privacy* is a relative infant in terms of the history of wargaming, but in terms of educational cyber gaming it is one of the more mature products available.

[221] Chau (2016)
[222] VOME website

The game is for three to five players who each assume the role of a character – there are 11 available representing a wide range of internet users including Hacker, Bank Manager, and Online Dater. Players are tasked with managing information about themselves, divided into six categories: Social, Digital, Financial, Biographical, Security, and Health. In each turn, players must decide whether to keep information hidden in their hand, reveal it for everyone to see, or trade it with another player, before replenishing their hand from the deck. Gameplay moves from player to player until all cards in the deck have been drawn. There is also a set of event cards representing unforeseen occurrences that inject randomness and force players to react. At the end of the game scoring is determined by comparing the goals for each character with the current state of play.[223]

Encouragingly, the design of the game was driven by desired learning outcomes – an approach which is considered ideal in educational wargaming.[224] The VOME team tested *Privacy* with a total of around 130 participants across various organisations, evaluating it as a game, as an educational and social intervention, and as a research tool.[225] As a game *Privacy* was well-received in terms of its production values (graphics and tactile qualities of the cards), but feedback indicated that gameplay could be improved in a number of areas.[226] In terms of educational value, *Privacy* was successful in leveraging the social situation of play to stimulate discussion between players, but at the same time both feedback and observations revealed the game to be overly complex, with players focusing more on playing the game rather than the thematic content of the cards.[227] Finally, the team appraise the game as a useful precursor to other qualitative research methods, but do not see it as a replacement for more established approaches such as focus groups.[228]

As an early attempt at an educational game in the cyber security area, *Privacy* is a very good trailblazer. The transparency of the project aims, game design, and

[223] *Privacy* card pack and instructions (2012), pp. 15-16
[224] Barnard-Wills and Ashenden (2015), p. 154
[225] Ibid., p. 153
[226] Ibid., pp. 154-155
[227] Barnard-Wills and Ashenden (2015), pp. 155-156
[228] Ibid., pp. 157-158

deployment evaluation serve as an indispensable guide for future game development. Although not a wargame, there are nonetheless important lessons to learn from the VOME team's efforts, not least the inclusion of event cards, which are reflected in the design and deployment of the game for this thesis.

3.5 Marketplace

The final noteworthy aspect from the analysed games is a marketplace, specifically as implemented in *Decisions & Disruptions*, although the concept also makes an appearance in *Maelstrom*.

Decisions & Disruptions

Decisions & Disruptions (shortened to *D-D*) is a game about the security of industrial control systems created by a team at Lancaster University in the UK.[229] The purpose of the game is two-fold: it is an educational tool as well as a means by which to study player's decision-making processes.[230] Lessons learned are not necessarily contained directly within the game itself, but instead come out in the discussions players have in and around the game.[231]

D-D is for three to five players who assume the role of a newly-hired information security team for a company. The game lasts four turns, during each of which the players assess the company's current security situation and decide how to spend their security budget, after which an unknown security incident may or may not occur (these follow a script and occur depending on which security assets were purchased).[232] The company has a number of assets at two locations: an electricity-generating water turbine plant and an office, separated by geographical distance but connected via a network. Assets include computers, databases, servers, routers, and a SCADA industrial controller.[233] The players invest a budget of 100,000 credits (per turn) in a selection of defences spanning

[229] *Decisions & Disruptions* website
[230] Frey et al (2017), p. 1
[231] Author conversation with *D-D* developers, ACE-CSR Conference, Solihull, 11 July 2016
[232] *Decisions & Disruptions* game rules, pp. 11-12
[233] *Decisions & Disruptions* game rules., p. 29

both technical measures – firewalls, anti-virus, network monitoring, upgrades, encryption, CCTV – and non-technical measures – security training, asset audit, and threat assessment.[234] The budget does not allow the players to purchase every available defence, so a decision must be made by the group about where to invest their money based on the vulnerabilities they identify in the company's systems and the threats they perceive facing the company.

The developers of *D-D* demonstrate a clear understanding of gaming principles, particularly surrounding the game experience (see Section 2.2.5). The *D-D* game manual, addressing the game facilitator, stresses that 'the immersion of players is an important success criterion. You, the Game Master, do not want you players to think they are playing a game as if they were solving a riddle.'[235] To enable this, the manual provides scene-setting scripts the facilitator can follow[236], gives guidance on how to run and conclude the game[237], as well as a comprehensive set of frequently asked questions.[238] The provisions here give unseasoned game facilitators a high chance of running a successful game. As a criticism, a useful addition to the manual would be a set of suggested discussion points, helping the facilitator guide discussion towards learning outcomes.

The researcher's first-hand experience shows that the game is excellently put together, both in idea and execution.[239] The game generates discussion around a number of cyber security topics and does so at a level accessible to players with no prior knowledge. The primary drawback of *D-D* is that, similarly to *[d0x3d]*, the game provides a player versus environment setting rather than player versus player. Some of the benefits of adversarial play in wargames are therefore not realised, although this has subsequently been recognised by the designers and a 'red team vs. blue team' version has been suggested as a future extension for the game.[240]

---

[234] Ibid., p. 14
[235] *Decisions & Disruptions* game rules, p. 12
[236] Ibid., pp, 16-17 and 18-19
[237] Ibid., p. 20-22
[238] Ibid, pp. 22-27
[239] Based on author's experience with the game at ACE-CSR Conference, Solihull, 11 July 2016
[240] Frey et al (2017), p. 15

In *D-D*, the market for purchasing new security products is an excellent way to force players to make decisions based on limited resources, and if facilitated correctly – as this author has experienced it – also encourages players to articulate the reasoning behind their decisions. The process is enhanced by the fact that *D-D* is a team game, meaning players must externalise their thinking and debate with each other to arrive at a consensus decision. Recalling from Section 2.2.2 that exploring and understanding human decision-making processes is one of the key benefits of wargaming, *D-D* demonstrates that a marketplace can be an effective way of realising this.

Maelstrom

Maelstrom is an 'Attack Lifecycle Game Concept' developed by Shane Steiger, first showcased at the DEFCON 24 conference in August 2016. Similar to *Game of Threats*, *Maelstrom* is explicitly based on the Lockheed Martin Kill Chain, but also 'borrows concepts from several MITRE Frameworks, attack patterns matched from previous campaigns and from real "cyber security life".'[241] This influence is reflected in the game board (see Figure 5), which has players navigating through the various steps of an offensive cyber operation. *Maelstrom* is intended to be used for 'education, demonstration and evangelism' to a variety of audiences.[242]

The game is for two to thirteen players, with one player assuming a defensive role and all others attack. Attackers choose or draw a role from 12 available, for example State Actor, Script Kiddie, or Insider Threat which are represented by a token. They then select or draw an objective such as Exfiltration, Denial of Service, or Blackmail from a deck of cards. Both these selections or draws are kept secret from the other players. A number of cards are then drawn from Attacker and Defender decks by the respective players, and it is these cards which are used to drive the game forward. Each card outlines an attacking or defensive measure and its effect in the game in terms of how many steps the player takes forward or is knocked back in the Kill Chain. Play is alternated between attackers and the defender, so that the defender has a chance to respond to each attacking move.

[241] *Maelstrom* game rules (2016), p. 2
[242] Ibid.

The game ends either when all the attackers have been discovered and locked out of the system, or an attacker successfully reaches the end of the game board and completes their objective.

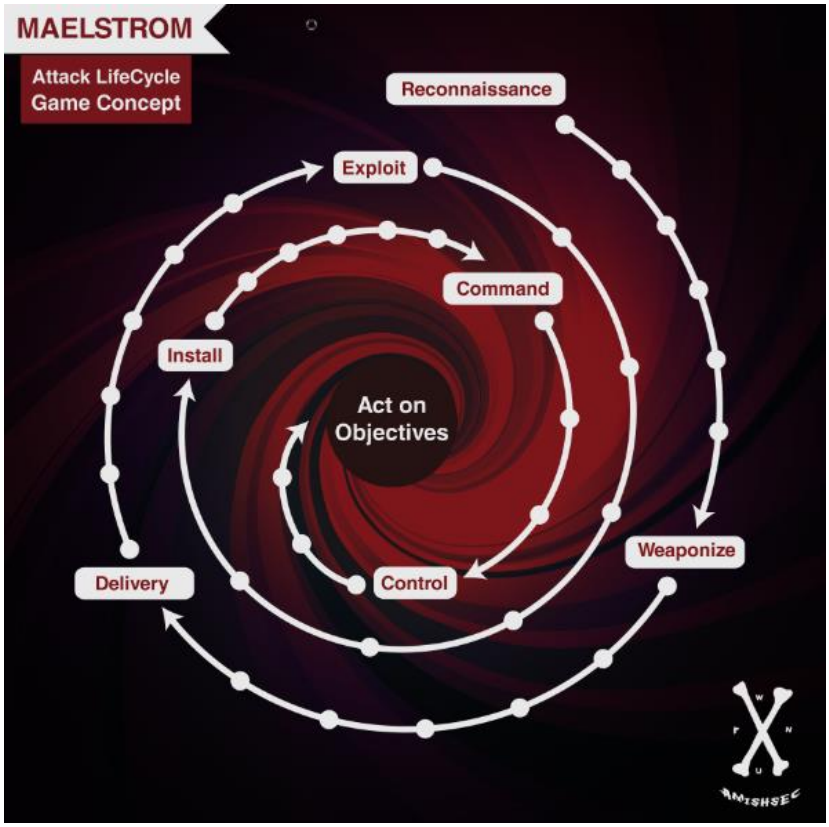

Figure 5: Maelstrom game board (from Maelstrom game rules (2016), p. 2)

To cater for different audiences, *Maelstrom* offers three levels of complexity. For high school level the designers recommend a 'quick and fun' version in which all roles and cards are initially drawn at random, and emphasise the importance of the 'story of play' in which players 'must supply a one or two sentence description of the way in which the card is being played.'[243] For college students the recommendation is 'tactical choices' where players select their cards based on the objective they want to achieve. Finally, termed 'Ninja Level', the advanced version of the game introduces 'strategic choices coupled with realistic challenges' and tasks players with managing a budget and buying only cards they can afford.[244]

[243] *Maelstrom* game rules (2016), p. 7
[244] Ibid.

In a demonstration video, the designers show how the 'story of play' really adds educational value to the game.[245] However, this also assumes some subject matter expertise on behalf of the players, as complete cyber security novices would not be able to articulate the details of specific attacking and defensive measures. Value can therefore be seen in the game by teaming up experts with non-experts (perhaps high-schoolers with college students and college students with seasoned professionals) to enable dissemination of knowledge through discussion. Interestingly, in the video the designers also express a preference for the tactical version of the game because the 'strategic [version] is too much like real life so it starts to feel like your job.'[246] Whilst this indicates that the marketplace function in *Maelstrom* achieves a degree of realism, the sentiment is an apt reminder that the element of fun is central to achieving engagement with games.

Chapter 3 Conclusion

The collection of 25 games analysed in this chapter represents the entire corpus of cyber wargames that fit the above criteria, as known at the time of writing. It may be that other games exist outside the author's sphere of knowledge which have escaped thorough research efforts, and in such cases these games would make valuable additions to further research.

In analysing virtually every available cyber security-themed wargame, hobby game, and educational game, this chapter serves as a much-needed reference point for others working in this space. The researcher's experience at the Connections US 2018 conference suggests that an increasing number of people, both wargamers and educators, are keen to explore cyber security but are unaware of many existing cyber games. Depending on the intended use, some of the 25 games covered in this chapter (plus the original game developed for the thesis) may be products that people can use in their current state, or else constitute starting points for further development or generate new ideas for

[245] SecureNinjaTV (2016)
[246] Ibid.

games. By highlighting the five most critical takeaways from the analysis it is hoped designers take these into account, ensuring that any new additions to the cyber wargaming corpus are robust and valuable.

Chapter 4: Designing a cyber security wargame

This chapter analyses the design strategy which underpinned the development of the original wargame for the thesis. As has been iterated previously, the most effective wargames are those which are designed with a specific purpose in mind, whether that be to impart a particular learning outcome or evaluate the result of a hypothetical scenario. For the thesis, the purpose of the game was to address one of the central research objectives:

- *Analyse the capacity for the game to create learning moments and enable players to share knowledge and ask the right questions.*

With such an open-ended objective in mind (the parameters of which are discussed in Section 5.1), the game needed to create an environment enabling multifarious learning experiences. Even if it might not be known beforehand exactly what kinds of learning moments might be created or questions players might ask, the game should contain myriad concepts and terminology from cyber security to stimulate inquisitiveness and conversation, giving players a chance to ask *something*. Across several game sessions with different audiences it would then be possible to analyse discussions players had to ascertain what the key learning moments were and whether players were indeed able to ask the right questions (see Chapter 6).

Following this experimental approach, this chapter does not provide an exhaustive overview of every game component or design minutiae. Instead, the chapter structures analysis according to the purpose served by particular game components and mechanisms. In this sense the chapter adheres to the standard set by related literature, where game design analysis is largely limited to those parts which materially impact players' learning experiences.[247]

[247] Notably Gondree and Peterson (2013) and Barnard-Wills and Ashenden (2015)

The chapter begins with an exposition of some design constraints which affected the development of the game, principally the balance between realism and complexity. Each of Sections 4.2 to 4.6 then opens with a rationale for why a concept was important to include in the game followed by an exposition of the relevant game components and mechanics. Section 4.2 outlines how the game conveyed the concept of various Entities[248] in cyberspace and links this to the UK National Cyber Security Strategy, which was the impetus for the main thrust of the game. Section 4.3 builds on this by showing how the game design included concepts surrounding strategic goal-setting in cyber security, again using the National Cyber Security Strategy as a case study. Section 4.4 shows how the game treated the large and complex topic of cyber attack and defence dynamics through various gameplay mechanisms, while Section 4.5 outlines how the game recognised the multidimensionality of cyber security through inclusion of geopolitical realities. Finally, Section 4.6 covers concepts around visibility and the difficulty of determining capabilities in cyberspace, before the chapter concludes with a summary of original contributions made.

Before delving into this material, it is imperative to note that the game design was not static but instead evolved over time. Over the course of the research, the game went through several iterations of development, sometimes resulting in drastic overhauls and sometimes in minor tweaks. Overall, it can be said that the game went through three distinct development stages: testing, refinement, and settled. In the testing stage, different game mechanics and components were experimented with to determine their suitability both for eliciting learning moments and for their playability – whether they created unnecessary friction in the game experience (for example by adding excessive complexity) or enhanced player engagement with the game. In the refinement stage the core game mechanics and components had been decided, but significant tweaks were required to ensure the game was balanced and there were no game-breaking features that might put an abrupt and unanticipated stop to the progress of the game. In the settled stage the game had reached a point where all mechanics and

[248] A brief note on terminology: throughout this chapter game components are treated as proper nouns, for example “Entities” or “Assets”. This is simply to differentiate them from their real-life counterparts, especially when used in the same sentence.

components served a useful purpose and were refined such that the game experience offered significant possibilities to elicit learning moments and enable players to ask the right questions. Of the 33 game sessions that informed this thesis, 10 were used game versions in the testing and refinement stages, while 23 used the final settled version of the game.

As a result of this progressive development process, the final version of the game differs from the version first conceptualised in many critical aspects and several of these are highlighted in the analysis. Refining a game along the development process is standard practice in wargaming, ranging from rule tweaks during playtesting to complete thematic overhauls.[249] In the sense that this thesis is experimental and explorational endeavour it was important to be able to not just tweak rules, but to adapt the game to respond to player requests or reactions. The final version of the game therefore represents the most optimal version in terms of maximising potential learning moments, which is a primary concern of the research, although as limited by the constraints analysed in Section 4.1.

4.1 Realism versus complexity in game design

One of the most fundamental challenges facing game designers is the balance between realism and complexity. Efforts to attain ever-increasing detail in game models lead to a higher degree of realism (or, less disjunct between the game and reality), but at the expense of an increase in the number of variables, counters, and rules required to play the game. This problem has also been characterised by at least one academic commentator as one of accuracy versus simplicity or realism versus playability.[250] Whatever the vernacular used, the main tenets remain the same: simple games are easy to play but not usually realistic, while realistic games tend to be more difficult to play. While greater realism may result in a richer experience, increasing the difficulty also ups the bar in terms of

[249] For example, Guy Debord's attempt to create a game of social commentary on 1970s culture which ended up being more of a simulation of battlefield logistics; see Galloway (2009)
[250] Sabin (2012), p. 19

participation, requiring a greater investment of time and energy, or prior knowledge and understanding.

Where on this scale the designer chooses to place their game depends on the purpose of the game and the target audience. Games for hobbyist wargamers, for example, tend to veer towards complexity because the players are interested in historical detail and the dynamics of the scenario.[251] For a more generalist audience, however, a game that sacrifices realism in favour of playability is more likely to gain traction. As an example, consider the difference between chess, a relatively simple and highly abstract game played by millions around the world, to *World in Flames*, an extraordinarily complex Second World War game of low abstraction but with a player base of perhaps a few thousand.[252] In this regard, Sabin's conclusions seem apposite: 'Above all, it is crucial to remember that a simple wargame that is played will be more instructive than a detailed wargame that is not.'[253] Furthermore, in terms of utility for education and training, great level of game complexity does not necessarily translate into real-life lessons. 'When you put a raw recruit behind gun A for the first time,' says David O. Ross, 'those six digits of accuracy go out the window.'[254] Given that this thesis is concerned with pedagogy for a non-specialist audience, it therefore seems pertinent to err on the side of simplicity and playability.

4.1.1 Length of rules

The desire to err on the side of simplicity and playability manifested itself in the game rules, the full set of which for the final version of the game can be found in Appendix B. The rules were printed on a double-sided A4 page and included in individual Player Dossier envelopes. Each player received an identical copy of the rules. The double A4 page was an important element of the development of the rules, and the game as a whole. As part of striving for playability, a simple rule set was required which players could grasp in a matter of minutes before getting

[251] Ibid., p. 20-21
[252] Exact numbers are hard to come by, but according to the *World in Flames Board Game Geek* listing, 2300 people own the game (*BoardGameGeek* website)
[253] Sabin, op cit, p. 30
[254] Ross (2008), p. 5

stuck into the game itself. More complicated wargames provide greater fidelity in their simulation, but, as attested by Sabin, can take several hours just to set up.[255] For the game for this thesis it was deemed more important that players could quickly engage with the game's content, so effort was made to not erect unnecessary barriers that may inhibit playing. As such, the one double-sided A4 page became a hard limit for the rule set, because this could be consumed relatively quickly (less than ten minutes).

The hard limit did mean that once the two pages had been filled with rules, any new additions would have to be accommodated by removing others. This meant that many good suggestions made by players for new gameplay mechanics were never implemented for the final version of the game. However, the final rule set reflects a balance of adopting new mechanics and leaving others out for new players to re-suggest. As is discussed in Chapter 6, thinking about alterations to game rules and components was one of the most effective methods for players to extract pedagogical outcomes. Many of the suggestions were therefore left out of future game versions on purpose, because it was felt more educational value was derived from having players suggest rules than play with them.

4.2 Key constituents of cyberspace

A crucial facet of cyberspace is that it is populated by a variety of actors ranging from governments and nation-states to organised crime groups and individuals. This is of course only a reflection of the physical world, but importantly, in cyberspace the relationships between these actors can significantly differ. The anonymity offered by technologies such as The Onion Router (TOR), for example, gives people and groups power to resist and reshape governance.[256] Indeed, this transference of power away from traditional governance structures underpinned John Perry Barlow's 'Declaration of Independence of Cyberspace' in 1996.[257] The extent to which Barlow's vision of independence has materialised can be debated

[255] Sabin (2012), p. 256
[256] As this author has argued with regards to the Silk Road online marketplace, see Haggman (2015)
[257] Barlow (1996)

and such a debate represents a discussion opportunity the game could be designed to prompt. It was therefore deemed important to include a variety of actors in the game for players to engage with.

The document which inspired the game was the UK National Cyber Security Strategy, first published in 2011 with an updated version released in 2016. The Strategy serves well as inspiration for a wargame because it creates just such an adversarial setting which wargames require. The Strategy makes it clear that the UK is under threat from a number of actors, including other nation states who seek to gain 'political, diplomatic, technological, commercial and strategic advantage.'[258] Although it stops shy of naming specific state actors, the Strategy nonetheless contains sufficient antagonistic language which labels cyberspace as a contested and competitive domain. A game based on the Strategy can therefore include not only 'friendly' UK actors, but also 'enemy' foreign actors.

The first edition of the Strategy contained an early recognition that building and promoting a safe and secure cyberspace requires synergy between the key constituents of UK society. This recognition resulted in a central trinity of actors promoted by the Strategy: individuals, businesses, and Government.[259] This trinity was the focal point of cyber security-related policies, but each of the constituents of the trinity were also assigned a share of the responsibility for a secure and prosperous UK cyberspace – it was not for the Government alone to act.

In the second (and current) edition of the Strategy, released in November 2016, the trinity of individuals, businesses, and Government remains, but it has been deemphasised and mutated from the previous iteration. Rather than appearing upfront in the introduction, the 2016 Strategy does not introduce the trinity until page 26 – a third of the way through the document – suggesting a decreased function for the trinity.[260] The Government, frustrated that 'a market based approach to the promotion of cyber hygiene has not produced the required pace

[258] National Cyber Security Strategy (2016), p. 18
[259] The UK Cyber Security Strategy (2011), p. 8
[260] National Cyber Security Strategy (2016), p. 26

and scale of change', has also been given a more prominent role in securing cyberspace, now leading from the front and shouldering more responsibility.[261]

From a game design perspective, the trinity of individuals, businesses, and Government, both as originally expressed in the 2011 Strategy and the altered version in the 2016 Strategy, begin to show what actors could be represented in a strategic cyber wargame. It could be also argued that these actors form a trinitarian relationship akin to the 'wonderful trinity' of government, people and military envisioned by Clausewitz to give balance to strategy.[262] Modelling the trinity of individuals, businesses, and Government in the game therefore creates scope to explore the tensions and interactions between the actors, taking inspiration from contemporary geopolitical contexts. The shift in the prominence of the trinity between the 2011 and 2016 versions of the Strategy suggests further changes may occur in the future and invites players to think about how the game design can be altered to reflect changing realities.

4.2.1 Entities

The game was designed with ten Entities representing the key actors as expressed in the National Cyber Security Strategy. Figures 6 and 7 illustrate the first version of the game board as originally conceptualised and the final version of the game board as implemented. The core trinities can be seen in the blue and red triangles, while two additional actors have been added representing a military/intelligence function and Critical National Infrastructure (CNI). These were introduced because, in the author's assessment, a conceptualisation of cyberspace which leaves these two out does not present a comprehensive picture. Indeed, both military/intelligence and CNI do appear at various points in the UK National Cyber Security Strategy, but they are not mentioned as part of the central trinity, hence why they are outside the blue and red triangles.

[261] Ibid., p. 13
[262] Clausewitz (1997b), p. 24; for more on the cyber trinities and Clausewitz, see Haggman (2014)

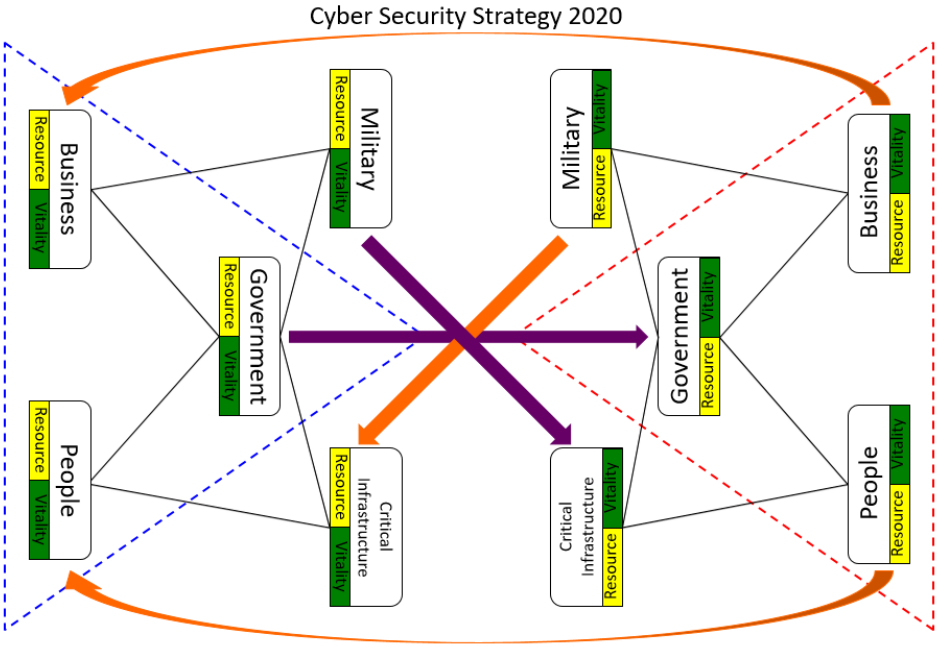

Figure 6: Version 1.0 of the game board

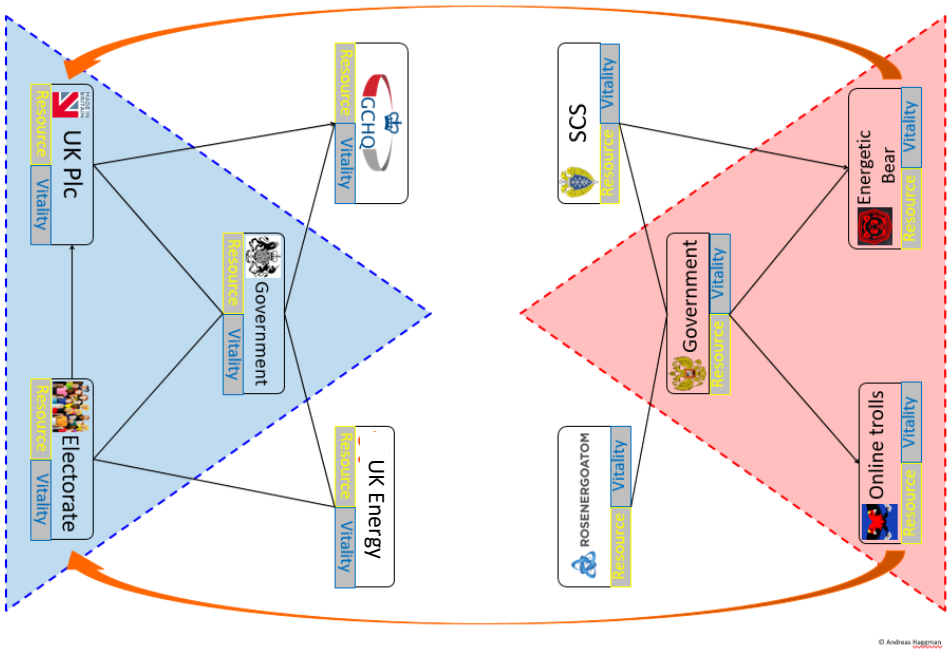

Figure 7: Final version of the game board

The game is laid out so that one side of the board represents friendly Entities, while the other represents a hostile foreign actor. In version 1.0 of the game the Entities were identically mirrored and anonymous, so both sides had the exact same Entities. In the final version the Entities have been given real-life identities

(UK and Russia), a decision which was taken with player engagement in mind. Early deployments of the anonymised game showed that players related the teams and Entities to real-world actors, so to further encourage this as a potential learning moment the actors were transposed directly into the game. Russia was selected as the game's antagonist because of the researcher's observations of Russian cyberspace activity, and the UK Government's assessment that Russia has been responsible for hostile cyber attacks targeting the UK.[263] While the Russian approach to national cyber security does not necessarily follow similar trinitarian tenets as the UK, these constituents are nevertheless present in their society, so representing the red side in this way can be justified and provides a potential discussion point for players.[264]

It is also worth reflecting on some of the representational politics that appear when assigning real-life identities to the in-game Entities. Using UK and Russia overtly in this way replays some of the rivalry and imagery associated with military and political contests between great powers. In this sense the most immediate comparison might be with the Cold War, where the Soviet Union, the great red state to the east – also incidentally on the right (east) of the game board as presented in Figure 7 – was directly opposed to the US and the West (see also Section 2.3.4). A more historically astute comparison might be to see the representations in the game as echoing the so-called 'Great Game' of the 19th century, where the UK and Russia contested a prolonged intelligence-led geopolitical battle for influence and control in central Asia.[265] The aptness of this comparison stems from the way the Great Game was shrouded in secrecy and underhandedness mirrors much of the activity that takes place in cyberspace today.

Another facet of the representations, especially that of Russia, is that it falls into a trap outlined by Andrew Foxall whereby a Russian '(geo)political identity' is assumed to exist, without interrogating the processes and manifestations of such an identity.[266] It is possible that the representation of Russia in the game is naïve

[263] National Cyber Security Centre (2017)
[264] Litovkin (2016); Gerden (2017)
[265] Hopkirk (2006), p. 123
[266] Foxall (2012), p. 236

in portraying Russia a homomorphic entity with clearly agreed national goals – although as outlined in Section 4.3.1 and Appendix A, attempts have been made to capture some of the divergent objectives of different actors on the Russian side of the game board. Indeed, the representation of Russia in the game is likely a product of the researcher's positionality as a Westerner with several years of UK education (see Section 5.2.1). Vincent Pouliot has argued that NATO (of which the UK is a part) 'thinks *from* their superior position to Russia [italics in original]' and in this sense the researcher has imposed their vision of Russia, replete with possibly erroneous or misinformed assumptions, onto the game.[267]

Crucially, the representational politics involved in using UK and Russia do not undermine their presence in the game. Drawing on analysis of statements by Vladimir Putin and Dmitry Medvedev, Edward Newman and Benjamin Zala have written that 'the international order and the evolving balance of power are at the heart of the rising power vision.'[268] This means that, whatever the shortcomings of the representation of Russia (and the UK) in the game, the great power contests which provided backdrops to both the Cold War and Great Game are still present today, at least in the Russian vision of the world. It therefore makes sense to use Russian and UK real-life identities for the Entities on the game board, because the design of the board with two directly opposing sides is consistent with the visions and actions of these actors in the real world.

The following sections provide some details about what each Entity represents in the game and some of the learning moments the representation can create.

UK Government and Russia Government

The two Government Entities represent the functions of the UK and Russian state apparatuses and correspond to the Government part of the trinity found in the National Cyber Security Strategy. In gameplay terms they play a pivotal role as the point at which new Resource (see Section 4.3.2) is gained and distributed to other Entities, inviting players to discuss the merits of such a centralised economic

[267] Pouliot (2010), p. 2
[268] Newman and Zala (2018), p. 876

model. Although there are no specific cyber security-related learning moments associated with the Government Entities, players are challenged to think about the role of the government as a driver in securing society, for example whether it should allow market forces to dictate proceedings (as in the 2011 Strategy) or take a more hands-on approach (as in the 2016 Strategy).

Electorate

The Electorate represents the individuals part of the National Cyber Security Strategy trinity. Here, individuals have been extrapolated to the entire civilian populace of the country, effectively equating it with the people part of Clausewitz's trinity.[269] Between version 1.0 and the final version, the people were relabelled as the Electorate, reflecting the UK's status as a democracy where the will of the people has a genuine effect on politics. The UK Government cannot enact policy without taking some regard of popular opinion, unlike some autocratic states which are genuinely top-down ruled.

A downside to using the Electorate label rather than people or individuals is that it automatically removes a swathe of the population from the game. Those under 18 years of age are not part of the electorate as they are ineligible to vote. Although this only represents some 20% of the UK population, it is also a demographic who have been born into the digital era.[270] The Millennial generation are largely unaccustomed to a life without smartphones and the Internet. As perhaps the sector of society most reliant on information technology, these people constitute a large target for cyber attacks and it is therefore critical they are attuned to security concerns and best practices. If a security culture can be instilled at this early stage, it can be maintained as they enter the labour force (and electorate) and become decision- and policymakers in their own right (or influencers to decision- and policymakers). Players of the game might not recognise the importance of this demographic, since they are explicitly left out, so the opportunity to educate current policymakers about the importance of getting

[269] Clausewitz (1997b), p. 24
[270] The Office for National Statistics (2017) provides a figure of 18.9% for under-16s, but does not provide a figure for under-18s.

youngsters' training and education right from the start is perhaps missed unless prompted by the game session facilitator.

Online Trolls

Online Trolls represent the people part of the trinity for the red team. This is a bigger departure from the original meaning of individuals/populace than the Electorate is, because whereas the Electorate represents a majority of the UK population, people trolling on the web are a small minority of the Russian population. However, the decision to characterise this Entity as Online Trolls was not based on their representativeness, but rather their mythology and potential effects. Originally a fairly benign activity, trolling is the act of goading someone into a response, mostly as an act of attention-seeking.[271] This is often done in online chatrooms or messaging boards and usually constitutes flippant remarks or deliberately incorrect or provocative statements that invite or force a discussant to respond. The term 'don't feed the troll' is a warning sounded by observers or participants to prevent others rising to the challenge – if the troll does not receive any attention it tends to fade away.[272]

Going back to the Soviet era, the Russians have a long history in controlling information to influence and deceive. Control and censorship of the media to limit the knowledge of the Soviet people is an example of defensive information operations. As an offensive example – what is often referred to as 'active measures'[273] – in the 1940s and 50s, the KGB (Soviet intelligence) had infiltrated the Polish resistance movement to the extent there were more intelligence operatives spreading misinformation than there were genuine members of the resistance.[274] Similarly, the collection of *kompromat* material (compromising material such as video tapes of extramarital affairs) on diplomats, dignitaries, and business people to later use as blackmail is a well-known tactic.[275]

[271] Cambridge Dictionary
[272] Phillips (2015), p. 160
[273] Kux (1985), p. 19
[274] For the KGB WiN operation, see Bagley (2007), pp. 118-132
[275] A thorough overview can be found in Ledeneva (2006), pp. 58-90

About the time the idea for the game was conceived in late 2015, academic understanding about Russian information operations in the cyber domain was gathering momentum. This all came to a head during the 2016 US Presidential elections, which the US intelligence community (representing 17 agencies) has by consensus concluded that Russia interfered in to get its preferred candidate – Donald Trump – elected.[276] Tactics used here included hacking into email servers of the Democratic National Committee and John Podesta (a close adviser to Trump's opposing candidate Hillary Clinton), and subsequently leaking stolen emails through WikiLeaks with the intent of defaming the Clinton campaign.[277] There was also an army of anonymous Twitter accounts, mostly automated bots, which would propagate news – both real and fake – to Clinton's detriment and Trump's gain.[278] Although Trump's victory in the election cannot be attributed solely to these Russian active measures (which the Kremlin vehemently deny), they have been judged to have had an effect.

In the wake of the events in the US, other countries with upcoming elections such as Italy[279] and Germany[280] became concerned about the integrity of their democratic processes and sought measures to mitigate any potential meddling by Russia. As an exceptionally active practitioner of information control, disinformation, deception, and influence, it was therefore important that Russia's role in these activities was represented in the game to give players an opportunity to engage with these concepts. Players should be able to recognise that threats in cyberspace do not just come from attacks on infrastructure that have destructive physical effects such as Stuxnet (more on this in Section 4.4.3), but also more subtle operations that have less obvious consequences.

UK Plc and Energetic Bear

UK Plc correlates with the business part of the National Cyber Security Strategy trinity. In the game, the Entity represents UK industry and business interests.

[276] Office of the Director of National Intelligence (2017), p. ii
[277] Rid (2016)
[278] Guilbeault and Woolley (2016); Ferrara (2016); O'Connor and Schneider (2017)
[279] Horowitz (2018)
[280] Reinbold (2017)

Energetic Bear represents the business part of the trinity for the red team. In version 1.0 of the game, the Entity had been conceptualised as a Chinese actor. In the years preceding the idea for the game, Chinese industrial espionage had been one of the main cyber security concerns for the West, with multiple attacks attributed to Chinese state or state-sanctioned actors. The infamous Mandiant APT 1 report, for example, singled out Chinese PLA Unit 61398 as a main culprit.[281] The results of such espionage have manifested in a number of ways. In a military case, the Chinese fifth generation jet fighter J20 Chengdu looks eerily similar to the US F-35 Lightning II, likely a result of F-35 blueprints being stolen from Lockheed Martin.[282] In a business case, AMSC, a US wind turbine software manufacturer, was the victim of espionage by Sinovel, a Chinese wind turbine manufacturer, who stole crucial code for operating turbines. Sinovel had been a customer of the AMSC, but rather than continue this relationship, Sinovel got the code they required through cyber espionage, causing AMSC to lose out on $800 million of business[283] and its stock value drop by 98%.[284] The case demonstrates how industrial espionage can directly serve the business interests of a country, meaning such actors can justifiably represent the business part of the trinity.

As the game developed and the red team was synonymised with Russia, it became necessary to find a Russian actor to fill the industrial espionage role. Energetic Bear, an Advanced Persistent Threat (APT) actor (variably known as Crouching Yeti or Dragonfly), is a hacking group affiliated with Russia and espionage attacks against industrial targets in the UK have been attributed to them.[285] (Note that Energetic Bear is not to be confused with APT28, Fancy Bear, another Russian hacking group who have been deemed the culprits of the attacks on the Clinton Presidential campaign.)

Similar to the inclusion of the Online Trolls, the presence of Energetic Bear in the game gives players an opportunity to explore some of the non-destructive threats

[281] Mandiant (2013)
[282] Gady (2015)
[283] Department of Justice (2013)
[284] Kappos and Passman (2015)
[285] Jones (2014); Kaspersky Lab (2014); Symantec (2014)

that emanate from cyberspace. These lessons are enhanced when combined with other game components such as the Ransomware Black Market Asset (discussed in Section 4.4.2), which introduce additional cyber security concepts through impactful gameplay mechanics.

GCHQ and SCS

Both UK and Russia have dedicated intelligence agencies for cyberspace. In the UK, the responsibility lies with Government Communications Headquarters (GCHQ), which is primarily a signals intelligence agency, but also has a role in information assurance and critical infrastructure protection. Other UK intelligence agencies – MI5 and MI6 – as well as various military units – 77 Brigade and Joint Cyber Reserve – also operate in cyberspace, but GCHQ is a more useful actor for this game as it has more prominent national defence remits and is therefore more closely linked to the other Entities on the game board. These defensive functions are, since October 2016, encapsulated in the National Cyber Security Centre, though because the Centre is a part of GCHQ it does not merit separate representation in the game.[286]

In Russia, the Special Communications Service (SCS) has a similar role to GCHQ, though organisationally it is different because SCS is a division of FSB, the Russian internal security service (equivalent to MI5). With SCS having largely defensive tasks, GRU, the foreign intelligence agency (equivalent to MI6), holds more of the offensive cyber responsibilities. Despite this, SCS are more fitting for the game as they are a specialised agency more closely akin to GCHQ, thereby preserving the mirrored setup of the game.

Encapsulating multiple agencies with diverging missions into one Entity could potentially mislead players who have no prior understanding of the UK or Russian intelligence communities and militaries. The representation in the game puts the onus for all cyber attack and defence on GCHQ and SCS, which may not be useful for players who need a more nuanced understanding of how these agencies

[286] National Cyber Security Centre website

function. This problem is a manifestation of the need for balance between realism and complexity. It would be possible to design the game to include whole intelligence communities, but this would sacrifice playability, which is the priority design guideline.

UK Energy and Rosenergoatom

Critical National Infrastructure (CNI) encompasses a variety of sectors including energy, transport, telecommunications, and finance. Version 1.0 of the game treated these as an amorphous Entity, so the process of narrowing it down to a specific sector and actor for the final version provided an opportunity for more precision. The decision to settle on the energy sector was largely the result of a joint UK-US exercise focusing on cyber threats to nuclear power plants, which was in the news concurrently to the game design process.[287] Nuclear can perhaps be considered an especially critical part of national infrastructure, partly due to its role in electricity supply, but also because any faults in a power plant can have catastrophic consequences, as demonstrated at Chernobyl in 1986 and Fukushima in 2011. Through vivid imagery associated with these disasters, nuclear might therefore serve a useful purpose in capturing players' imaginations.

Although not explicitly referenced in the game, the UK the primary nuclear operator is EDF Energy, which is due to construct new reactors complementing those already in operation at Hinkley Point. Intriguingly, EDF is a French company building UK nuclear plants with Chinese money. This complicates the relationship between EDF and the UK Government. By extension, the French and Chinese governments are also involved, giving the initiative a diplomatic as well as a business dimension. However, as neither EDF nor the French or Chinese are represented in the game, so the diplomatic dimension will remain unexplored in gameplay, though is simple to inject into post-game discussions.

[287] And discussed further in Haggman (2016)

In Russia, the nuclear industry is centralised with a state-owned operator and regulator – Rosenergoatom. Given this centralisation, the relationship between Rosenergoatom and the Russian Government is simpler than in the UK.

It is important to recognise that concentrating on nuclear energy production at the expense of other CNI sectors also limits how players think about this area. Attacks on national financial systems may not provide the physical impact of a nuclear meltdown but could nevertheless have significant impact. As an example, a nine-hour outage of a Bank of England clearing system in October 2014 delayed almost £290 billion worth of payments, causing disruption to property purchases due to be completed that day.[288] A deliberate and sustained attack on such systems could cripple the economy. Similarly, Britain runs an import/export deficit on every food supply apart from whisky.[289] Retail grocers operate a 'Just-in-Time' stock level with only a few days' worth of supply, so an attack which disrupts imports or transport systems that carry this food to all parts of the country can cause widespread havoc.[290] Because the game does not explicitly consider CNI sectors such as these, players' learning moments are likely to be limited to nuclear energy and electricity supply.

This is a shortcoming of the learning potential of the game, but one which is difficult to address because it is another manifestation of the need to balance realism and complexity. Although all sectors of CNI are important and players should be educated about them, the UK Government defines 13 such sectors.[291] Including each one would increase the complexity of the game and detract from playability, which has already been justified as the priority factor in the game's design.

[288] Deloitte (2015)
[289] Parliamentary Office of Science and Technology (2017), p. 1
[290] Baker and Morgan (2012), pp. 3-4
[291] Centre for Protection of National Infrastructure website

4.2.2 Relationships between constituents

In the same way that each part of Clausewitz's trinity relies upon the other two to support it, so do each of the Entities in the game relate to each other. It is important for players to understand that cyber security in a networked society cannot be the sole responsibility of one actor. As an example, even if the military has high-grade protection on its own assets and communications, hostile actors can attack more vulnerable targets in the industrial supply chain, such as the case of Lockheed Martin and the F-35 outlined previously. Similarly, criminals may be deterred from attacking the infrastructure of banks, who invest considerable resources into cyber defences, but can instead target unknowledgeable customers who unwittingly give criminals access to their bank accounts via telephone scams or email phishing links.

Relationships between Entities on the same team are represented on the game board by thin black lines joining the Entities, some of which are arrows representing one-way relationships. In gameplay terms the lines dictate how Resource, which is the in-game currency, can be transferred between Entities and which Entities take damage in case of an attack (see Section 4.4.4 for further discussion). There are 16 possible linkages in total, but only 12 are actually joined up. The sections below analyse a selection of the relationships and the learning moments associated with them.

UK Plc – GCHQ

The industrial-military complex is well-documented and in version 1.0 of the game this relationship was intended to reflect this close intertwining of business and the military.[292] In this complex, the military conveys its needs to industry who oblige with products for the military to purchase. It is a loop of ever-increasing expenditure where projects run into billions of Dollars/Pounds. In the final version of the game, where the military/security Entity had been identified explicitly as an intelligence agency, the relationship was refined to a more nuanced

[292] Hinshaw and Stearns (2014), pp. 317-318

understanding of how these Entities interact. Although there is certainly an intelligence-industrial complex, the relationship in the game is only partly concerned with the supply of products. It is true that certain hardware and software is required for cyber security and cyber operations, but most of these are not autonomous and require users to operate them; and whereas there are many skilled tank drivers and jet pilots, there is a dearth of skilled cyber experts. Across all of industry globally there will be a shortage of some 1.5 million people in 2020.[293] Of the ones that exist, most choose to work for private companies where they can command significant salaries which the public sector – including military and intelligence – are unable to match. In response, the UK created the Joint Cyber Reserve to tap into this pool of expertise, staffing it with part-time volunteers from industry.[294]

The potential learning moment here is for players to understand that the link between UK Plc and GCHQ is less about sale of products and more about the transfer of expertise. Indeed, the fact that the relationship is a one-way arrow on the game board forces this issue: business can lend their people to the agency, but the agency cannot pay businesses for their products or people. Although this is a gross simplification of a complicated issue, the representation is intended to stimulate debate rather than act as a realistic simulation.

UK Government – Electorate

The UK Government's relationship with the populace is symbiotic. The Government derives its legitimacy from the people through parliamentary democracy and the people are a source of Government income through taxation. Similarly, the people rely on the Government to provide the functions of the state in national security and legislation, and for financial support through social security and development programmes (such as tax relief or property help-to-buy schemes). If the people become discontent or disillusioned, perhaps as a result of adversarial disinformation operations (such as the campaigns discussed in Section 4.2.1), this sentiment may be passed on to the Government through

[293] Zadelhoff (2017)
[294] 'Working for JFC' website

protest or diminishing electoral support. Likewise, a decline in the Government's ability to perform its functions will cause a negative effect on the population. As such, the relationship here is two-way, with either Entity being able to transfer Resource to the other, and likewise suffer when the other does.

The intention of this relationship, combined with the Attack Vector enabling Online Trolls to target the Electorate (see Section 4.4.3), is to demonstrate how the populace can become a burden on a democratically elected government. In many ways, the people form the soft underbelly of an otherwise resilient society and can be a source of frustration for a state attempting to create a secure and prosperous society. Government and business networks may be hardened against attack with firewalls and cryptographic protocols, but the sentiment of the people cannot be defended in the same way. The tensions between the Government and Electorate enables players to explore the difficulties inherent in running a modern liberal democratic country and their implications for cyber security.

Russia Government – Online Trolls

There was a need for this relationship to be reconsidered between version 1.0 and the final version of the game, because the Online Trolls Entity does not represent the general populace. Instead of a two-way link, it was decided to make this a one-way arrow where the Government could transfer Resource to the Trolls but could not receive any in return. Combined with the lack of relationship between the Trolls and Rosenergoatom, this effectively turns the Trolls into a Resource sink where any Resources transferred in must be spent as it cannot be transferred out.

This relationship is intended to signify that the Trolls are under some modicum of control of the Russian Government but are still a force unto themselves. The Government provides cash for the Trolls to conduct their nefarious activities, but cannot rely on a return on the investment, nor a return of the investment. Instead of launching trolling operations, the Trolls may spend the Resource to reinforce their own position, or just hoard it. In real life, mercenary hackers recruited for information operations are not necessarily beholden to any national allegiance and may well prove a waste of money. Consider a stereotypical example where a

teenaged computer enthusiast receives a few thousand Roubles from a shady source to generate a fake news campaign; but instead of fulfilling this task, they publish one or two stories then squander the remaining money.

It is notable that this relationship is also favourable to the Russian Government because they can distance themselves from the trolling activities. If attacks or information operations cannot be attributed directly to the Russian state, there are far fewer repercussions on the international stage. Representing some of these nuances in the game (see Section 4.4.5 for further discussion of attribution) offers players opportunities to explore these topics through both gameplay and further discussion.

GCQH – UK Energy and SCS – Rosenergoatom

The lack of a direct relationship between these Entities is a result of the military Entity in version 1.0 of the game being envisioned as a more offensive force (see Section 4.4.3 for discussion of Attack Vectors). The military was primarily tasked with attacking the enemy's CNI and did not have any links to its own side's CNI. In the final version of the game, with the Entity now being an intelligence agency, there may have been scope to revise this relationship. In 2016, the UK public cyber security apparatus was restructured around the National Cyber Security Centre (NCSC), whose remit included that previously held by the Centre for Protection of National Infrastructure (at least its cyber functions). Since the NCSC is a part of GCHQ, there is a real direct role for GCHQ in the defence of CNI, and the same can certainly be said of SCS and Rosenergoatom. It would therefore have made sense to create a relationship on the game board between these Entities.

There are two reasons why a design decision was made to not link GCHQ to UK Energy and SCS to Rosenergoatom. The first was that from a gameplay perspective this link would have made the respective sides too well-connected, making it easier to marshal Resource between the different Entities and limiting the amount of decisions the players had to make. The second reason, which became apparent after a few game sessions, was that the absence of a

relationship was conducive to creating learning moments. As evidenced in Section 6.2.2, several players noted the lack of relationship, commenting that this was an inaccurate representation of reality. Fewer such comments were made about any other relationships on the game board (whether it was regarding the absence or presence of a link), so omitting the link made sense from the perspective of the main thesis question: if the absence of a link caused players to react and have a discussion it was doing its job as a pedagogical device. Omitting the relationship in the final version of the game was therefore a deliberate decision to prompt players to comment on the lack of relationship and thereby enhance learning moments created by the game.

Overall assessment of relationships

The way the relationships are set out in the final version of the game makes gameplay strategies significantly different from version 1.0. Whereas in the earlier version both teams had identical pathways to move Resource around, in the final version the UK has more links and therefore more opportunity to marshal Resource to where it is needed. On the other hand, increased interdependency also leads to a higher chance of contagion when things go wrong. The Russian setup limits this risk through compartmentalisation at the cost of not being as flexible in moving Resource. In some sense, this reflects a UK society with better interconnectivity and cohesiveness, but also the weakness of democracy compared to a more centralised system of governance. Although these are subtle points to pick up, several players did recognise the crux of the setup and were able to discuss it during game sessions (see Section 6.2.2), vindicating the final design of the game board as a tool for educating players about the key constituents of cyberspace and the interactions, dependencies, and tensions between them.

4.3 Strategic goal-setting in cyber security

In the past decade, many states have developed and documented some form of national strategic approach to cyber security. As of January 2018, the NATO

Cooperative Cyber Defence Centre of Excellence listed 81 countries plus two intracontinental unions (European Union and African Union) that had published national cyber security strategies.[295] The ubiquity of these documents suggests that states have recognised the importance of cyber security and of tackling its challenges in a well-planned manner. Guidance from the European Union Agency for Network and Information Security suggests that the first step in developing a national cyber security strategy is to set out 'vision, scope, objectives and priorities.'[296] In the 2016 UK National Cyber Security Strategy this is summarised as the vision that 'the UK is secure and resilient to cyber threats, prosperous and confident in the digital world,' with objectives to 'defend, deter and develop'.[297]

Given that a target audience for the game are policy- and decision-makers whose role it is to write, or inform, strategy (either in a national or business context), it was deemed important that the process for developing a cyber security strategy was represented in the game design to some extent. This was realised by including the idea of strategic goals: Objectives which players had to achieve to win the game. All games require winning and losing conditions, otherwise they are not games.[298] In early draft versions of this game, the aim for the teams was simply to annihilate the opposition, but this represented an overtly bellicose scenario where the two teams had reached a stage of all-out cyber warfare and left little room for players to think about more nuanced strategic goals. For this reason, additional, more peaceful, Objectives were added to the game, delivered to players by means of individual dossiers for each Entity.

In the first versions of the game, these Objectives were non-quantifiable, intended primarily to elicit debate from the players in order to create learning moments. The Electorate Entity, for example, had an Objective which said:

> "Hold Government accountable – whenever the Government makes a decision or performs an action (such as transferring resources or attacking) you must demand clear reasoning and justification for this."

[295] CCDCOE website
[296] ENISA (2016), p. 14
[297] National Cyber Security Strategy (2016), p. 9
[298] Although there is serious divergence in academia about this. See Salen and Zimmerman (2004), p. 79 for a concise summary.

While the UK Government's reciprocal Objective was:

> "Please the people – the UK is a democratic country and without popular support your mandate to govern will dissipate. You must therefore ensure the Electorate are happy with you, which entails supporting them in achieving their goals."

Crucial feedback from playtesting showed that players did not understand how these Objectives would be measured. The original thought had been that success would be decided by consensus – in the Electorate case above it would be up to the players to determine whether they felt the Government's actions had been satisfactorily justified. Although the pedagogical purposes of this approach were recognised, the playtesters questioned its feasibility as a gameplay mechanic, in many ways capturing the debate around the efficacy of matrix games as analysed in Section 3.1.2. In reaction to this feedback, all subsequent versions of the game only had quantified Objectives that could be easily measured, and a Victory Points mechanic (earn Points for achieving Objectives, most Points at the end of the game wins) was added to make the whole system transparent. The Victory Points mechanic was only implemented reluctantly because wargaming literature warns against it; players can become fixated with chasing arbitrary points and lose sight of the wider lessons of the game.[299] Nonetheless, because the mechanic is easy to understand it makes the game more playable, which was the overriding design concern.

4.3.1 Player Objectives

The following sections highlight some of the Objectives as presented in the final version of the game and links these to lessons players might learn. All player Objectives can be found on the dossiers in Appendix A.

[299] Frank (2014), pp. 9-10

GCHQ Objectives

GCHQ has one objective:

1. Recruitment drive – swell your staff numbers by increasing Vitality every quarter (end of March, June, September and December).
   +1 Victory Point for single quarters
   +3 Victory Points for two consecutive quarters
   +5 Victory Points for three consecutive quarters
   +7 Victory Points for the entire year
   (Not cumulative)

The lack of skilled personnel in cyber security has already been discussed in Section 4.2.2, especially with regards to the public sector. This Objective tasks the player with redressing this skills gap by growing personnel numbers. Although seemingly straightforward, the Objective is quite difficult to achieve because of other pressures on the GCHQ Entity in the game, notably the need to access the Black Market which is a drain on Resource. The UK team can of course divert Resource from UK Plc to GCHQ, but this will compromise UK Plc's ability to achieve their Objective. There is therefore tension here the UK team must manage, and players can experience some of the difficulties that the UK policymakers are currently grappling with, giving players insight into real-world cyber security policy problems.

In earlier versions of the game, GCHQ's main objective had been to directly compete with SCS in a cyber arms race, but this was changed with the removal of the UK Government – Russia Government Attack Vector (see Section 4.4.3). With the UK's in-game stance becoming more defensive, in line with its real-world stance, it was deemed more appropriate to align Objectives with this defensive outlook so that learning moments for players would more closely match the real-world scenario.

Energetic Bear Objectives

Energetic Bear has one Objective:

1. Those who can't, steal – grow your business by whatever means possible.
   +1 Victory Point for having more Vitality at the end of April than the start of the game
   +3 Victory Points for having more Vitality at the end of August than April
   +5 Victory Points for having more Vitality at the end of December than August
   (Cumulative)

This Objective represents the business interests of industrial espionage (also discussed in Section 4.2.1). Espionage is conducted to gain an advantage over a competitor or reveal intellectual property or other trade secrets which can be sold for profit. The way the Objective is formulated for the final version of the game makes any damage Energetic Bear causes to UK Plc a secondary concern, though in earlier versions of the game this was the primary aim. The change in priorities puts less emphasis on the offensive aspects of cyber security, instead encouraging players to think about more nuanced strategic goals and relationships. Is it more advantageous to damage a competitor than it is to promote innovation and growth within your own company? Does cyber industrial espionage represent a good return on investment versus the risks associated with attribution? Is industrial espionage conducted with the backing of the state, whether tacit or overt? These are important questions which players can discuss and the answers to the questions also help stimulate thought about how to assume an appropriate defensive posture against industrial espionage.

SCS Objectives

SCS has one Objective:

1. Win the arms race – have a better cyber arsenal than the UK.
   +2 Victory Points every month you end with more Attack Assets than the UK's Defence Assets

This Objective represents a Russian ambition to gain an upper hand in technical capabilities over the UK by hoarding vulnerabilities and exploits from the Black Market (see Section 4.4.2). Although the title of the Objective says it is an arms

race, the race is one-sided because in the final version of the game the UK does not have a corresponding Objective to participate in the race. The UK can still become involved by competing with Russia on the Black Market, but they are not rewarded for doing so, other than potentially denying Russia Black Market Assets and resultant Victory Points. Intriguingly, the Objective rewards hoarding of any acquired Assets, though there will inevitably be tension with Energetic Bear and Online Trolls who want to use the Assets as part of their offensive efforts. The Russian team must therefore continually evaluate whose Objectives they want to pursue throughout the game and how they might most optimally use Black Market Assets. Players' engagement with these issues closely resembles trade-offs facing real-world policymakers. Working out when to 'burn' undisclosed zero-days (software exploits with no previously known mitigation), for example, is a very inexact science, though efforts exist to create more precision in this space.[300] In terms of creating learning moments, understanding the value of certain cyber capabilities and deciding when to deploy them is therefore a worthwhile topic for players to be able to explore.

4.3.2 Managing limited resources

The policymakers who formulate national cyber security strategies need to consider the context of their own countries, not only in terms of threats facing them but also resources available to mitigate problems. Even for states with large economies there are usually not enough resources (both people and money) available to solve every problem – hence why the ENISA guidance on national cyber security strategies emphasises that prioritising desired outcomes is a key first step.[301] For game players to be able to engage with this tension, it was important that the balance between resource availability and task priority was represented in the game.

The representation takes the form of two sets of counters which the players must manage for each Entity: Vitality and Resource. Vitality represents the well-being of the Entity, which is purposefully nebulous to allow players to think about what

[300] Axelrod and Illiev (2014)
[301] ENISA (2016), p. 14

well-being means for each Entity. For people it might mean health, happiness, safety, security, and/or financial stability; for businesses it might be a productive workforce and thriving trade; and for a government it can be social stability, national security, and legislative capacity. In pure gameplay terms, however, Vitality is the hit points of the Entity and it should never reach zero.

Resource represents the wealth of the Entity and can be thought of as a monetary resource which the Entity can spend. However, in line with the idea of skills shortage and transfer as discussed previously, Resource can also represent non-tangible assets. In order to convey the pressures associated with prioritising strategic goals, the number of Resources available to players is never sufficient to achieve all their Objectives. Players must therefore decide which Objectives they will pursue, perhaps re-evaluating these decisions as the game progresses and other Objectives become more attainable. The pedagogical idea is then to discuss these decision processes and allow players to reflect on why they chose to pursue certain Objectives instead of others. If players can relate their in-game decisions to real-world dilemmas facing policymakers, lessons can be learned about the difficulties of formulating national cyber security strategies with limited resources.

From a game design perspective, it is worth noting two physical aspects of the counters. Firstly, the colours chosen – blue for Vitality and yellow for Resource – took into account colour blindness. According to the UK National Health Service, colour blindness affects the red-green spectrum more than any other colour, so red and green were avoided for the counters. [302] Secondly, the tactility of the counters was important. For the earliest versions of the game, small square chits had been constructed by simply printing and cutting regular paper, but these proved flimsy and difficult to handle. Instead, small wooden cubes were procured, which are a mainstay of board gaming. These are easy to handle and stand out visually on the game board. Feedback from players in multiple game sessions indicated that the cubes had a satisfying feel – there is something more meaningful to picking up a wooden cube that a small piece of paper. These points are worth keeping in mind for future game designers.

[302] NHS Colour vision deficiency website

4.4 Cyber attack and defence dynamics

Not all wargames involve combat, but most do, and this game is no exception. Inclusion of combat in the game served multiple pedagogical purposes. From the setup of the game board and the Objectives, players could learn lessons about key actors in cyber security and some of the tensions between them, but cyberspace is an antagonistic arena with a variety of threats, so it was important that players were exposed to cyber attack and defence dynamics in order to engage with key concepts in this field and how combat in cyberspace might be different from combat in physical space.

4.4.1 Dynamics of time progression

Time progression is not straightforward when modelling combat in cyberspace. Cyber is often said to be a fast-moving medium, yet this is only true of actual operations.[303] The deployment of a cyber capability can be near-instantaneous, but the actual brunt of the work is often done in the lead-up to the attack. A distributed denial of service attack, for example, can be executed in a matter of minutes, but building the botnet of computers used to mount the attack could take several months. The question is how this could be represented in a wargame. If the total time span of the game is from the beginnings of botnet building to the launch of the actual attack, the time span is several months. It might then be reasonable that one turn in the game represents one month of "real" time. But what occurs on the final turn of the game? Suddenly, this turn only represents a few minutes of "real" time, when all the others had represented a month.

Similar time distortion dynamics are evident in the aftermath of cyber attacks. It may only take a few minutes for a hacker to steal some vital documents, but the repercussions are not necessarily immediate. An apt example of this is the Sony hack of 2014, where hackers managed to obtain copies of millions of emails held

[303] Howard (2017); Jacobsen (2014), p. 14; Applegate (2012), p. 186

on Sony's servers, which were subsequently leaked to the public. This caused not only great inconvenience and embarrassment for Sony staff and executives, but disparaging remarks made about certain film actors also harmed their business relationships.[304] Furthermore, when North Korea was accused of orchestrating the hack, the situation escalated into a diplomatic event resulting in US President Barack Obama invoking additional economic sanctions on North Korea.[305] All of this of course played out in the weeks and months following the actual cyber attack, meaning a wargame based on this episode would likely have turns representing different amounts of real time.

Wargaming literature recognises that manipulating time in this way can be disorientating for the players, which can lead to disillusionment and disengagement.[306] With the primary aim of designing a playable game that players would first and foremost engage with, it was therefore decided that each turn in the game would represent the same amount of real time: one month. This meant that the timescales of some actions within the game, such as launching cyber attacks, would not fit into the timescales represented by each turn. However, from a pedagogical standpoint, it seemed more effective to deliberately create a misrepresentation which players could identify and discuss, than to attempt to create an accurate simulation.

Gameplay phases

In many wargames, turns are subdivided into phases, for example movement and combat. A giant of the wargaming hobby, Jack Scruby, recommends that that novice players begin with an 'alternative move' game where one player takes a full turn consisting of all phases, followed by the opponent taking a full turn of all their phases. As players become more familiar with wargaming mechanics they can proceed to more complex rule sets with intertwined turns or simultaneous phases.[307] The game design for this thesis assumed no prior wargaming

[304] Stedman (2014)
[305] Executive Order 13687 (2015)
[306] Kainakara (2003), p. 14
[307] Scruby, pp. 13-14

experience on behalf of the players, so, following the advice of Scruby, a simple alternative move approach was selected.

In reality, of course, war does not involve one side idly awaiting their turn while the opponent manoeuvres and fires. In that respect, the game with simultaneous moves is perhaps the best reflection of real warfare. However, this would still not be a true characterisation, as strategy and tactics often revolve around reacting to an opponent's actions, or proactively anticipating them. As such, war is not a balanced activity where each side get a fair share of 'action time' – compare, for example, an army geared towards Blitzkrieg-style tactics which can pick and choose the time and location of their attacks, against a slow and immobile defender which could only try to absorb the assaults as and when they come.

This type of warfare is probably the most apt metaphor for the current state of affairs in the cyber domain. It is commonly accepted that cyber attackers have the upper hand over defenders.[308] Defenders, especially anti-malware vendors, are constantly reacting to new threats and attacks and this will remain the case as they have no remit (legal or otherwise) to counterattack and try to regain the initiative. Arguments have been made to allow private companies to 'hack back' in response to a cyber attack[309], but for the time being this privilege is reserved by nation states.[310] Depending on the entities represented in a wargame, this can be relatively easily modelled by simply removing the defender's ability to conduct offensive combat (see discussion of Attack Vectors in Section 4.4.3). The point, however, is that despite its simplicity, an alternative move game is not necessarily an inaccurate method of representing the dynamics of defenders continually reacting to attackers in cyberspace. To reinforce this point, the game rules stipulated that Russia always conducted actions first each turn, putting the UK in the position of a reactive defender (see Appendix B).

[308] Convertino et al (2007), p. 72; Sanger (2012), p. 208; *The Economist* (2012)
[309] For example Denning (2008), pp.422-426; Rosenzweig (2014), passim.
[310] Notably in the UK National Cyber Security Strategy (2016), p. 47

4.4.2 Dynamics of cyber capability development

The third objective of the UK National Cyber Security Strategy states that the UK 'will acquire and strengthen the tools and capabilities that the UK needs to protect itself from the cyber threat.'[311] The Strategy proceeds to outline the methods by which these capabilities will be acquired, which largely involve stimulating skills growth, industry innovation, and academic research. All of these are worthwhile discussion points for players and the game design incorporates many of these dynamics through player Objectives and Resource management. An aspect of the Strategy where capability development is less transparent, however, is in offensive cyber capabilities. Although the Strategy notes that the UK will seek to strengthen and develop offensive cyber tools, exactly how this will be achieved is not described.[312] This is largely owing to the often-secretive nature of cyber security (as discussed in Section 5.2.2) but could also be a result of offensive capabilities being acquired through less salubrious means.

A Black Market for cyber capabilities

In the game, the primary method of acquiring cyber capabilities is through the Black Market, where players can spend Resource to gain Assets that modify in-game abilities (see Figure 8). The Black Market was partly inspired through first-hand experience with *Decisions & Disruptions* (see Section 3.5), which implemented a purchasing system for in-game capabilities. This system was very effective in terms of forcing players to make decisions about how to spend their limited in-game currency and, importantly, discuss the rationale behind these decisions. Implementing a similar system in the game for this thesis therefore seemed to be a pertinent method to emulate some of the learning outcomes of *Decisions & Disruptions*.

[311] UK National Cyber Security Strategy (2016), p. 55
[312] Ibid., p. 51

Figure 8: The in-game Black Market

In real life, sites exist on the dark web where vulnerabilities, exploits, and other cyber tools are traded for up to six-figure sums.[313] The association with the dark web is why the Market in the game is Black. However, this is really a misnomer, because many of the Assets available to buy on the game Market are legitimate tools or programmes. Some players have identified this, but as far as terminology goes, Black Market has a certain allure to it which is both a source of amusement and serious discussion, for example the ethics around the UK Government paying money to the Black Market. In this sense, the Black Market is able to spur a greater range of discussion than the purchasing system in *Decisions & Disruptions*, thereby creating more learning moments.

Black Market Assets

There are nine different Assets available to buy on the Black Market: three attacking and six defensive. The sheet containing all Asset cards is shown in Figure 9, from which each individual card is cut out to form a small deck. Cards are fed into the Black Market periodically, making them available for players to purchase.

[313] Greenberg (2012); *The Economist* (2013)

Although the Assets have in-game consequences that affect gameplay, they also have pedagogical purposes, a selection of which are discussed below.

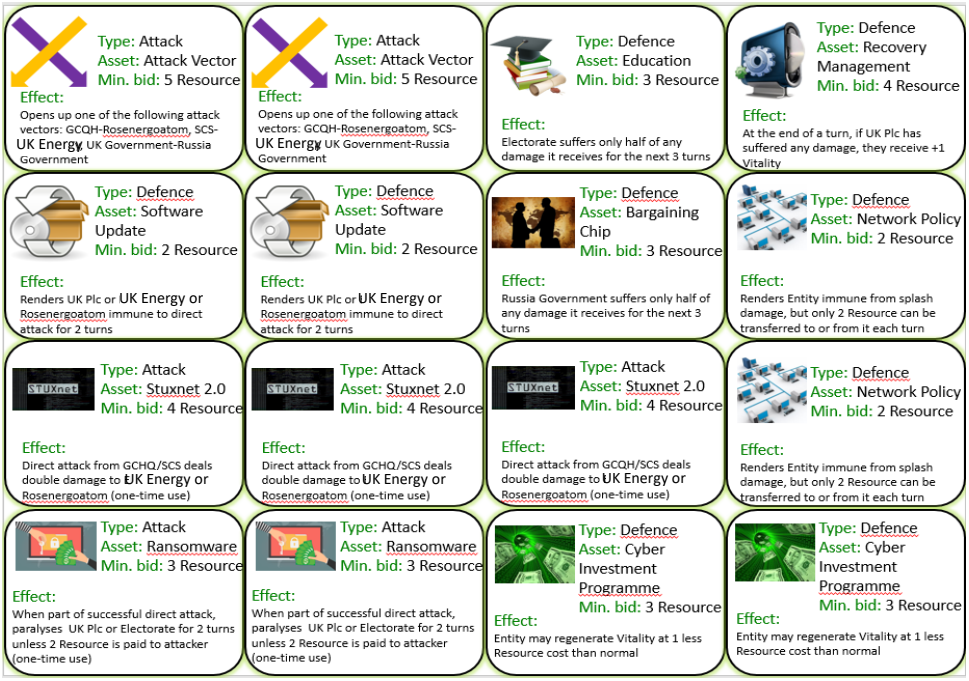

Figure 9: Black Market Asset cards

Software Update

Perhaps the single, most basic practice contributing to good cyber security is software updates. Updates remove vulnerabilities in programs, closing routes in for an attacker. For most consumer programs, for example Microsoft Windows, these updates are frequent and free (insofar as they are included in the original purchase price) and happen automatically in the background unless the user opts to install them manually. In more specialised and bespoke systems, such as control programs for industrial sites – including CNI – the availability and cost of updates can vary, and updates can be difficult to deploy to inaccessible systems.[314] In these cases, onus falls on the end user to ensure provisions are made for the future upkeep of programs before a purchase is made.

The Software Update Asset simulates the temporary protection provided by updates by granting UK Plc, UK Energy, or Rosenergoatom immunity from direct attacks for a short duration. The intended learning moment is for players to

[314] Kaspersky Lab (2017)

engage with the idea that updates deny vulnerabilities to would-be adversaries, but the limited time frame also reminds players that updating is a continuous process. The asking price of the Asset is very cheap, partly because many of the most critical updates are inexpensive (businesses also use Windows), and partly to encourage players to purchase the Asset. The principle here is to positively reinforce the importance of updates by lowering the barrier to players engaging with the concept.

Network Policy

The Network Policy Asset aims to expose players to some of the dynamics of defence through segregation. Segregating networks and systems from each other is a potentially effective way of limiting both attack surface and contagion from an incident. A computer which is not connected to the Internet, for example, cannot receive spear phishing emails. In more sensitive settings – such as CNI – a system may be completely 'air-gapped' from its surroundings, meaning it has no physical or wireless connections to other systems.[315] Extreme versions of this might put additional barriers in place to prevent intrusion, such as Faraday Cages which block out all electromagnetic activity. In these cases, an attacker would require physical access to the system, which brings an attack beyond the realm of a pure cyberspace operation and out of reach of all but the most advanced actors (usually state intelligence agencies).

The downside to isolating computers and systems is that they do not gain the benefits brought by interconnectivity. A computer without emails would not be much use in an office setting where communication with colleagues and customers is paramount. Similarly, an air-gapped system cannot be controlled or maintained remotely, making it more expensive to run because of the need to have operators or engineers on-site. The benefits of connectivity are usually weighed as more valuable than the security risks, so organisations opt for networking over segregation.

The Network Policy Asset represents the trade-offs associated with segregation by making the Entity it is deployed on immune from residual damage (damage

[315] Libicki (2012), p. 326

received as a result of a linked Entity receiving damage), but also limits the amount of Resource which can be transferred to or from it. In this representation, malware is limited from spreading from neighbouring systems, but the utility and operability of the system is restricted. Although the defensive benefits of the Asset are simple to recognise, players are faced with more difficult decisions about where to place the Asset. By encouraging player discussions about gameplay benefits and drawbacks, learning moments about the defensive dynamics of network segregation can be created.

Stuxnet 2.0

One of the most emblematic offensive operations in the short history of cyberspace is Stuxnet. Stuxnet was a computer virus allegedly developed by US and Israel to disrupt operations at the Natanz nuclear facility in Iran.[316] At the time of its discovery in 2010, Stuxnet was one of the most advanced pieces of malware seen in public. It infected an air-gapped system, used three zero-day vulnerabilities to compromise defences, and employed two stolen software certificates to appear authentic. Stuxnet took control of the Supervisory Control and Data Acquisition (SCADA) system for the centrifuges which enriched uranium at Natanz, causing them to spin outside their operating bounds and thereby incapacitating them, all while evading detection and spoofing safety features to make it appear as the system was operating normally.[317] Although the actual effect of Stuxnet on the Iranian nuclear programme can be questioned, this author has argued that the operation captured the imagination of military planners, security specialists and academics, to whom it had been demonstrated that purely digital weapons could have physical effects.[318]

SCADA systems are used in industrial settings such as manufacturing or energy production plants. In the game, both UK Energy and Rosenergoatom are in the energy production business and SCADA systems will be a part of nuclear plants such as those at Hinkley Point in the UK. The Stuxnet 2.0 Asset follows its real-life namesake by targeting such systems: it causes an attack by SCS on UK Energy or GCHQ on Rosenergoatom to deal double damage. Although powerful, players

[316] Thomson (2013)
[317] Falliere et al (2011)
[318] See Haggman (2014)

need to make carefully-deliberated decisions about its use. Firstly, the Asset carries a large price tag, reflecting the development costs of high-end cyber weaponry; the original Stuxnet has been estimated at up to $100 million. [319] Secondly, the Asset is single-use only, reflecting that once zero-days are 'burned' (made known), attack routes will be closed by system updates. Players therefore need to discuss whether it is worth investing in, and using, Stuxnet 2.0 or whether their Objectives can be achieved in other ways. These discussions give players an insight into dilemmas facing real-world policymakers.

Ransomware

Ransomware is malware that infects a target computer and encrypts files so that they cannot be accessed by a user. The malware then informs the user that they can purchase the key to decrypt their files, and provides instructions on how to do this, usually by using the cryptocurrency Bitcoin. The payments sought are normally relatively small, between $300 and $700 for consumers.[320] The Ransomware Asset simulates a ransomware attack by forcing the attacked Entity to either pay a small amount of Resource to the attacker or be incapacitated for a short time. The low ransom cost mirrors the small charges levied by cyber criminals, while the time duration of the incapacitation reflects that an affected person or organisation who does not pay should eventually restore use from a backup system. The gameplay mechanisms associated with the Ransomware Asset force players to make decisions about whether to pay ransoms or suffer the inconvenience associated with incapacitation, mirroring decisions facing real-world victims of ransomware attacks.

Ransomware had been a scourge of cyber security for many years before the WannaCry attack in May 2017, but this incident really brought the issue to the public's attention. In the UK, this was not least because of the debilitating effects of WannaCry on the National Health Service, where multiple hospitals were severely disrupted, leading to a public debate about who was at fault.[321] Was it hospitals for using outdated systems (Windows XP)? Users for clicking on infected links? Microsoft for not providing updates? IT administrators for not applying

[319] Gilbert (2014)
[320] Everett (2016), p. 10
[321] SC Staff (2017); Martin et al (2017); Sood et al (2017)

available updates? Or Government for withdrawing funding? Wherever ultimate responsibility lay, WannaCry encapsulated many important cyber security concepts. The Ransomware Asset can serve as a catalyst for players to explore these concepts and how they tie in to other parts of the game.

4.4.3 Attack Vectors

Cyberspace is a domain of constant hostile activity, stemming from a need for prospective attackers to probe the networks and systems of their targets to find vulnerabilities that can be exploited at the time of attack. Ben Buchanan has described how this can be a dangerous and escalatory process, a modern version of the Thucydides Trap.[322] In this situation, no actor in cyberspace (whether nation-states, organisations, or individuals) can exist in isolation from adversaries. It was important for players to understand some of the dynamics around this constant hostility because it is such a fundamental aspect of cyber security. The game introduces this to players through Attack Vectors on the game board: two permanent and three available to purchase on the Black Market.

Permanent Attack Vectors

The permanent Attack Vectors are the orange arrows in Figure 7, leading from Energetic Bear to UK Plc and Online Trolls to Electorate. These represent, respectively, industrial espionage and disinformation campaigns, as described in Section 4.2.1 and are one-way Vectors; UK Plc and Electorate have no attacking remit in the game. These UK Entities' inability to Attack represents UK policy that the Government has a monopoly on offensive cyber operations. Players are able to debate the efficacy of this policy and whether organisations should be empowered to 'hack back' against hostile actors to recover stolen material, or even pre-emptively attack to deter or disrupt potential Attacks (as mentioned in Section 4.4.1).

[322] Buchanan (2017)

The permanency of the Vectors is intended to illustrate to players that Attacks along these lines are a constant threat, even if the Attacks themselves are not constant. Because the Vector is always there, players are reminded that the dynamics between cyber attack and defence is an ongoing competition where defenders are usually on the back foot (as discussed in Section 4.4.1). Players therefore learn that defences against such attacks need to be constantly maintained as any lapse in defence is liable to be exploited by attackers.

Purchasable Attack Vectors

The Attack Vectors available to purchase on the Black Market were a development which came about from experiences with earlier versions of the game. As can be seen in Figure 6, the first version of the game included three additional permanent Attack Vectors: SCS targeting UK Energy, GCHQ targeting Rosenergoatom, and UK Government targeting Russia Government. The first two of these were intended to represent sophisticated attacks on critical infrastructure, as exemplified by Stuxnet or the 2015 BlackEnergy attack on the Ukrainian electricity grid.[323] However, feedback about the game design from an academic in the military establishment indicated that this representation would likely skew the game's potential learning moments as too overtly offensive. According to the academic, blatant attacks on CNI would only occur in exceptional circumstances (such as war), yet the game model made them appear part of the norm, on par with industrial espionage and disinformation. Players might therefore get the wrong impression about the prevalence and severity of different types of attacks. In reaction to this feedback, the game design was altered by removing these two Attack Vectors (SCS on UK Energy and GCHQ on Rosenergoatom) from the game board, instead making them options available to players who purchase the Attack Vector Black Market Asset, as seen in Figure 9. In this way, the game places less emphasis on CNI attacks and instead focuses on the operations which are more prevalent in day-to-day cyber security (espionage and disinformation). To create learning moments, players can think about why the CNI

[323] ICS-CERT (2016)

Attack Vectors are not permanent features on the game board and discuss how the game model could be changed in terms of Attack Vectors.

It is also noteworthy that moving these Attack Vectors to a Black Market Asset created a better representation of capability development. It has already been mentioned that attacks on CNI are often highly sophisticated, and large research and planning efforts underpin these operations. With Stuxnet, for example, it has been surmised that certificates embedded in the software were physically stolen from two companies in Taiwan[324], and that a replica of the Natanz facility had been built where the malware could be tested.[325] By making players invest Resource into the Asset to create an Attack Vector targeting CNI, some of the supporting efforts of such operations are better represented than having the Vector available by default, thereby affording players a more realistic experience of cyber capability development.

The final Attack Vector, UK Government targeting Russia Government, had initially been designed as a non-cyber Vector. It represented both the UK's ability to wield greater democratic clout thanks to its standing in the international community, and its greater economic capacity and ability to levy sanctions on Russia in response to aggressions, for example in the aftermath of Russia's annexation of Crimea.[326] However, a surreptitious meeting with a member of the UK intelligence community yielded design feedback which suggested this Attack Vector may create inaccurate learning moments. The interlocutor highlighted that in international processes regarding cyber security, such as the UN Government Group of Experts, Russia actually wields a high degree of power because it has the support of many smaller nations. [327] Indeed, disagreement over the applicability of UN Article 51 (right to self-defence) in cyberspace, suggests that Cold War allegiances are still influential on the diplomatic arena when it comes to cyber issues.[328] As a result of this feedback, the Attack Vector was removed from the game board and instead made available as part of the Attack Vector Black Market

[324] Matrosov et al (2010), p. 13
[325] Sanger (2012a)
[326] European Commission (2015)
[327] Author conversation with [anonymous] at ACE-CSR conference, Solihull, UK, 11 July 2016
[328] Bowcott (2017)

Asset. To further reflect the dynamics of international cyber security policymaking processes, the Bargaining Chip Black Market Asset was also added (see Figure 9), which allows Russia to leverage its support base in the international community. With these changes, the final version of the game more accurately represents the real world, enabling players to engage with concepts surrounding power balances in international cyber security and how these affect dynamics around Attack Vectors.

4.4.4 Dynamics of attack risk and reward

As has been alluded to in previous sections, many actions in cyberspace entail trade-offs between benefits and drawbacks. With cyber attacks, as with other military operations covered in wargames, trade-offs can manifest themselves as the balance between risk and reward. The risk can be characterised as the amount of resource committed to an attack combined with the chance of discovery and attribution, while reward equates to the damage or other effects caused. A low-level Distributed Denial of Service (DDoS) attack, for example, can be launched with very little risk because of the anonymity offered by botnets, but the reward is not very high because the attack can be easily mitigated. On the other hand, state-sponsored operations against CNI, such as Stuxnet, have a high potential reward in disrupting infrastructure, but also carry a higher risk of political fallout if the attack is discovered and attributed to the attacker.

In order to convey some of these dynamics to players, the game required an Attack mechanism with a scale of risk and reward. Following the standard used by most wargames, a mechanism was designed which allowed players to spend Resource to Attack, then roll a die to determine the outcome of the Attack. The use of dice depicts the uncertainties of war, where outcomes are never deterministic.[329] In the first version of the game, this was implemented as a simple formula:

$$Damage = (Resource\ Spent) - (Die\ Roll)$$

[329] Kainikara (2003), p. 7

A combat results table, another mainstay of wargaming, with all the possible outcomes from this calculation is shown in Figure 10. There were three problems with this initial approach. Firstly, the mechanism used a four-sided die, but feedback from an early game session with a professional military wargamer suggested that most people's unfamiliarity with non-standard dice would likely cause some confusion. Secondly, the formula meant that players had to roll a low number for a successful Attack. Feedback from the same professional wargamer suggested this was highly counterintuitive. In most games that employ dice, whether wargames or casual board games, high numbers equate to good results, so players naturally expect this standard. Forcing players to reverse their thinking process introduces a small but significant moment of friction to their engagement with the game. Players might roll a high number and expect a good result, only to realise the opposite was the case. Any positive emotions conjured would therefore be taken away by a game technicality, potentially causing player disillusion with the game.

		Die Roll			
		1	2	3	4
Resource spent	1	0	-1	-2	-3
	2	1	0	-1	-2
	3	2	1	0	-1
	4	3	2	1	0

Figure 10: Version 1.0 combat results table

		Die Roll					
		1	2	3	4	5	6
Resource spent	1	0	1	1	1	1	2
	2	0	1	1	1	2	2
	3	-1	0	1	2	2	3
	4	-1	0	1	2	3	4
	5	-2	-1	2	3	3	4
	6	-2	-1	0	3	5	6

Figure 11: Final version combat results table

The third, and most critical, problem with the first version of the Attack mechanism was that it presented risk and reward on a linear scale where there was an equal chance of success and failure. Feedback and observations from early game sessions suggested this balance achieved counterproductive pedagogical outcomes, because it did not reflect a realistic risk calculation – there was little point launching an Attack with anything but the maximum number of Resource. This model did not reflect the real world, where the vast majority attacks are cheap but unsophisticated and unlikely to cause a great deal of damage. To remedy this situation, the Attack formula was abandoned in favour of a new combat results table, as seen in Figure 11, which reflects a dynamic where low-risk Attacks can be launched cheaply, but without any great potency to cause damage. Higher-damage Attacks require a greater Resource investment and come with a higher risk of failure. With this model, players have more difficult decisions to make about how they want to mount offensive operations and what their risk appetite is. In this way, the final version of the game simulates the trade-offs that are present in the real world to a reasonable degree of accuracy, exposing players to these concepts in a more realistic way and enabling richer discussion around the issues.

4.4.5 Dynamics of attribution

A critical dynamic of cyber attacks is the issue of attribution. In addition to speed of deployment (as discussed previously), cyber capabilities have also been lauded for their stealth provided by anonymity.[330] Unlike physical weapons which leave traces indicating their origin, such as missile trajectories, cyber weapons' traces can be obfuscated or deceptively altered, making it seem as if they were deployed from somewhere other than their real point of origin. The attribution process for cyber attacks therefore requires more than technical indicators; Thomas Rid and Ben Buchanan, for example, propose a 'Q model' for attribution that involves 'minimising uncertainty' on tactical, operational, and strategic levels.[331] The key

[330] For example Applegate (2012), p. 194; Farwell and Rohozinski (2011), p. 27; Gross (2011); Jacobsen (2014), p. 14; Liles et al (2012), p. 171; Mumford (2013), p. 43; Sanger (2012b), p. 208; *The Economist* (2012); Betz (2011), p. 22; Gregory (2011), p. 245
[331] Rid and Buchanan (2015)

words here are 'minimising uncertainty', which highlight how attribution often does not deal in absolutes, but in degrees of certainty. After the Sony Pictures hack mentioned in Section 4.4.1, the US State Department levied new sanctions on North Korea, who had been deemed the perpetrators of the attack, yet this was based on what the Federal Bureau of Investigation called 'not just high confidence, but very high confidence.'[332] Similarly, the Mandiant report regarding Chinese cyber espionage referenced in Section 4.2.1 reached only a 'most probable conclusion.'[333] The point here is that attribution of cyber attacks is not a definitive science and it is important for players to be able to engage with some of the dynamics around this process.

The game design conveys attribution in two ways: one deliberately misconstrued and one more realistic. The misconstrued way is the two permanent Attack Vectors on the game board: Energetic Bear targeting UK Plc and Online Trolls targeting Electorate (also see Section 4.4.3). These Vectors are not misconstrued in their existence – industrial espionage and disinformation campaigns targeting the UK do happen, as discussed in Section 4.2.1 – but misconstrued in their clear attribution. Referring to Figure 7, the orange arrows on the game board leave players in no doubt where the Attacks on UK Plc and Electorate are coming from; in other words, they have perfect attribution, which is not representative of real-world attacks. In this way, the mismatch between the game model and reality can provide players with discussion opportunities leading to a learning moments about attribution.

The more realistic way the game conveys attribution is in failed Attacks. Referring to Figure 11, the negative numbers in red result when players commit a medium or large amount of Resource to an Attack, representing a greater degree of sophistication, but roll a low number on the die, representing the Attack failing. A failed Attack results in damage to the attacker, representing blowback effects of the Attack, and additional effects representing the Attack being attributed (a Resource penalty, and/or the attacking Entity being incapacitated for a short duration, and/or a Black Market Asset being given to the attacked team). In the

[332] Park and Ford (2015)
[333] Mandiant (2013), p. 59

game, attribution is only possible for attacks at more sophisticated levels because these attacks leave more traces, both technical and otherwise, to limit the uncertainty associated with attribution. As part of their risk-reward calculations when deciding to Attack, players therefore also have to take into account whether they are willing to chance having the Attack attributed to them, with the attendant repercussions. In this way, players can engage with some of the dynamics around attribution, generating discussion points and potential learning moments.

4.5 Geopolitical realities of cyber security

Events happen in the world which are not controllable, perhaps not even predictable, but which nevertheless have some effect and need to be reacted to. Cyber security is not immune from such events, nor are affectual events limited to cyberspace; geopolitical occurrences in the physical world can have significant consequences in the digital world. It was important for players to be able to engage with these unpredictable events in order to understand how cyber security can be impacted by events which may not seem to have a direct connection, but nevertheless create situations in which cyber security policy or technology is affected.

To represent some of what can be termed geopolitical realities, a deck of Event Cards was designed for the game, which are drawn randomly to simulate the unpredictability of events. The deck consists of 16 Cards, half of which create an Event, shown in Figure 12, and half of which allow play to proceed as normal, shown in Figure 13. Players have to react to the Cards by adapting their gameplay strategies, similar to how a policymaker in the real world might have to react to an unfolding situation. In gameplay terms, the Event Cards also add a layer of entropy, in addition to the use of dice, making the game less deterministic. The sections below discuss some of the Event Cards and the learning moments associated with them.

Figure 12: Event cards

Figure 13: Non-event card

4.5.1 Clumsy Civil Servant Event Card

The frailty of the human link in the security chain is often highlighted in information security literature and no subset of society seems to embody this more than civil servants.[334] With alarming frequency stories emerge about suitcases, laptops, or storage devices with millions of citizen's sensitive data being

[334] For example, see Mitnick and Simon (2002), p. 3; Arce (2003), p. 74; Lineberry (2007), p. 44; Pfleeger et al (2014), p. 491

left on planes, trains, or in public places.[335] Perhaps chastising civil servants is unfair as this undoubtedly happens to employees in every variety of organisation, but civil servants' errors are especially grave because of the data they handle and their public positions, which no doubt brings additional media attention to incidents.

The Clumsy Civil Servant Event Card simulates such an incident, aiming to educate players that these events result in negative repercussions for both the Electorate and the UK Government. For the Electorate, the exposed personal data can be used by criminals to commit identity theft and fraud, undermining the integrity of people's personas. For the Government, a costly clean-up operation must inevitably follow, including re-securing the data and compensating any persons who are the victims of crime as a direct consequence of the lost laptop. Although not catastrophic, this card puts the UK team at a disadvantage, forcing them to adapt any plans they had made in light of new gameplay conditions. Players thereby receive the benefits of an *ersatz* experience (as discussed in Section 2.2.5) of dealing with the consequences of human error in information security.

4.5.2 Banking Error Event Card

The financial sector is a part of CNI and in the UK its contribution to the economy is outsized given the prominence of the City of London as a global marketplace. Any major disruptions to the workings of the sector are likely to cause significant, if not catastrophic, effects on the economy (as discussed in Section 4.2.1). Although no malicious cause has been attributed to the Bank of England 2014 incident, it can be envisaged that a directed and determined attack on multiple systems simultaneously might achieve effects orders of magnitude higher.

The Banking Error Event Card creates a similar incident by simulating a Bank of England transfer protocol error and restricting the UK side from transferring Resource between Entities. This does not bring the country to a complete standstill – the UK can still use Resource where it currently is – but it does

[335] For a list of examples, see BBC News (2009)

severely limit the UK's options, as well as potentially delaying or derailing any planned moves. The Card can prompt players to think about the criticality of some of the systems which underpin a modern economy, perhaps leading to discussions about how reliance on centralised mechanisms can be reduced. Although not mentioned explicitly in the game, distributed ledger technologies may be a potential solution in this space – and has been actively explored by multiple financial institutions[336] – so the Card has potential to inspire discussion about disruptive innovation in cyber security.

4.5.3 People's Revolt Event Card

Under the leadership of Vladimir Putin, political opposition and public dissent in Russia has been repressed. In the 2018 elections, for example, Alexei Navalny, the only viable opposition candidate, was barred from running.[337] Public protests are staged from time to time but are often met by police violence and arrests. Assassinations also appear to be a viable instrument of power, with multiple opposition party members, political activists and critical journalists meeting untimely and mysterious deaths.[338] In this environment it is difficult for any narrative which questions the official line to gain foothold, and serious challenges to Putin's grasp on power do not appear forthcoming.

The People's Revolt Event Card simulates a situation in which this repression reaches boiling point, with people taking to the streets in protest. In keeping with the thematic cyber content of the game, the trigger for the protests is Internet censorship and a person bearing a Guy Fawkes mask – associated with hacktivist group Anonymous – is on the Card. The in-game effect of the Card is that Russia does not gain any new Resource that turn, representing the people's unwillingness to pay taxes under the current regime. Although there are no long-term repercussions in the game, representing the historical fleetingness of similar protests, the Card invites discussion about regulation of free expression and the role of the Internet in galvanising groups of people. Of additional importance, this

[336] For a summary, see World Bank Group (2017)
[337] Roth (2018)
[338] Jackson (2015)

is the only place in the game Anonymous explicitly appear, meaning the Card can serve as a catalyst for discussing the role of non-state actors in cyberspace, and where such actors may play a role in other parts of the game.

4.5.4 Quantum Breakthrough Event Card

The other seven Event Cards paint a rather gloomy picture of cyberspace where every incident only has negative consequences. Breaking with this trend, the Quantum Breakthrough Card represents a technological advance which benefits all sectors of society and industry. The Card states that Google rolls out quantum computing to all its devices and services, granting all Entities a one-off Resource and Vitality payment, representing some of the potential benefits quantum computing can bring.

Quantum computing takes advantage of the superpositionality of atoms to enable unparalleled processing power. Shor's algorithm, for example, can (theoretically) be used to factor large numbers, which would undermine many of the assumptions that enable modern cryptographic technologies.[339] However, foreseeing this diminishing of security, post-quantum cryptography is already developing algorithms that will be resilient to quantum computing, meaning secure communications can still be achieved.[340] Quantum technologies will also enable increases in speed and efficiency of communication, as demonstrated by a Chinese satellite experiment in 2017.[341] Fast, cheap, and secure communication has underpinned globalisation and the movement of goods and money, increasing the quality of life for billions of people, which could be taken to another level in the post-quantum world. The Quantum Breakthrough Event Card prompts players to debate which of these touted benefits will materialise, or whether the Card is in fact unrepresentative in its effects and that quantum computing will irrevocably undermine modern cryptography. Given that Google are explicitly mentioned on the Card, there is also scope for discussing ownership of technologies and the motivations of technological giants. Similar to the Banking Error Card, the

[339] Shor (1997)
[340] For an overview of the field, see Berenstein et al (2009)
[341] Ananthaswamy (2017)

Quantum Breakthrough Card thereby challenges players to think about the direct effects of technological change and extrapolate this to wider societal impacts.

4.6 Visibility in cyberspace

Sections 4.4 and 4.5 outlined game components and mechanics which convey Clausewitzian friction – unforeseen difficulties. However, little has been said about the fog of war – imperfect information – which is the other part of Clausewitz's famous 'fog and friction' concepts. [342] The fog of war can be taken literally in terms of visibility on the battlefield. Historically, the cacophony and tumult of battle could shroud commanders' views of the battlefield to such extremes that armies mistakenly charged upon themselves, or complete obliviousness that a battle had taken place at all.[343] In modern war, literal line-of-sight visibility is perhaps less important than the battlespace awareness created by geospatial plotting devices (such as radar) and intelligence about unit dispositions. Nonetheless, the fog of war can be present here too, with incomplete or inaccurate information shrouding visibility.

In the cyber domain, the lack of visibility is amplified further than the smoke-filled Napoleonic battlefields on which Clausewitz was schooled. Not only can we not physically perceive the electrical impulses on which computing and telecommunications are based, the structure of the Internet also prohibits a comprehensive overview of the operational landscape, despite attempts made in this direction.[344] It is important for players to be able to engage with this concept, as decision-makers and policymakers rarely have a complete visibility of a problem or situation before they have to address it.

There are established techniques within wargaming for simulating the fog of war. In his wargaming manual, for example, Scruby recommends that a curtain is set

[342] Although it should be recognised that Clausewitz himself never used this phrasing, Kiesling (2001), p. 85
[343] Englund (1991), pp. 14-15
[344] Kiravuo (2015)

up in the middle of the table so that 'troops may be set up in secret,'[345] mimicking the uncertainty a commander experiences prior to battle, while John Setear suggests six design tools: referees real and simulated, counters that conceal, counters potentially in play, the rulebook, modifying the map, and the laws of war.[346] In early prototype versions of the game some of these were experimented with, for example using counters to cover portions of the game board. Ultimately, however, the game board has been left entirely visible to all players and hidden information is instead conveyed through the player dossiers (which each team keeps secret from the other team) and pre-allocated Black Market Assets (which are dealt face-down before the start of the game).

The decision to hide information about players, especially their capabilities, rather than the game board stemmed from the difficulty of determining capabilities in cyberspace. Although cyber attacks of varying scales occur with regular frequency, they usually reveal more about targets' weaknesses than attackers' capabilities. From the effects of a cyber attack we can infer a minimum level of adversarial capability in that they are able to exploit certain vulnerabilities, but we are not given information about any further capabilities which may be able to achieve effects above and beyond what has been achieved. These difficulties are exacerbated by the nature of cyberspace as non-physical. The weapons deployed in cyberspace have no engine, chassis, hull, or barrel, nor do they fire bullets or shells. Gaining meaningful intelligence about adversaries' cyber capabilities therefore becomes enormously difficult.

In this sense, the design decision to limit visibility of capabilities rather than the operating landscape follows the standard set by many games about carrier task forces, where fog of war is used to represent intelligence capabilities rather than physical line of sight. [347] It also follows Clausewitz's dictum that 'In the whole range of human activities, war most closely resembles a game of cards.'[348] By giving players cards (Black Market Assets) which are hidden from opposing players they have at their disposal unknown capabilities which represent a form of

[345] Scruby, p. 13
[346] Setear (1989) pp. 6-18
[347] Sabin (2012), p. 109
[348] Clausewitz (1997a), p. 27

information superiority – the players know something the others do not know. There is no game mechanic which allows the opposing players to find out what these capabilities are until they are played in the game, closely simulating the difficulty of determining capabilities in cyberspace.

In having to deal with the fog of war, players gain an experience of making decisions based on incomplete information, as a policymaker would in the real world. There are also discussion opportunities around how the visibility mechanics have been implemented in the game, for example the whole game board being visible or players' inability to gather intelligence. Such discussions allow players to explore the issue of visibility in cyberspace and learn lessons about the difficulties associated with constructing a complete and accurate picture of the operating environment.

Chapter 4 Conclusion

Wargaming literature is rife with analysis and advice regarding the game design process. This chapter has taken much of this advice under consideration, for example Scruby's assertion that simple time flows are best for inexperienced players (Section 4.4.1), or Frank's warning that victory points mechanics can distract players from the purpose of the game (Section 4.3). Perhaps most crucially, a core tenet of the design philosophy was Sabin's dictum that a simple wargame that is played is more instructive than a detailed game which is not played (Section 4.1). In almost all design matters, simplicity and playability was favoured over complexity and accuracy. This was to serve the game's purpose as an educational tool, rather than an analytic or simulation tool.

Where this chapter has made original contributions to the field is in applying wargame design concepts to the topic of cyber security. Chapter 3 demonstrated some of the deficiencies in current cyber wargaming efforts and the game design outlined herein is an attempt to plug a gap in the extant corpus. There are three contributions of crucial significance. First, this game is explicitly based on the UK National Cyber Security Strategy; the design of game board, the Entities present in

the game, and players' Objectives are to a large extent derived from the designer's interpretation of the Strategy. The games analysed in Chapter 3 almost exclusively deal with tactical issues, either of a technical nature or confined to one organisation, whereas the original game designed for this thesis concerns a much wider gamut of strategic topics. Although ambitious in scope, including more topics and concepts increases the learning opportunities contained within the game, serving the primary aim of using the game for educational purposes.

Second, the game contains a more nuanced representation of cyber attack and defence dynamics. Several of the better games analysed in Chapter 3 pitted players against the game system rather than other players, thereby foregoing many of the benefits of wargaming (see Section 3.2.2). Even in the matrix-style games, where players could argue with each other, the results of conflict were decided almost arbitrarily by the umpire. This game allows players to face off against human opponents, but with solid game mechanics and independent variables determining the outcome of attacks. These mechanics and variables are based on the designer's interpretation of real-world cyber security dynamics, which have been extensively documented throughout the chapter. Importantly of course, players would be able to question design decisions based on their own knowledge or expertise, thereby stimulating pedagogic discussion.

Lastly, this game has showcased how successful game mechanics can be innovatively borrowed from existing games. The effectiveness of event cards in simulating unpredictability, particularly as implemented in *Privacy*, led to a similar system being designed for this game. Similarly, the marketplace contained in *Decisions & Disruptions* was deemed exceptionally effective in both forcing players to make decisions about how to use limited resources and articulate their reasoning behind these decisions. The Black Market implemented in this game is intended to achieve the same effects, but broadening the lessons from tactical to strategic, and including a competitive arms race element. Examples like these illustrate the value of understanding an existing wargaming landscape for a given topic and being able to transpose useful concepts rather than reinvent the proverbial wheel.

By analysing design concepts with close regard to a wide variety of cyber security issues, this chapter has demonstrated that a wargame can encapsulate both technical and geopolitical aspects of cyber security whilst maintaining playability, with the ultimate aim of educating players. The efficacy of the game in achieving this outcome is analysed in Chapter 6.

Chapter 5: Methodology for studying games and players

This chapter outlines the methodological approaches of the thesis. In practical terms it could be said that the research takes the form of "create wargame, deploy wargame, observe results." However, underpinning each stage of this process are theoretical foundations that guide and shape how the research is conducted. In the sense that the thesis represents experimental work, a core focus of the methodology is grounded theory, which affords a certain flexibility to research that emphasises emergence of findings through creative analysis and interpretation of data.

Grounded theory does not have a strong precedent for use within academic gaming research. John Salisbury and Tom Cole point to a 'lack of rigorous and transparent use of [grounded theory] in Game Studies.'[349] Until recently, in the subset of wargaming research, this lack has been even more apparent. Anders Frank, for example, used what he calls an 'interactionist perspective' as the theoretical framework for his 2014 doctoral thesis, giving him a fairly narrow lens through which to analyse the 'gamer mode' phenomenon his work is concerned with.[350] Colin Newcombe's experience using wargames for teaching history hinted at the benefits of grounded theory, but did not elaborate further; 'the more elastic one's approach, the more is to be gained in terms of class discussion or individual research,' he says.[351] Jonathan Barbara, meanwhile, touched on aspects of ethnographic practice (also discussed in this chapter) but shied away from grounded theory with his use of pre-prepared questionnaires to evaluate player experiences.[352] As of the time of writing, the only considered and critical use of grounded theory in academic research is Johan Elg's 2017 doctoral thesis concerning wargaming in military education. Similar to the approach of this thesis,

[349] Salisbury and Cole (2016), p. 2
[350] Frank (2014), p. 49
[351] Newcombe (1970), p. 302
[352] Barbara (2015), pp. 633-634

Elg only partially implements grounded theory; he embraces the notion that it enables theory development yet emphasises that this is of interest only so long as it is relevant to the practice of wargaming.[353] The use of grounded theory in this thesis therefore joins Elg in representing a novel approach to wargaming research.

The chapter begins by outlining the basics of grounded theory, before more closely analysing how it is applied in this thesis, specifically the use of grounded theory in an inspirational mode, rather than a strict guide for research. Following this, Section 5.2 proceeds to look at the applicability of ethnographic practice to the thesis, interlacing core tenets of ethnography with methodology themes from wargaming literature. A short biography of the researcher is provided as a way of addressing strategic positionality, and the difficulties of security and classification as applied to this research are enumerated. Section 5.3 analyses issues around facilitation and adjudication, which are key to wargaming practice, resulting in the first part of an exposé of tactical positionality covering the tensions between the roles of game designer and game facilitator/adjudicator. Section 5.4 returns to questions around research design, covering different methods for capturing data and evaluating results. The section justifies the primary data-collection methods used in the thesis – fieldnotes and photographs – while outlining why another candidate – video recording – was not employed. This discussion leads onto the second part of tactical positionality, looking at the tension between the roles of facilitator/adjudicator and researcher. The chapter concludes with commentary on the contributions of the thesis to wargaming research methodology.

A crucial consideration to keep in mind throughout this chapter is that experiences of conducting the research are elaborated in detail in Chapter 7. This includes comparisons of how the experiences reinforce or challenge assumptions and predictions stemming from the methods. As such, the current chapter presents the methodology in theory, while evaluation in practice can be found in the later chapter.

[353] Elg (2017), p. 17

5.1 Grounded theory and its links to wargaming

Most academic research follows the traditional positivist scientific approach. This approach begins with the formulation of research questions, which in turn guide how the research will be conducted. The evidence gathered is then used to confirm, dispel or reformulate the pre-selected hypothesis. In essence, grounded theory seeks to flip this around, so that data is gathered first, and a hypothesis or theory only emerges once this data is analysed. Although first formulated by Brian Glasner and Anselm Strauss' 1967 work *The Discovery of Grounded Theory: Strategies for Qualitative Research* in the field of sociology, in the past fifty years grounded theory has established itself as a highly regarded qualitative research method, especially in health and education studies but also human geography and politics and international relations.[354]

Given that this thesis is to a large extent concerned with pedagogy, it is therefore important to consider how grounded theory is instructive. In the area of education, Sally Hutchinson has provided a comprehensive overview of how to approach research using grounded theory. She notes constraints on the researcher such as 'bracketing' (or positionality, discussed further in Sections 5.2.1, 5.3.1 and 5.4.2 below) and the reliability and validity of data, and makes recommendations on how to record data.[355] She also points to Glasner's 1978 book *Theoretical Sensitivity* as the best guide on the subject, yet, perhaps ominously, deems it 'tedious, difficult, and carelessly edited,' imploring that 'it is best to read the book as you are doing your research; to read Glaser's work in isolation from empirical data is un-productive.'[356] If we take this statement to be a reflection of the academic consensus, grounded theory appears ironically self-fulfilling. In the same way that grounded theory itself involves the collection of data before a postulating a theory, in order to employ grounded theory in the first place, the research that feeds into it must already be done.

[354] Thomas and James (2006), p. 768
[355] Hutchinson (1986), pp. 57-60
[356] Ibid., p. 57

Despite an apparent close fit to the research being conducted (create-deploy-observe), this thesis does not simply embrace grounded theory uncritically, but uses it strategically to inform research design and methods. As a reminder, the central objectives research presented here are:

- *Create a wargame for cyber security education.*
- *Analyse the capacity for the game to create learning moments and enable players to share knowledge and ask the right questions.*
- *Reflect on the researcher's experience as a wargaming practitioner.*

This is accompanied by a selection of sub-questions, including: What are wargames useful/not useful for? What difficulties emerge when designing a wargame for cyber security? How might a wargame that deals with cyber security look? Are wargames good learning tools for cyber security? With the final question as a notable exception, the common characteristic of these questions is their open-endedness. It is not yet known what the potential answers to the questions are and as a result it is not known what type of evidence or data should be gathered. Indeed, the questions are intended as loose guidelines rather than rigid interrogatives and should be flexible enough to be amended or reconsidered in light of whatever data emerges as the thesis progresses. In this sense, the present research is comparable to that of Carlo Fabricatore et al, whose study of game playability (albeit computer games) started with the open-ended question 'what do players want in video games?' and went on to apply grounded theory to derive conclusions.[357] Applying grounded theory as an informative, rather than prescriptive, method in games research also has precedent in Nathan Hook's 2012 social psychology study of live action role-players.[358]

Roy Suddaby argues that grounded theory is too often taken to mean 'anything goes' when it comes to data collection and analysis.[359] The research for this thesis is infused with an awareness of some of the uses and limitations of grounded theory. For example, Kathleen Wells' criticisms about the difficulties of

[357] Fabricatore, Nussbaum and Rosas (2002)
[358] Cited in Hook (2015), p. 317
[359] Suddaby (2006), p. 640

implementing a 'constant comparative method' and evaluating grounded theory for practical potential are well-noted.[360] This method calls for new data to be analysed with regards to previous data as and when it is collected. As the scope of research grows and the amount of data increases, this can become an onerous, potentially unmanageable, task. Taking this into account, Hook lauds Emily Brown and Paul Cairns' 2004 study of game immersion, which drew grounded theory-based conclusions based on just seven data interviews.[361] However, the point here is that this thesis must not limit the amount of data collected simply to ensure grounded theory remains a viable method, and those aspects of grounded theory should not shackle the research. The research may outgrow the applicability of constant comparison, but grounded theory can still remain informative in interpreting data at later stages.

As a final insight, noteworthy of early reviews of grounded theory is the emphasis on the creativity required by the researcher. Both John Scott[362] and Helmut Wagner[363] were enthusiastic about Glaser and Anselm's focus on exploration of data by a human researcher with an understanding of the study area. Perhaps precognisant of this thesis, Wagner states that grounded theory 'emphasizes curiosity, imagination, and openness as prime virtues of sociologists rather than infatuation with statistical techniques: the prime area of sociological action remains the field, not the IBM or computer centre. [sic]'[364] Recalling the analysis provided in Section 2.2, there is clear overlap between grounded theory and some of the advantages of wargaming. Just as wargames can capture human elements of conflict better than operational research techniques, so can grounded theory harness the human aspects of the subject being investigated – in the case of this thesis wargaming and cyber security. Furthermore, the onus on the researcher to creatively apply their cognitive faculties is reminiscent of the creativity required of a wargame designer when creating games. In these aspects, at least, wargaming and grounded theory seem to be close fits.

---

[360] Wells (1995), pp. 35-36
[361] Brown, Emily and Paul Cairns, 'A grounded investigation of game immersion', in *Proceedings CHI '04 Extended Abstracts on Human Factors in Computer Systems* (2004), pp. 1297-1300, cited in Hook (2015), p. 317
[362] Scott (1971), p. 335
[363] Wagner (1968), p. 555
[364] Ibid.

5.2 Ethnographic practice

This thesis is not a classic ethnography. The research does not comprise extended embedding within an organisation or community to make longitudinal observations. Nonetheless, the practical elements of the thesis do draw on many accepted ethnographic practices as the research conducted involved multiple engagements with varied stakeholders in the UK and overseas. Martyn Hammersley and Paul Atkinson's seminal work on ethnography identifies five facets which make up most ethnographic work:

1. People are studied in everyday contexts rather than contrived setups
2. Participant observation forms the main part of the data gathered
3. Data collection is unstructured
4. Focus is on a few, small-scale cases for in-depth research
5. Analysis involves interpretation of human actions, extrapolated to wider contexts.[365]

Of these five, only facets 2 and 3 apply wholly to this thesis; the data collection portions of the research are largely built on the researcher's observations during gaming sessions, and these observations were not designed to spot certain behaviours or actions, nor designed to be recorded in any set format. Facet 1 does not apply at all; gaming sessions represent an artificial setting where players are often encouraged to abandon their everyday roles and mentalities. Facets 4 and 5 apply partially: there were not a great number of gaming sessions enacted as part of the research, but the intent was not to do an in-depth study of each one; while data analysis may involve wider extrapolation, but only if the data permits, which cannot be known before the analysis is actually done.

The implication of this mixed applicability is that the research conducted for this thesis is not directly comparable to classic ethnographic studies. Seminal ethnographic work like that of Edmund Leach[366] or Margaret Mead[367] very closely

[365] Hammersley and Atkinson (2007), p. 3
[366] Leach (1964)
[367] Mead (2001)

follows the five principles outlined above and the present study should not be measured against these, either in terms of how the research was conducted or in terms of impact. At the same time, however, it would be remiss to attempt to completely distance this thesis from ethnography. Given that the research does feature some central tenets of ethnographic study, trying to work in isolation from such well-established theoretical and practical concepts might be seen as reinventing the wheel (at best) or academic negligence (at worst). This section therefore recognises existing theoretical and practical considerations of ethnography, but rather than apply these considerations wholesale, limits analysis to those parts applicable to this thesis.

5.2.1 Strategic positionality

In ethnography, the role of the researcher is pivotal to shaping both the conduct and outcome of the research. The researcher's understanding, skills, and behaviour will affect the level of access granted, what observations are made, how data is recorded and analysed, and how participants react to the research. With regards to initial and overarching influences, we can refer to what Hammersley and Atkinson call 'background knowledge, social characteristics and circumstances' as strategic positionality.[368] Strategic positionality is intended to encompass the broader particularities of the researcher which influence the research. This concerns aspects of the researcher's personal background which may need to be taken into account when determining how the research should be conducted, or when analysing data. These aspects include sociocultural-economic background (class, race, ethnicity, gender, nationality, language), educational attainment, and employment experience. It is important to make these disclosures because other researchers attempting similar work may find different results, and such variation can be caused by the researcher's own characteristics. Strategic positionality is contrasted with tactical positionality (detailed in Sections 5.3.1 and 5.4.2) which refers to specific instances during the research, particularly how the researcher behaves during a game session. Factors that may influence behaviour include the tensions between the roles of the researcher and

[368] Hammersley and Atkinson (2007), p. 25

game designer/adjudicator, and between distanced observation and close engagement.

Researcher's background

As part of identifying strategic positionality issues, it is useful to provide a short overview of the researcher's background. This section highlights some facets of the researcher's personal, academic and professional experiences before commencing the thesis, which are pertinent with regards to positionality.

Gender

The most immediately obvious personal characteristic is that the researcher is male. This is their birth gender and they have never identified in any other way. The advantage of being male when researching a predominantly security- and military-affiliated topics should not be underestimated. These environments have traditionally been male-dominated and, in the case of the military, built on strong cultures of comradeship and bravado associated with testosterone-fuelled acts. Writing of US foreign policy mechanisms after the Second World War, Robert Dean refers to 'socially constructed brotherhoods' from which the likes of John F. Kennedy and Lyndon B. Johnson gained prominence, not least on the back of their much-vaunted respective military service.[369] Although Western societal attitudes have largely steered away from patriarchal dominance in recent decades, military demographics have yet to catch up with an increasingly gender-balanced world. As of April 2017, for example, the UK's Regular Armed Forces were composed of 10.2% females, and the official target was 15% by 2020.[370] As such, a male researcher is likely to more readily be accepted in this environment, because they fit into existing masculinised structures. In her, ethnographic work exploring the world of defence intellectuals, Carol Cohn characterised her experience as 'bizarre'[371] and that her initial naivety meant she was 'not prepared for what [she] found.'[372] Cohn's work is admittedly dated, having been written over 30 years ago, but even the passing of this amount of time will not have completely undone

[369] Dean (2003), p. 13
[370] Dempsey (2017), p. 11-12
[371] Cohn (1987), p. 690
[372] Ibid., p. 692

centuries of masculinised military structures. It could be posited that a male researcher, being less susceptible to a Cohn-like culture shock, would more quickly assimilate into the environment (which took Cohn some time), making the environment less of an obstacle to the research.

As wargaming has military roots, it has inherited a male bias among its practitioners. This is recognised by Pat Harrigan and Matthew Kirschenbaum, who make a point of highlighting the contributions of female authors (11 out of 66 total) to their edited 2016 volume *Zones of Control*.[373] Anecdotally, judging by the attendance at professional wargaming conference Connections UK in 2015, 2016 and 2017, females accounted for less than 15% of participants. In 1992, Dunnigan estimated that females made up as little as 1% of the wargaming community.[374] Unfortunately, the peculiarities of a male-dominated community can sometimes materialise as negative consequences for female participants. Twitter user Katrina Clifford, for example, has shared her experience of a wargaming event where 'people talked only to my husband & looked right past me when on my own [sic].'[375] Being female in this environment can evidently be a handicap, but one that has not had to be contended with as part of this research.

Cyber security, the other primary environment this thesis is concerned with, is equally male-dominated. A 2017 survey by Reed et al found that just 11% of the global cyber security workforce were women, and in Europe (where this thesis is written) it was even lower at 7%.[376] Foley et al reported that one of the inhibitors to female participation in this profession was a perceived 'boys' club', with workplace culture being cited as a major cause for career dissatisfaction.[377] However, these problems are widely recognised by the cyber security community and concrete steps are being taken to address the imbalance. Eleanor Dallaway, for example, has constructed an action plan targeting every level from school children to existing industry professionals.[378] Anecdotally, this author is also aware of a growing number of male cyber security professionals who refuse to

[373] Harrigan and Kirschenbaum (2016), pp. XXII-XXIII
[374] Dunnigan (1992), p. 163
[375] https://twitter.com/kmlclifford/status/926135773321187329
[376] Reed et al (2017), pp. 3-4
[377] Foley et al (2017), p. 12
[378] Dallaway (2016), pp. 8-9

participate in conference panels without female representation. These efforts notwithstanding, at the current impasse, being a male researcher in this environment can clearly be an advantage in terms of removing some of the friction associated with gender disparities.

Nationality and language

Another advantage of the researcher's background they have been able to exploit for research purposes is their dual nationality and bilingualism. The researcher was born in Sweden and spent their early childhood there, before immigrating to Australia where they spent most of their teenage years. Courtesy of this, they hold both Swedish and Australian citizenship, and are proficient to native standard in both Swedish and English. This has proved a boon to the research, as it was possible to leverage both linguistic ties and contact networks (old and new) to arrange gaming sessions in both these countries (see Section 7.1.1), providing important international perspectives and data points. An additional consideration with regards to nationality is the researcher's lack of British citizenship, which could be imagined as a hindrance given the association of the thesis with the UK military establishment. In practice, however, only security and classification, not necessarily tied to nationality, proved an issue in this regard – see Section 7.2 for further discussion.

Education

The researcher's prior education has proved fundamental in shaping the course of the research. The researcher received an undergraduate degree in War Studies with Digital Humanities from King's College London, later followed by a master's in Intelligence and International Security from the same university. Both degrees were based in the university's Department of War Studies, which 'seeks to understand the complex realm of war, conflict and international politics.'[379] In addition to providing the researcher with a solid foundational understanding of various aspects of war and conflict, there were two crucial outcomes which have affected the research for this thesis. The first was an initial exposure to wargaming used for pedagogical purposes. The researcher had previously encountered both board games and miniature figure games in recreational

[379] Department of War Studies website

settings, but a professor at King's – Philip Sabin – used wargames in an undergraduate module as tools for teaching strategic and tactical components of the Second World War. This gave the researcher a basic understanding of how wargames could be used in an educational setting, although at the time this purely served personal interest – this thesis was still several years away from conception. Notably, Sabin also convenes an optional module on the War Studies master's programme dedicated to wargaming, covering multiple aspects of wargame use and design (including many of those discussed in Chapter 2 and Chapter 4), and students must for their final projects design and construct a wargame based on a historical military campaign or battle of their choosing. Unfortunately, at the time the researcher did not elect to take this module simply because others appealed more. In hindsight, the researcher missed out on knowledge and experience which would have served them well for this thesis – although they have been able to catch up on much of the module's content as it is contained within Sabin's *Simulating War*.[380]

The second outcome from the researcher's education are the benefits which come with the King's brand. The Department of War Studies carries a very good reputation, both within the UK and internationally, from which the researcher has been able to derive a certain degree of personal credibility by virtue of being a War Studies graduate. Partly as a result of this reputation, many King's graduates go on to work in prominent positions the military, civil service, security organisations, and other companies, many of which are prime targets for the research in this thesis.[381] Although the researcher has not formally exploited the university's alumni network to build a contact network, being able to appeal to their King's background has enabled them to build rapport with key individuals they have met who also happened to be War Studies graduates. This combination of King's reputation and connections has created access routes to organisations which may not otherwise have been open – see Section 7.1.1 for further discussion. Importantly, these exact same effects have also been possible in the cyber security world thanks to Royal Holloway's Information Security Group, which has a comparable reputation and connections. It is entirely possible that

[380] Sabin (2012)
[381] Department of War Studies Employability website

conducting this thesis research without the gravitas associated with both King's and Royal Holloway would not have achieved the same outcomes.

Employment

The final facet of the researcher's background pertinent to shaping this research is their employment history, the most important part of which is the 18 months (6 full-time then 12 part-time during their master's) they spent working for an events company organising conferences, exhibitions, and industry fairs. More specifically, the researcher worked for the part of the company organising such events for the defence and security industry, ranging from conferences with 150 participants to international exhibitions with 34,000 visitors. The researcher's role was on the VIP team and involved liaising with senior military, government, and diplomatic officials both in the UK and overseas regarding their attendance at the events. Having had no prior first-hand exposure to the military or defence-industrial complex, the researcher's time in this role was invaluable in terms of immersing them in the cultures of these worlds and learning how to communicate with the people working there. The peculiarities of communication in this environment should not be underestimated; Cohn, for example, notes how she was 'startled' by the language used, particularly the liberal use of acronyms.[382] Given that a lot of the fieldwork conducted for this thesis involves defence-related organisations, being able to interface with this environment seamlessly is an invaluable skill, partly to ease the flow of communication when setting up the fieldwork and partly to avoid any friction during the fieldwork itself.

5.2.2 Strategy for targeting research participants

In Section 1.1 it was stated that the theoretical target audience for the game were senior policy- and decision-makers, though that in practice participants came from a wide range of backgrounds. Moreover, with reference to Appendix C, it may be noted that there is a high proportion of military and central government organisations in the list of participating organisations. Out of 14 distinct organisations, 5 are affiliated with the military and 3 with government, while many of the mixed sessions also had representatives from these organisations.

[382] Cohn (1987), p. 703

The prevalence of military and government among the participants can be traced to two factors. Firstly, the researcher made a concerted effort to make inroads with government organisations because this had been identified as the primary source of senior policymakers. Indeed, the conceptual "moon shot" for the thesis was Number 10 Downing Street – to have the Prime Minister play the game. Without any direct contacts at those ultra-high echelons of government, attempts were made to build relationships at lower levels, with a view to working upwards as the game gained traction. This resulted in multiple central government organisations taking part in game sessions, even if the ultimate aim of reaching Ministers was never realised.

Secondly, as outlined in Section 2.1, owing to the history of wargaming there is a close synergy with the military. Notwithstanding the presence of "war" in the terminology, the military pioneered wargaming and are therefore attuned to its use. Although Perla has noted that wargaming goes through peaks and troughs of popularity, at the time of writing the thesis wargaming is near one of these peaks.[383] The aforementioned memorandum from Robert O. Work (see Section 2.2.1) exemplifies this in the US, while in the UK renewed interest in wargaming is evidenced by the 2017 release of the Ministry of Defence Wargaming Handbook.[384] Combined with the researcher's strategic positionality, which as outlined in Section 5.2.1 contains significant military and defence elements, the game therefore quite naturally attracted attention from military organisations, resulting in their participation in game sessions.

What should be clear from the preceding paragraphs is that while some efforts to garner research participants were directed, much of the traction of the game grew organically. This resulted in the participation of organisations which the researcher had scarcely been aware of, let alone targeted. The details of this process, including the role of strategic positionality and 'snowballing', are extensively analysed in Section 7.1.1.

[383] Remarks made by Peter Perla at the Connections UK Conference, 9 September 2015, London, UK

[384] Defence, Concepts and Doctrine Centre (2017), in which the researcher actually features, see p. 37

5.2.3 Security and classification of information

Issues surrounding access are well-covered in ethnographic literature. Hammersley and Atkinson note that while access is often a practical matter concerning physical presence[385] and relationships with gatekeepers[386], there are also theoretical understandings about how negotiating access feeds into the research[387] and ethical considerations.[388] What Hammersley and Atkinson's account lacks, however, is a thorough treatment of the effect of secrecy and classification on ethnographic practice, despite citing examples where this would have been relevant.[389]

This thesis is written at an entirely unclassified level. All sources consulted are public and open, and no security sensitive material is actively sought in gaming sessions or meetings. Cyber security, however, is notoriously over-classified and problems of secrecy may prove a hindrance to access to material.[390] This problem is by no means a nascent one. Nearly 60 years ago, Robert Specht noted that with regards to wargames:

> 'Unfortunately, the operations and results of such games [national policy-making level] are hedged about with tight security restrictions - the reports bear, in fact, the security classification BBRSC, which stands for "Burn Before Reading and Shoot the Courier."[391]

Although tongue-in-cheek, the underlying point remains valid. It is perhaps little wonder that post-wargame reports are enshrouded in such secrecy; after all, they would provide an adversary with useful insight into how the organisation playing the game operates, how they might react in certain situations, and, above all,

[385] Hammersley and Atkinson (2007), p. 43
[386] Ibid., p. 49
[387] Ibid., p. 41
[388] Ibid., pp. 42-43
[389] For example, Anna Lisa Tota being suspected of being an Italian Secret Service infiltrator, Hammersley and Atkinson (2007)., p. 41
[390] Testified by General Michael Hayden, ex-CIA and NSA Director, in *Zero Days* (2016)
[391] Specht (1957), p. 14

what they know (or think they know) about the adversary. With this in mind, Nina Wilhelmson and Thomas Svensson suggest that issues of security, accreditation and secrecy should be settled before even the planning of a wargame commences.[392] With cyber security being high on many lists of national priorities, classification is especially pertinent in cyber wargames. Reporting to US Congress on the first ever cyber security exercise conducted by the US National Security Agency, ELIGIBLE RECEIVER, Steven Hildreth complained that 'reliable, unclassified results are hard to come by.'[393] Despite the justified reasoning behind such secrecy, classification is nevertheless a methodological problem for this thesis, as it is restricted in what previous work it can draw on, which participants can be accessed, and what these participants can contribute – see Sections 7.2.1 and 7.2.2 for discussion of how these restrictions were realised.

Despite being conducted at an unclassified level, during the course of the research sensitive material was nonetheless encountered. The restrictions on what could be divulged about PwC's *Game of Threats* (Section 3.2.1) illustrate the resulting tensions of unwittingly gathering commercially sensitive material. Similarly, in creating a safe space (Section 2.2.7), players may feel comfortable sharing things they would not otherwise have done, or at least would not want attributed to them. Although anonymity may be relatively easy to preserve, there is some disciplinary resistance to further secrecy-enhancing practices. Gerald Berreman, for example, states that 'the repudiation of secret or clandestine activity in the name of anthropology has been the most long-standing and the most consistently, unequivocally enunciated of ethical principles embraced by American anthropologists.'[394] This thesis may not be an anthropological endeavour, but Berreman's words provide a note of caution about tensions that may arise during the course of conducting and publishing ethnographic research. One the one hand there is a need to preserve security and privacy, and on the other an impetus to publish research stemming from privileged access not available to other researchers.

[392] Wilhelmson and Svensson (2013), pp. 22-23
[393] Hildreth (2001), p. 4
[394] Berreman (2012), p. 341

5.3 Facilitation and adjudication

Although some wargames are self-contained, most professional games are convened by a second-party (the game designer) or third-party (other convenor/facilitator). Sometimes the convener simply introduces the game and explains the rules then lets the players play, but often the convener acts in a pivotal facilitating role where they enforce the rules and adjudicate on outcomes. There can therefore be great pressures on the convener to perform their role impartially, consistently, efficiently and confidently.

In his practice-based doctoral thesis, Anders Frank states that the role of the instructor (facilitator) is two-fold: to 'support players' role-play and professional orientation' and to 'explain events in the game by providing real-world references.'[395] While the first part seems straightforward, there is widespread disagreement with the second. A whole host of authors attest that the facilitator should very explicitly *not* explain events in the game, but should allow and encourage players to do this themselves. 'A facilitator isn't there to give opinions,' writes Terence Mahoney, 'but to draw out the opinions and ideas of the group members'[396] to create what Warren Wiggins refers to as a 'feedback-loop.'[397] This conviction is reinforced by both Steven Downes-Martin who says that 'it is the players' job to illuminate the problem with insights and understanding, not the adjudicator'[398] and Shawn Burns who concludes that 'focused discussion led by a war game faculty member [facilitator], as opposed to a rambling free-flow player-led discussion, can drive the discussion toward reflection related to game objectives.'[399] The point here is that that facilitator/adjudicator role is to guide players, but not necessarily to impose their own interpretation of and on the game.

The task of prompting players to create their own learning moments is not an easy one, requiring strong pedagogic and interpersonal skills on behalf of the

[395] Frank (2014), p. 73
[396] Mahoney, p. 1
[397] Wiggins, p. 1
[398] Downes-Martin (2013), p. 71
[399] Burns, p. 3

facilitator. Some of this may be aided (or hindered) by positional factors, such as the gender of the facilitator when working in gender-imbalanced settings, but a lot also hinges on the facilitator's observation and communication abilities. Frank provides the useful insight that a turn-based game was better for 'getting a grip on the situation' because the pace of the game was slower.[400] Aside from the personal characteristics of the convenor, the game setup and locale should also foster an engaging and participatory environment. In particular, Wilhelmson and Svensson prescribe a 'positive atmosphere' where 'participants should not feel vulnerable or that their weaknesses have been exposed to their colleagues and superiors.'[401] Similarly, Burns highlights 'concern for being critiqued by peers or seniors for speaking contrary to the collective view of the group' as a barrier to reflection.[402] Selection of players therefore becomes paramount, as do the rooms in which the game is played, and who is able to observe the game in-play and read any post-game reports. Should participation in the game therefore be limited to players of equal seniority, encouraging a freer exchange of views at the expense of seniors not being there to share directly in the learning moments and juniors to provide specialty input? There is no definitive theoretical answer to this question; the approach taken will vary depending on the circumstances of each game.

On a practical level, the game designer and/or facilitator may not have any control of these factors, instead being constrained by what the participating organisation is able to arrange. A game for six to eight players, for example, might be best played on a medium-sized table in a private boardroom, but the host organisation is only able to arrange a large lecture hall requiring an improvised playing surface of smaller desks joined together, or a noisy recreational room where the choice of surface is limited to a snooker table, knee-height coffee table, or the bar. All of this should be kept in mind throughout the game cycle, including designing, playing, and evaluating the game. A multi-purpose game intended to be reused in many settings needs to be less sensitive to situational changes, whereas a bespoke one-off game can be tailored to factor in the spaces available and players who will participate. Similar considerations also apply to the game facilitator. A formal setting might require a more authoritative voice and presence, while an

[400] Frank, op. cit., p. 95
[401] Wilhelmson and Svensson (2013), p. 19
[402] Burns, p. 3

informal setting invites a more relaxed demeanour. In cases where the facilitator follows the game to different settings, as in this research, a great degree of adaptability is clearly required. The researcher's experiences in this regard are discussed in Section 7.1.2.

5.3.1 Tactical Positionality I

In contrast to the strategic positionality outlined previously, tactical positionality is here used to refer to short-term localised influences and constraints. Issues around tactical positionality emerge from the quadruple-hatted role assumed by the researcher. For this thesis, the author simultaneously acted as game designer, game facilitator, game adjudicator, and PhD researcher. The tensions between these are broadly divided along two fault lines: between designer and facilitator/adjudicator, which is addressed in this section, and between facilitator/adjudicator and researcher, which is treated in Section 5.4.2.

The tensions between the designer and facilitator/adjudicator roles fall into two categories. First might be called the trap of the overzealous salesman. For this research, designing a game was not sufficient, the game must also be deployed. In order to get buy-in from prospective players, the virtues of the game would need to be communicated to them: why the organisation should commit staff and time to playing the game and what the potential learning outcomes are for players. The potential pitfall here is that the game's benefits are over-sold, either unwittingly by an overenthusiastic designer, or wittingly in the quest for (more) participants. If the game fails to deliver on the promised benefits, participants will be disappointed, which not only yields negative (though valid) data from that game session but can also hinder the game from gaining traction for future game deployments. Such a failure to deliver can either be actual – players did not achieve the touted learning outcomes – or perceived – players achieved learning outcomes, but the organisation did not see the value of the game in eliciting these. Actual failure points to erroneous game design or delivery which may require changes in game construction or deployment, whereas perceived failure should be mitigated by expectation management. However, Dunnigan points out that 'the difference between a false prophet and a real one is usually only

detectable after it's too late,' meaning any corrective efforts may be futile as the damage (for example to the game's or the designer's reputation) may already have been done.[403] The optimal solution, therefore, is to be cognisant of the trap of the overzealous salesman at the outset of the research, and factor this in when communicating the benefits of game to potential participating organisations, to prevent the researcher from becoming a false prophet.

The second category is taking feedback personally. As the owner of the product, it would be understandable for the designer to develop a personal and professional attachment to the game. After spending up to 2000 hours designing a game, the game can become an extension of the designer themselves in terms of their personal and professional identity.[404] If players offer feedback about the game to the facilitator it is then entirely plausible that the designer (being the same person) takes this feedback personally, especially criticisms. This could be envisaged as a potential pitfall as it may create a sour environment in the game session with a despondent designer causing the facilitator to be unenthusiastic or the adjudicator to be impartial against the critical party. In this sense, we would benefit from heeding the advice of Harriet Hawkins who, as part of her work on creative research methods, highlights 'the importance of appreciating the processes of creative practices…rather than only as a means of production leading to an output.'[405] A wargame designer may feel an attachment to their creation, but if this feeling overrides the perceived value of feedback (part of the creative process), a large part of the purpose of the game is lost. While a level of pride in the game should be maintained, it can be posited that it is equally important to be able to disassociate from the product during the course of critical feedback.

[403] Dunnigan (1992), p. 110
[404] Dunnigan (1992), p. 271
[405] Hawkins (2015), p. 264

5.4 Methods for capturing game results and player experiences

In order to measure whether learning objectives are met, devices for tracking players' thoughts and actions within the game and for recording game outcomes need to be constructed. Although a plethora of data collection techniques are available, and a selection are discussed in this section, there are few established standards for which techniques should be used in wargaming, because what is recorded and how this is done depends on the design of the game and the learning objectives, which are unique to each game. Rather than outright emulation of any previous research in this field, this thesis therefore builds a bespoke data collection mechanism, but to avoid the 'anything goes' grounded theory trap, analysis of existing literature can illuminate some basic approaches and pitfalls with this process.

There are two primary targets for data collection. The first is interaction between players, which falls into three broad categories: interaction through game play (such as capturing another player's pieces), direct interaction (such as negotiation or trade within the rules of the game), and social interaction (outside the rules of the game).[406] The second is interaction between the players and the facilitator/adjudicator, either as part of gameplay or in discussion sessions outside the rules of the game. All of these interactions are likely to contribute towards players achieving learning objectives and should therefore be recorded as the game progresses.

In other research using games, notably by Johnathan Klein and Dale Cooper, attempts have been made to capture players' internal thought processes through 'cognitive mapping' which 'provides a means of representing the way in which a decision-maker models his decision-making environment, in terms of the concepts he himself uses.'[407] Though certainly interesting and potentially useful, two factors hinder this technique from being applicable to this research. Firstly, having

[406] Nicholson (2010), p. 25
[407] Klein and Cooper (1982), p. 64

players continually reflect on their own decisions is likely to interrupt the flow of the game, thus interfering with its immersive qualities. Given that this thesis is more interested finding out the potential value of games than analysing players' decision processes, it seems imprudent to jeopardise the former in an attempt to capture the latter. Secondly, these maps can only be developed from a rich recording of game progress, player interactions, and player thoughts, so they are dependent on thorough data collection in the first place. With the research in this thesis being highly experimental, it is not known a priori whether the data collected could satisfy the requirements for cognitive mapping. As such, this technique will not be pursued as part of this research.

5.4.1 Data gathering methods

Existing wargaming literature points towards data gathering techniques that may be employed in this space. In a handbook for wargame designers, the US Naval War College outlines four: summaries of player discussions, survey questionnaires, player-submitted game products (such as move sheets), and transcripts of final plenary discussions.[408] Defence company Boeing, in delivering a wargame for the UK Ministry of Defence, used seven types of data collection techniques: pre-experiment questionnaires, analysts' observations, Instant Messenger logs, situational-awareness survey sheet, end-of-session questionnaires, semi-structured interviews, and end-of-experiment questionnaires.[409] Of these, Instant Messenger logs can be immediately discarded for this thesis since these are only applicable to computerised games. Additionally, evidence from wargaming, specifically cyber defence exercises, suggests that questionnaires are unreliable because it can be difficult to motivate players to fill them out.[410]

In keeping with the foundations of a joint grounded theory-ethnographic practice approach to research, three of the techniques provided above appear most suited to this research: summaries of player discussions, player-submitted game

[408] Burns, ed. (2013), pp. 41-42
[409] Multinational Experiment 7 (2013), p. 3-1
[410] NATO Cooperative Cyber Defence Centre of Excellence (2010), p. 17

products, and analysts' observations. Discussion summaries and analyst observations are recorded via the thesis' primary data gathering method: fieldnotes; while photographs are used as supplementary evidence. There are also player-submitted game products in the form of Record Keeping Sheets which provide quantitative data about game progress. Each of these methods have advantages and drawbacks, which are evaluated below, followed by two rejected data gathering methods involving video and voice recording.

Fieldnotes

The most obvious and prevalent method of capturing researchers' observations is through diligent and extensive notetaking. This thesis relies on the researcher taking advantage of their privileged role as game facilitator to gather insights into players' attitudes, behaviours, and communications. Although seemingly simplistic, notetaking is not necessarily a straightforward practice. Returning to Hammersley and Atkinson, notetaking is selective, fraught with trade-offs between breadth and depth, dependent on what the researcher perceives as important, suffers from issues with timing and covert/overtness, and the character of notes can change as the research progresses.[411] Many of these aspects are captured in issues around tactical positionality (see Section 5.4.2), but it is important to be cognisant of the potential pitfalls in relying on notetaking as the primary data gathering method. The experience of the researcher in using fieldnotes, as compared to the theoretical background provided here, are evaluated in Section 7.1.2.

Record Keeping Sheets

Record Keeping Sheets are a game component created for the game used in this thesis which allows players to track the state of the game as it progresses. Each Sheet (one per team) contains tables which the players fill out every game turn, effectively recording the placement of counters and cards across the game board. Completion of the Sheets is a mandatory part of gameplay and is therefore a

[411] Hammersley and Atkinson (2007), p. 142

guaranteed source of data. The data is entirely numeric and is in the same format for each game session. As a result, the data accumulated over the course of multiple gaming sessions constitutes a quantitative dataset which can be mined for statistics. During the course of game development, such statistics help game designers balance a game. In an analytical game, statistics are also the core mechanism for deriving lessons from the game and for measuring player or team performance. While the game produced for this thesis is educational rather than analytical, it would be a shame to let the data go to waste. As such, some statistical results are produced in Sections 6.1.2 to 6.1.4, though they are only intended to as anecdotal highlights rather than substantive insights.

Rejected data gathering methods

One visual data gathering method adopted by some researchers in this space is to capture video. This was used by Frank in his doctoral thesis[412] and by Frey et al in their studies using *Decisions & Disruptions*, but neither reflected on their experience of using this data gathering method.[413] From a critical perspective, a more insightful source is Daniel Bos, who utilised video recordings of game players to analyse their interactions with games in his geopolitics study of the *Call of Duty* video game franchise. Bos' experience with this method reveals the consequences of imposing an artificial research environment on participants: in doing so he undermined the 'everydayness' of play he intended to capture.[414] Attempting to overcome this problem, Bos altered his method from a laboratory-like setup to filming participants in their own homes. Crucially, however, all participants who agreed to this were close friends of Bos and their awareness of his research objectives impacted how they behaved in front of the camera.[415] To borrow a phrase from Sarah Pink, such 'camera consciousness' does not adhere to the principles of ethnography, which hold that participants should be recorded in everyday settings.[416] Although it has already been established that the game sessions used in this thesis do not constitute everyday settings, it is nonetheless

[412] Frank (2014), pp. 35, 41
[413] Frey et al (2017), p. 7
[414] Bos (2015), p. 53
[415] Ibid., pp. 54-55
[416] Pink (2007), p. 99

important to avoid introducing extra-ludic elements which can distract players from approaching a game in a natural manner. For this reason, the presence of a video camera was assessed to be overly imposing and likely to alter players' behaviour in the game, and therefore rejected as a data gathering method.

Another method utilised by Bos was to record his own thoughts about a game, during gameplay, by using a Dictaphone.[417] This approach is suitable in an autoethnographic setting, where the researcher is also the subject of research and/or interacting with the object of research. However, as further elucidated by the tensions of tactical positionality in Section 5.4.2, capturing introspective voice recordings during a game session would not have been appropriate for this thesis. Pausing a game session, even briefly, to record observations or comments would likely be intrusive on the players and made them self-conscious about their actions and interactions in and around the game. An alternative would be for the researcher to remove themselves from the immediate game area to make the recording out of earshot of the players, but this would also mean removing themselves from the role of facilitator/adjudicator. Neither approach was deemed constructive for the research and voice recording was therefore rejected as a data collection method.

Ethics and consent

An important consideration when working with human research subjects is the issue of ethics and consent. Royal Holloway has ethical review processes which all research must pass through to protect research subjects, researchers, and the institution itself. These review processes ensure research will not cause harm to participants, whether physical or psychological, and that research adheres to moral and legal guidelines, for example when monetary or other rewards are offered to participants for taking part in the research. When research has the potential to cause harm or tread moral boundaries, participants should be informed of any anticipated consequences and consent to participating in the research. The processes are also intended to ensure research complies with data protection principles; participants should know what data is collected about them,

[417] Bos (2015), p. 42

how this data will be stored and used, and be allowed to opt out of the research if they wish.

Limitations on consent

Despite procedures to ensure informed consent, it is not a straightforward consideration, as Hammersley and Atkinson put it: 'consent is often neither possible not desirable in ethnographic (or, for that matter, other) research.'[418] Examples abound of covert research where participants were unwitting and therefore could not consent to taking part[419], or of acceptable deceptive practice by researchers.[420] Hammersley and Atkinson also provide a series of reasons why informed consent may not be practical, and in the context of this thesis, even though the research was overt, three of these reasons are particularly pertinent.

Firstly, 'continually seeking consent may be disruptive to the research.'[421] During the course of a game session, the flow of events and player discussions could be interrupted if the researcher frequently paused proceedings to ascertain whether a participant agreed to individual actions or comments being included in the research data. Sami Abuhamdeh and Mihaly Csikszentmihalyi state that a commonly reported feature of 'flow experiences' is 'high attentional involvement', so any disruption to flow may impact participants' attention to the game (see Section 6.3.3 for discussion of engagement).[422] Furthermore, from a logistical point of view, such pauses would also use up time in a game session, which was often capped. As discussed in Section 4.1.1, the game design was intended to minimise time participants did not spend interacting with the thematic content of the game, and continually seeking consent would counteract these efforts.

Secondly, 'the researcher may not know what the research will entail or what the consequences will be.'[423] For this thesis, the evolving nature of the research meant data gathering requirements changed as the research progressed. At the

[418] Hammersley and Atkinson (2007), p. 42
[419] Ibid, p. 210
[420] Ibid, p. 211
[421] Ibid., p. 210
[422] Abuhamdeh and Csikszentmihalyi (2012), p. 265
[423] Hammersley and Atkinson, op cit., p. 210

conception stage, the focus of the research was very much the wargame itself – a legacy from the genesis of the thesis (see Section 1.3) – and any human participation was anticipated to merely feed into the improvement of the game. As the research advanced, the focus shifted from the game to the participants, with the game design remaining constant (as described in Chapter 4) and data instead being gathered about player interactions with and around the game. In line with the grounded theory approach of the research, however, it was not known precisely what this data would capture or reveal, so a complete assessment of the impact of the research was not practical a priori.

Finally, 'divulging information about research purposes may alter participant behaviour, invalidating the research.'[424] It is possible that participants would act differently in a game session if they were aware of the kinds of observations and notes the researcher was making. For example, if the researcher had said that they would count how many times people take out their phones (a possible sign of disengagement), participants may consciously or subconsciously suppress any desire to take out their phones, because they know this would be recorded. Alternatively, participants may exaggerate actions they perceive as positive, such as humorous remarks. In both cases, the natural disposition of the participant would be compromised. This is similar to Pink's phrase 'camera consciousness' for research subjects who alter their behaviour because they are on camera (as discussed regarding rejected data gathering methods). Returning to Abuhamdeh and Csikszentmihalyi, another feature of 'flow experiences' is 'a reduction of self-consciousness', so making participants conscious of their actions, by way of informing them about research purposes, could disrupt the flow of the game or discussion.[425]

Efforts to obtain informed consent

Throughout the fieldwork conducted for this thesis, all game sessions included a verbal briefing by the researcher about the nature of the activity that was about to take place. Players were informed that the game session formed part of ongoing academic research into cyber wargaming and that the

[424] Hammersley and Atkinson (2007), p. 211
[425] Abuhamdeh and Csikszentmihalyi (2012), p. 265

researcher/facilitator would be making observations and taking notes about player behaviour and interaction in the game environment. At this point players were able to opt not to participate in the game session, but none did, thereby granting the researcher a manner of consent to continue with the game session as described.

Approaches to gathering consent in related research varies. One method is to hand information sheets to participants explaining how their data might be used, which they can sign to formally declare informed consent. In similar PhD projects where player observation was central to the research, use of such information sheets has been inconsistent: Bos, for example, did use them[426], while Frank did not, opting instead to remediate ethical concerns in game debriefings.[427] The verbal consent obtained for this research seems to fall somewhere in between these approaches, and to ensure privacy of participants, the thesis has been anonymised so that no individual participant nor organisation can be identified from data gathered and presented in this document (publicly available data notwithstanding). This has been done to protect players who were acting and speaking in a safe (as per Section 2.2.7) and highly-engaging environment (see Section 6.3.3), where they may have forgotten that they were participating in research.

5.4.2 Tactical Positionality II

The emphasis of this research on participant observations comes with tactical positionality caveats which need to be taken into account. In the Boeing game documentation, it was noted that 'observing and gathering relevant information without interfering in a task, influencing subjects or biasing [player] decisions is tricky to balance.'[428] These warnings are reinforced by Wilhelmson and Svensson, who say that

[426] Bos (2015), Appendix E
[427] Frank (2014), p. 94
[428] Multinational Experiment 7 (2013), p. A-1

> The evaluator should carefully reflect on the most ideal place to be during the exercise so that participant observations can be done in the best possible way. However, it is important to note that it is not good to be too close to the participants since this can disturb them or since this runs the risk that the evaluator is "drawn into" the exercise.[429]

From this evidence we can infer that there is a careful balance the convener must tread between being a good facilitator to achieve learning objectives and a good evaluator (researcher) to ensure proper data collection. A good facilitator is physically involved in the thick of the action, immersing themselves in the game so that the players feel the facilitator is simply a part of the activity.[430] A good evaluator, on the other hand, is removed and invisible, seeing and hearing proceedings but not interrupting the game itself. When the convener is a single person, as in the case with this thesis, this dual-role can be envisaged to be particularly tricky to manage.

In addition to the evaluator disturbing the conduct of the game, the researcher may let this role influence their role as facilitator/adjudicator. It may be that the researcher is looking to duplicate an earlier observation, leading them to abuse their role as adjudicator to force a particular outcome to the game. This is not only unacceptable academic practice, but also nullifies the point of the game. 'In order to retain the value of wargaming,' says Sanu Kainikara, 'it is of utmost importance to ensure…the progress of the game is neutrally observed to ensure impartiality at all times.'[431] Although true impartiality may not always be achievable, managing the position at the nexus of adjudicator and researcher is a key aspect of this research.

5.5 Data analysis methods

In ethnography there are myriad techniques for analysing data collected from fieldwork. Depending on the types of data, the analysis might involve textual

[429] Wilhelmson and Svensson (2013), p. 96
[430] Kriz (2010), p. 667
[431] Kainikara (2003), p. 27

interpretation, auditory transcription, or visual inspection. When research has a clearly defined question or objective, this helps guide the analysis by providing a lens through which to view the data. For this thesis however, although a central research objective exists, the objective is open-ended and the appeal to grounded theory in the methodology is intended to enable findings to emerge from the data, rather than data be channelled into narrow lanes of investigation.

With this in mind, data analysis of this thesis comprised the following method. First, as outlined in Section 5.4.1, primary data from game sessions was gathered in the form of hand-written fieldnotes and player-submitted record keeping sheets. These notes and sheets were then digitised by transcribing them into two spreadsheets. The first spreadsheet contained the notes taken by the researcher, appended with metadata including:

- Session identifier
- Types of players taking part in the session (see Section 6.1 for further details)
- Type of note (researcher observation, participant quote, participant feedback)
- Timing of the observation or quote (pre-game, during game, or post-game)

As the notes were typed into the spreadsheet, the researcher also coded them by assigning categories and labels regarding what learning moment was enabled (using the game design in Chapter 4 as a guide to defining codes) and/or what link to wargaming theory that note provided (such as engagement, decision-making, or facilitation). The result of this process was a chronologically-ordered record of every fieldnote, but owing to the additional metadata and coding, it was possible to simply sort the spreadsheet so that all related notes from different game sessions were grouped together, making it easy to compare and draw links between them.

In the second spreadsheet, the numerical values from the record keeping sheets from each session were entered to create a database of game progress and results. By running various queries against the data, some tentative findings could be extrapolated (see Sections 6.1.2 to 6.1.4). Furthermore, this spreadsheet

contained data about participant types and numbers, meaning this data could be spliced and interrogated for further insights (see Section 6.1.1). It should be stressed that for both spreadsheets, the data structures were not imposed by the research questions, but were instead intended to be as open as possible to allow findings to emerge as the datasets grew and were analysed.

Chapter 5 Conclusion

As a practical research endeavour, this thesis is informed by two theoretical foundations: grounded theory and ethnography. These have long histories of academic use and attendant literature both critiquing their utility and guiding researchers in how to employ the techniques contained therein. In analysing this literature, it has been concluded that neither grounded theory nor ethnography can be applied in their entirety to this thesis, but are instead used in inspirational modes, informing the research without binding it to methodological constraints. This is not indifferent from Elg's research approach, for whom grounded theory was useful in inspiring the creation of new theory, but only insofar as theory informed practice. In this thesis, the inspirational mode is adopted with full consciousness of Suddaby's warning that grounded theory is often erroneously viewed as 'anything goes', and justifications have been offered for every modification made of grounded theory. This is also true of ethnography and the thesis only wholly embraces two out of five facets outlined by Hammersley and Atkinson, yet with good reasoning behind these choices.

Methodologically, the most original contributions of the thesis are in formulating what was termed strategic and tactical positionality. Positionality has received ample coverage in both ethnographic and wargaming literature but has not previously been associated with the terms 'strategic' and 'tactical.' Thinking about positionality in this way frames the problem more militaristically, thereby bringing the problem closer to the roots of wargaming. The value here is in aligning disparate strands of literature along the same lines and relating everything back to wargaming, which is the core of the thesis.

Chapter 6: Pedagogy and practice in cyber wargaming

This chapter outlines and analyses the outcomes of 33 game sessions conducted with a variety of participants. Rather than treat each session individually (a full list can be found in Appendix C), the chapter is structured according to themes which emerged during data analysis. Many of these were designed into the game as outlined in Chapter 4, but several themes pointed to learning moments which had not been deliberately designed for The themes address the central thesis objectives by elucidating *what* participants discussed during game sessions, but also evaluates the efficacy of the game as a teaching tool by analysing *how* players engaged with the game.

The chapter is broadly divided into three parts. The first part provides a quantitative overview analysing metadata about players and data about game results, linking these to theoretical and methodological aspects highlighted previously (Chapters 2 and 5 respectively). The purpose here is to demonstrate alternative uses to wargaming, such as the analytical approach favoured by McNamara (Section 2.1), though this was not the primary intention of the thesis and the findings are illustrative rather than prescriptive.

The second part of the chapter analyses qualitative data collected in terms of researcher observations and player discussions. These form an original contribution of the thesis to wargaming, building on the tentative findings of the likes of Rieb and Lechner[432] and Barnard-Wills and Ashenden[433], whose games were analysed in Chapter 3 (Sections 3.2.1 and 3.4 respectively). In order to address the central thesis objectives, the analysis is organised thematically by the learning moments created in game sessions, where possible aligning these with the purposes served by different game components (as discussed in Chapter 4).

[432] Rieb and Lechner (2016)
[433] Barnard-Wills and Ashenden (2015)

In the final part of the chapter, qualitative data is analysed with regards to some of the theoretical wargaming concepts discussed in Chapter 2, particularly surrounding player engagement. Some ideas, such as Perla and McGrady's 'story-living experience' (cited in Section 2.2.5), are corroborated and validated, while others, such as Jim Wallman's assertion that writing game rules is easy, are questioned. The chapter then concludes with a summary of key points.

6.1 Gaming by numbers: quantitative uses of metadata and game data

From each game session diverse sets of quantitative data were collected. Firstly, metadata regarding players (types, numbers, genders, roles/ranks) were recorded where available. This data can be aggregated and compared to data regarding game progress and outcomes to find out which types of players performed better in the game. The data can also reveal dynamics around which types of people participate in wargaming, allowing us to ask questions about the inclusivity of wargames and how this might be improved, particularly in a cyber security setting.

One of the categories into which this metadata has been sorted is called 'type', signifying the organisational identities of the game session participants. Three primary types were identified: military, civilian, and mixed (game sessions with both military and civilian players). Further, the civilian category has been divided into four subcategories: industry (private companies), academia, civil service, and mixed. All 33 game sessions were classified according to these categories.

Secondly, data about game progress and outcomes (winning teams, Victory Points achieved) was created as part of gameplay, with players completing record keeping sheets during the course of the game, capturing the state of the game during each turn (the amount of Resource and Vitality possessed by each Entity, as well as the number of Black Market assets owned by the teams). These sheets were explained to players as being for the calculation of Victory Points and to

prevent cheating, which was true, but the sheets also recorded a numerical representation of game progress.

By digitising this data, it has been possible to run computations on the numbers, as an analytical wargame would, to find patterns and correlations which reveal information about player behaviour.

6.1.1 The gender imbalance in wargaming

Section 5.2.1 discussed gender imbalances in the military, in wargaming, and in cyber security, concluding that all three fields were male-dominated. Some of that analysis was based on quantitative data – for example UK armed forces figures – but other parts were anecdotal – such as the number of female attendees at the Connections UK wargaming conference, the only conference of its kind in the UK. By collecting data about participants in this research, it is possible to corroborate and strengthen the previous findings regarding the paucity of female participation in wargaming with statistical insights.

Overall, out of 259 participants, 211 (81%) were male while 48 were female (19%). The highest disparity between genders was with military participants, most likely owing to a large starting imbalance amplified by the imbalances in wargaming and cyber security. The greatest parity was found in civil service participants, albeit from a small sample, and with two-thirds male there was still far from equal participation. A full breakdown of categories and subcategories is shown in Table 2.

Table 2: Gender breakdown of game session participants

Category	Subcategory	Male	Male %	Female	Female %
All		211	81%	48	19%
Military		39	91%	4	9%
Mix		67	87%	10	13%
Civilian		105	76%	34	24%
	Academia	26	76%	8	24%
	Civil Service	8	67%	4	33%
	Industry	24	77%	7	23%
	Mix	47	76%	15	24%

These results reinforce the research stated in Chapter 5, which held that the environments the thesis investigates are predominantly male-dominated. The figure of 9% female military participants is close to the overall proportion of females in the UK armed forces (10.2%, as stated in Section 5.2.1). Encouragingly, the 19% female participation rate across all categories exceeds the proportion of females in both wargaming (1% to 16%) and cyber security (7% to 11%) by all metrics used in Section 5.2.1. Indeed, if we exclude the low female military participation rate, the overall figure rises to 23.5%. Despite a lingering male dominance in these fields, it may be possible that wargaming is a potential method to attract more gender diversity to cyber security, and vice versa – cyber security can encourage more gender diversity in wargaming. There is no shortage of research indicating the benefits of gender diversity in organisations, so this finding should be interpreted as a positive result.[434]

6.1.2 In-game performance as a guide to real-world performance

One use of wargames is to derive direct real-world lessons from the game results (the perils of which were discussed in Section 2.3.3). For example, an in-game action with positive results can be interpreted as a guide to action in the real world. Such an approach has been taken by Hagen Lindstädt and Jürgen Müller, who have developed a game theory tool that allows players to go through an

[434] For example Herring (2009); Cumming et al (2015)

iterated decision-making process to find 'the best path for different combinations of factors.'[435] Although originally intended for business managers, this has also been used in a cyber security context.[436] Another interpretation of game results might be that players' accomplishments in the game correlate to their ability to perform their real-world roles. In the LOCKED SHIELDS cyber defence exercise, for example, a scoring system is implemented to measure participants' performance and to structure feedback.[437]

In the game developed for this thesis, the Victory Points game mechanic was designed with player engagement in mind, rather than as a method of ranking players or deriving real-world policy suggestions. Nonetheless, the design process shifted the mechanic away from a subjective measure which would have been different between each game session to an objective measure which was the same in each game session (as detailed in Section 4.3). With such a standardised mechanic, Victory Points can be compared across games and provide some insights along the lines which might be expected in an analytical game. Importantly, however, in this instance the exercise intended to illustrate a possible alternative use for the game; it does not provide any conclusive evidence about player performance.

In terms of results, across all game sessions, the average Victory Points achieved were 19.08. This compares to a maximum score of 47 (achieved by a UK team played by a mix of players) and a minimum score of -2 (achieved by a UK team played by academic players). Looking at averages, the highest performing types of players were civilian industry players (23.33 Victory Points), followed by a mix of civilian plus military players (22.25 Victory Points). At the other end of the scale, the second-worst performers were academics (10.25 Victory Points), while the worst were civil servants (7.50 Victory Points). These scores could conceivably be used as a guide to determine which types of people are most suited to manage strategic national cyber security.

[435] Lindstädt and Müller (2010), p. 3
[436] Author experience at German military education institution A, January 2017
[437] 'Cyber Defence Exercise Locked Shields 2013 After Action Report' (2013), p. 12

What the above conclusion fails to account for, however, is the inaccuracy of the game model. The game is not a simulation tool based on minute reconstruction of the real world. The game takes some aspects of the real world and represents them stylistically, often deliberately inaccurately (for example the non-existence of the relationship between the intelligence community and critical national infrastructure, as discussed in Section 4.2.2). Therefore, to conclude that players' performance in the game is representative of their real-life capability would be akin to concluding that an expert chess player could command armies on the battlefield. A high score in the game only demonstrates proficiency *at the game itself* and does not prove proficiency in any other skill or activity.

6.1.3 In-game results as a guide to real-world results

One of the concerns a game designer should take into account is how closely game outcomes align with real-world outcomes. For historical games based on conflict that has already occurred where the outcome is known, Sabin has outlined different approaches in this space, referred to as the 'width of probability distribution', summarised in Figure 14.[438] The game designer can choose the frequency with which game outcomes mirror the historical outcomes. In games where the outcome distribution is aligned with the historical outcome (a 'narrow' distribution), players who simply follow the historical events will usually not produce an unexpected game result. Consequently, if the players want to achieve an ahistorical outcome they will need to make decisions which do not follow the historical account. As an example, a game depicting the historical outcome of 1815 Battle of Waterloo usually results in British/Allied victory, but to achieve French victory the players would have do something Napoleon did not, perhaps commit the Imperial Guard at an earlier opportunity.

[438] Sabin (2012), p. 55

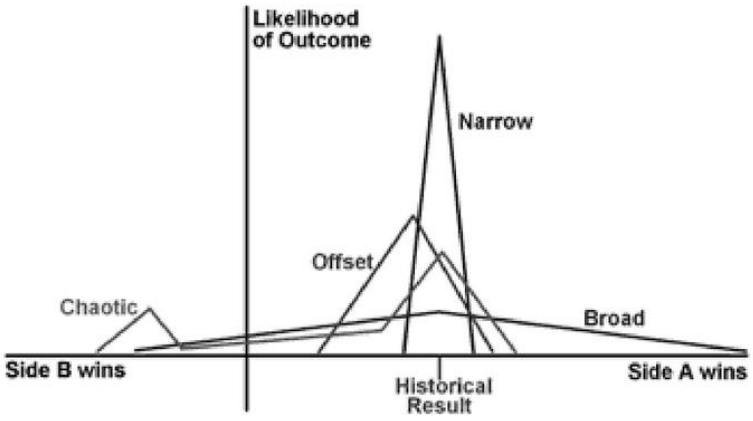

Figure 14: Wargame outcome probability distributions. From Sabin (2012), p. 56

The game designed for this thesis depicted a future, rather than historical, conflict, but it is possible to envisage that Sabin's model can be flipped around to extrapolate predictions. In this approach, the distribution of game outcomes could be interpreted as a guide to the outcomes of future conflicts. Analysing the data through this lens results in a conclusion that a cyber conflict between the UK and Russia would be evenly matched. Across all game sessions, the UK achieved a 50% win rate, with Russia at 42%, and 8% ties – reflecting a design approach which gave both teams a roughly equal chance of victory. Therefore, if the game is a guide to action, it suggests that both the UK and Russia need to make improvements to their current cyber capabilities and/or strategies in order to increase their chance of prevailing in conflict.

Crucially, however, the inaccuracy of the game model means it is not a guide to action. The game outcomes are not intended reflect the probable result of a conflict between the UK and Russia and it would be a mistake to think that the UK and Russia are evenly matched in cyber capabilities based solely on knowledge gleaned from this game. Other wargames do strive to predict the future to help military planners when deciding force composition and disposition – such as the analytical games discussed in Section 2.1 – but that was never the purpose of this game. Indeed, as discussed in Section 4.6, the difficulty of ascertaining cyber capabilities means constructing such an analytical game would be very difficult for this topic. Instead, from a pedagogical perspective it makes more sense to take advantage of underlying assumptions of the game model and use them as

discussion prompts, from which players can derive learning moments and be enabled to ask the right questions.

6.1.4 Playing styles of different groups

To illustrate one final possible use of the quantitative data, figures from the record keeping sheets can be analysed to discern playing styles of different groups. This analysis is based on the 23 game sessions from which record keeping sheets were retained; of the ten sessions for which data does not exist, nine were early playtesting sessions where either the record keeping mechanism had not yet been introduced, or the values had not been standardised so cannot be used for comparison, while in one session (UK government department B) the participants kept the sheets for internal reference (along with a copy of the game).

One approach using this data is comparing one group's values to the average values across all game sessions. For example, looking at the average Resource and Vitality values for Energetic Bear we see Resource steadily decreasing and Vitality increasing. This would be expected since the objectives for Energetic Bear required them to increase Vitality (see Appendix A), which is achieved by spending Resource, and their attacking remit, which also requires Resource commitments (as discussed in Section 4.3.2). By comparison, the data from the second game at Swedish military education institution A suggests that the team which played Russia in this session were more intent on Attacking than completing Objectives. For this team, Energetic Bear had zero Resource from the third turn until the end of the game, meaning any new Resource gained each turn must have been spent, while the Vitality values did not increase (in fact they decreased towards the end of the game, suggesting unsuccessful Attacks). The Resource was therefore not spent on new Vitality, which means it was spent on Attacking (see Table 3), so this team de-prioritised their assigned Objectives in favour of some alternative strategy.

Table 3: Resource and Vitality values for Energetic Bear

	Average		Swedish military education institution A, Game 2	
Turn	**Resource**	**Vitality**	**Resource**	**Vitality**
Start	3	4	3	4
January	3.00	4.52	3	4
February	2.35	4.87	3	4
March	1.74	5.04	0	4
April	1.91	5.18	0	4
May	1.64	5.32	0	4
June	1.09	5.64	0	4
July	0.90	5.62	0	4
August	0.67	5.67	0	4
September	0.44	5.94	0	4
October	0.69	6.00	0	4
November	0.83	6.42	0	3
December	0.08	6.42	0	3

Another approach could be to look at usage of Black Market Assets to measure attacking intent. In the standard setup of the game, both teams were assigned one offensive Asset at the start and Russia would be expected to use theirs (as well as any new ones acquired) because of their attacking Objectives. The UK, on the other hand, had no attacking Objectives, nor indeed any attacking remit (recall the lack of Attack Vectors, as discussed in Section 4.4.3). To even use their offensive Asset, the UK would first need to purchase an Attack Vector from the Black Market. Therefore, if at any point a team playing the UK had zero offensive Assets it must mean they not only used the Asset they had originally been assigned, but also purchased the additional prerequisite Asset. Such a strategy would be a significant deviation from the strategy proscribed by the UK's Objectives, which generally rewarded what some players referred to as "turtling"

– an entirely defensive approach focused on preventing and deflecting Attacks while building up large amounts of Vitality.[439]

Across all recorded game sessions, the Black Market Asset data indicate that eight UK teams pursued an offensive strategy (three mixed civilian, three military, one mixed civilian/military, one civilian industry), yet only three of these were ultimately victorious in the game. Indeed, the offensive strategy was catastrophic in two instances, causing a team from the UK military education establishment B to record a 23-7 loss, and a team from International military education institution A to lose by a margin of 28-7. Interpreting this data in the same vein as an analytical wargame would suggest that just because the UK has offensive cyber capabilities, it should not necessarily use them.

Ultimately, however, it must again be stressed that none of this analysis is meant to accurately represent how these groups might approach strategy in cyberspace in real life. Downes-Martin has argued that such uses of wargames is not possible for games covering novel subject matters, of which cyber security is one.[440] Indeed, by virtue of the game being a safe space to experiment and express views (as discussed in Section 2.2.7), players may often have deliberately acted contrarywise to what their real-world course of action would have been. Importantly, such deliberately experimental actions often present ideal discussion opportunities, from which learning moments can be derived, thereby fulfilling the true purpose of the game. These discussions are not captured in quantitative data, but we must instead turn to qualitative data to discern how effectively these discussions were generated and what was contained within them.

6.2 Learning through the game: expected and unexpected results

In each game session, qualitative data was collected to address the central thesis research objective: what capacity did the game have to create learning moments

[439] Author fieldnotes, 21 April 2016; 6 March 2017
[440] Downes-Martin (2013), pp. 71-74

and enable players to share knowledge and ask the right questions? As discussed in Chapter 4, certain topics were deemed of high importance and were deliberately designed into the game, but there was also a high degree of open-endedness to the design, intended to encourage players to contribute with their own knowledge and understanding to generate pedagogic debate. Resultantly, the observations made by the researcher were partly to capture whether the designed learning moments were discussed, and partly to capture any unintended moments (the challenges for the researcher in observing for both these outcomes are discussed in Section 7.1.2). The following sections analyse learning moments in relation to the themes outlined in Chapter 4 and, where applicable, the game component which prompted the moments to be created. Note that the learning moments presented herein are not comprehensive but selected based on two distinct measures: either how strongly the data suggested that a learning moment was created, or by the volume of discussion around the subject or the strength of the discussion.

6.2.1 Entities

The central components of the game board were the ten Entities representing different actors in cyberspace. Because players engaged closely with these through gameplay they were also popular targets for discussion. These discussions varied between debates around the actors already represented in the game and actors which were not represented but perhaps should have been.

Critical National Infrastructure

CNI was represented in the game via the UK's and Russia's respective nuclear energy operators: UK Energy and Rosenergoatom. Two primary learning moments were created in this area. Firstly, foreign ownership of the UK's nuclear energy sector was debated, with players on two occasions remarking on the UK operations of EDF Energy, a French company. On one of these occasions the influx of Chinese investment was also discussed, which, when UK Energy were taking damage later in the game, led to one player exclaiming: "Where is that Chinese

money?!"[441] For this player, this aspect of CNI had clearly stuck with them as an important consideration, and their vocalisation of this likely provoked other participants in that game session to engage with the topic, thereby enabling participants to ask more directed questions if they were to follow up with discussion or research after the game session.

Secondly, and most crucially, on multiple occasions players engaged in discussions about the diversity of CNI. Recall from Section 4.2.1 that one of anticipated drawbacks of the design choice to explicitly focus on nuclear energy was that other CNI sectors would not receive attention. However, players across the spectrum were able to recognise that CNI comprises more than energy production and were keen to suggest how this Entity could be represented differently in the game. One participant argued that CNI should sit in the middle of the game board because all other parts of the trinity depend on it[442], while banks[443] and National Grid (the UK's national electricity distributor)[444] were proposed as alternatives. In one game session the group decided that CNI should be represented by something which, if not working, would "bring the country to a standstill."[445] After a lively debate which considered everything from supermarket Waitrose (thereby recognising food supply as a CNI sector) to tea-making manufacturers the group settled on train operators.[446]

In terms of providing players with learning moments about the sheer diversity of CNI, this game component can therefore be considered a success.

Russia as an actor

The representation of Russia in the game, as a combination of Entities, was the subject of much discussion, often with a humorous dimension (see Section 7.3 for an in-depth analysis of the role of humour). Remarks around this topic often

[441] Author fieldnotes, 30 March 2017
[442] Author fieldnotes, 24 April 2017
[443] Author fieldnotes, 24 January 2017
[444] Author fieldnotes, 25 April 2017
[445] Author fieldnotes, 29 June 2017
[446] Author fieldnotes, 29 June 2017

centred on perceived characteristics of Russian behaviour and aspects of its autocracy. In one game session, for example, the following exchange was observed when a Russia team was deliberating its Black Market bids:

> Player 1 (to another player): "Don't worry, you can't make a wrong decision."
> Facilitator: "That doesn't sound very Russian."
> P1: "But we know where your children live."[447]

Such exchanges were not uncommon, especially with players who exhibited a high level of engagement with the game (see Section 6.3.3 for further discussion of engagement), and enabled players to disseminate insight into Russian decision-making. However, we must also recognise the caveat that the humour which inspired much of this debate also likely clouded the accuracy of the lessons learned. Unless the players had prior expertise on the functioning of the Russian state, exchanges like the one outlined above were likely based on knowledge of stereotypes depicted in films or literature such as the James Bond movie *GoldenEye*[448] or Tom Clancy's novel (and later film) *The Hunt for Red October*.[449] As Henri Tajfel outlined in a seminal 1969 paper, stereotypes are grounded in reality, but they also exaggerate and distort it.[450] In this sense, players' engagement with the game may in some cases only have served to reinforce stereotypes of the Russian state rather than provide insightful pedagogical outcomes.

On the other hand, when players did have expertise in Russian state behaviour, the game provided an outlet to share these with other participants. On two separate occasions a player (one from a Russian background and one from a Finnish background) noted that there should be some mechanic in the game for Russia to cheat or bend the rules, because that is what they do in real life. The Finnish participant pointed to *maskirovka* (concealment, deception, and disinformation[451]) as an example of this[452], while the Russian participant

[447] Author fieldnotes, 29 June 2017
[448] Campbell (1995)
[449] Clancy (1984)
[450] Tajfel (1969), p. 177
[451] Beaumont (1982), pp. 1-3
[452] Author fieldnotes, 24 January 2017

suggested that stealing Resource from the facilitator's supply or bribing players or the facilitator would not be out of character.[453]

Such remarks exemplify players bringing their own knowledge of the world to a game session and using the game as a tool to disseminate this knowledge to other participants, thereby creating peer-led learning moments

Missing Entities

With only ten Entities on the board representing two countries, the game design was not an exhaustive representation of cyberspace. Players frequently recognised this and were able to discuss which actors were missing and perhaps should be present. The two actors which received the most commentary were Anonymous and China. Anonymous is a hacktivist group which has in the past attacked diverse targets including the Church of Scientology[454], ISIS[455], US security firm HBGary Federal[456], and the city of Orlando, Florida.[457] One civilian player noted that Anonymous' non-affiliation would make them a perfect third party in the game because they can work against both Russia and UK as an unpredictable selfish actor.[458] Military players, on the other hand, agreed that Anonymous should be in the game, but were divided as to how they should be represented. In one session with military players the prevailing opinion ascribed significant threat to Anonymous and that they should therefore be on the game board itself.[459] In another such session, however, one player stated that the absence of Anonymous on the board made sense because the game models state-on-state conflict, but they could be added as a Black Market Asset that allows an unattributable attack.[460]

[453] Author fieldnotes, 30 March 2017
[454] Vamosi (2008)
[455] Lockhart and Burke (2015)
[456] Taylor (2011)
[457] BBC (2011)
[458] Author fieldnotes, 9 February 2017
[459] Author fieldnotes, 24 January 2017
[460] Author fieldnotes, 13 March 2017

China had been omitted from the game design partly because Russia was judged by the designer to be a more imminent threat to the UK, and partly to limit the complexity of the game by only including two teams. The absence of China was noted by a variety of participants. A military observer, for example, asked where China was because "they're the ones doing all the attacking,"[461] while a civilian player in a different session said "they're everywhere."[462] In a discussion during a civilian mixed game session, China was also proposed as an ideal third party because they could be antagonistic towards both UK and Russia.[463] These suggestions for both Anonymous and China, and the rationale behind them, demonstrate how the game enabled learning moments where players could think about the important actors in cyberspace, despite these actors not being represented in the game, and articulate these thoughts to other participants.

Energetic Bear as an actor

Energetic Bear, representing Russian business interests, received only a moderate amount of attention in discussions. One of these discussions, however, was emblematic in demonstrating how the game enabled peer-didacticism between players. In a game session with a civilian mixed group of players, one participant asked a question about who Energetic Bear are. The question was directed at the facilitator, but before they could answer, another player stepped in and provided a detailed and accurate explanation of Fancy Bear (this was not confusion, as cautioned in Section 4.2.1) and Russian use of hacker groups for espionage and crime. They also expanded on this, pointing out that Energetic Bear is a rogue operator and suggested segmenting the game so that Energetic Bear was in a separate room and unable to communicate with the other Russia players.[464] Given that the participant who asked the original question was clearly entirely unfamiliar with Energetic Bear, the game in this case fulfilled its potential for enabling players to ask the right questions, and the information provided by the knowledgeable player can only have been enlightening.

[461] Author fieldnotes, 13 March 2017
[462] Author fieldnotes, 24 March 2017
[463] Author fieldnotes, 29 June 2017
[464] Author fieldnotes, 6 September 2017

The example shows the capacity of the game to enable players to set up informal temporary knowledge-exchange relationships with each other, similar to how Jeroen de Kloet and Liesbet van Zoonen have described 'fans' who share their knowledge and experience of events or cultural artefacts, often with a 'performative dimension.'[465] In this case the performative dimension was the game and the knowledge exchange was a learning moment focused on non-destructive cyber threats.

6.2.2 Entity relationships

The relationships between the Entities represented interdependencies between different actors and the flow of Resource between them. These were the subject of a high degree of attention in discussions, here broken down into three topics: the link between UK Plc and GCHQ, UK Energy's multiple relationships, and the overall asymmetry of the game board.

The UK Plc-GCHQ relationship

Firstly, the relationship between UK Plc and GCHQ had been intended to represent the transfer of expertise between the private sector and intelligence agencies. A learning moment exploring precisely this was borne out in a game session with a civilian mixed group, where one player remarked on the inaccuracy of GCHQ's ability to marshal Resource, to which another player retorted that GCHQ can contract out work to UK Plc, taking advantage of the industrial base.[466] On this occasion, therefore, the game component stimulated the exact debate it was designed to do.

UK Energy's relationships

Secondly, similar to how UK Energy spurred significant debate about its role as an Entity, relationships connecting UK Energy to other UK Entities were also a source

[465] de Kloet and van Zoonen (2007), p. 330
[466] Author fieldnotes, 6 September 2017

of discussion. In two separate game sessions, players suggested that UK Energy should be directly connected to UK Plc[467] and GCHQ respectively.[468] The former of these likely reflects the context of that game session, which was held with a technology company. That company may have seen a role for itself, or the wider industry, either in helping protect CNI, or the suggestion inferred that UK businesses are dependent on electricity production and would suffer if production was compromised. Thinking about the dynamics of this issue allowed players to create learning moments which were not designed into the game. The latter suggestion, on the other hand, fulfilled a conscious design choice, in that realistically GCHQ does have a role to play in protecting CNI, but omitting this relationship in the game prompted discussion about the topic (as discussed in Section 4.2.2).

In one game session, UK Energy's relationships were discussed with regards to the context of Germany, where the game session was taking place. Here, one military player suggested that if the game design was based on Germany, the link between Government and CNI would have to be removed because the German government only regulates, it does not make investments.[469] This observation demonstrates how the game can be used to challenge participants to consider alternative approaches to energy policy, and more broadly that strategy and policymaking are dependent on geopolitical context. This stands out as an example of players bringing their own knowledge to the game and using it to enhance learning moments for the wider group.

Asymmetry of relationships

Finally, one of the most prevalently discussed aspects of the game's relationship was the asymmetry between the two sides. The design rationale behind this was discussed in Section 4.2.2, and it was encouraging that so many players were able to engage with the concepts contained within this game component. In one session with civilian industry players, the rationale was understood almost

[467] Author fieldnotes, 30 March 2017
[468] Author fieldnotes, 13 March 2017
[469] Author fieldnotes, 24 January 2017

verbatim, with participants noting how the UK's better interconnectedness made them more vulnerable to residual damage from an attack, but also conferred an advantage in transferring Resource.[470] Feedback from a military player in another session stated that their takeaway from the game was that "non-mirrored adversary models mean teams play to different rules."[471] For this player it would be clear that projected thinking – thinking that others think the same way as you – likely leads to misconstrued understandings of adversaries: every country's context will influence how they approach policy and strategy, so we cannot assume that the UK's approach is followed elsewhere. Also noteworthy is how this player's interpretation the game and articulation of this interpretation reveals information about their professional and academic training. The player had a prior understanding of adversarial modelling, perhaps learned through military education, and this understanding shaped the learning moments they were able to create in the game.

As a final example, we can consider the civil servant player who expressed their frustration at not being able to move Resource freely.[472] It is unclear whether this frustration was also prevalent in their real-life role as a policymaker, in which case the game would be an accurate representation, or whether this was simply limited to the game itself. Regardless of the accuracy of the game model, it could be inferred that the game create a learning moment for this player, and the other participants with which they vocally shared their feelings, regarding a need to reduce barriers to strategic sharing of resources (capital or skills) to ensure effective policymaking in cyber security.

6.2.3 Objectives

As outlined in Section 4.3, Objectives were one of the game components which underwent significant change from conception to final implementation in the game. Throughout this process, however, the purpose of the Objectives as pedagogical instruments remained consistent. The idea was for players to

[470] Author fieldnotes, 6 March 2017
[471] Written player feedback, 15 May 2017
[472] Author fieldnotes, 6 December 2016

understand that in formulating cyber security policy and strategy, they must work backwards from the outcome they want to achieve.

With this in mind, the game appears to have created learning moments along two lines: tactical distractions, and knowledge of the adversary's objectives. Although the realisation of these moments was novel in the cyber context of the game, they are also manifestations of player behaviour observed by other wargamers. The idea of tactical distractions, especially, is not far removed from Frank's concept of 'gamer mode' (referenced in Section 4.3), or what Frey et al called 'meta-gaming', in which players manipulate game systems to win, losing sight of the purpose of the game.[473] While tactical distractions as used here is meant to refer to in-game attention diversions, the final outcome of missing larger objectives still resonates.

Tactical distractions

One theme that emerged in several game sessions was that players lost sight of Objectives because of distractions in the game. One player noted how "in the heat of the moment" their team was more focused on what was happening in the game and how they would react, and Objectives were lost by the wayside.[474] Similarly, feedback from a military player stated that their lesson learned was that "distraction of toys + power means it distracts from original plans [sic]."[475] In this game the UK team had acquired offensive cyber capabilities and decided to launch an all-out attack on Russia, which spectacularly backfired, resulting in the UK knocking itself out. In both cases it is evident that players became enamoured with the tactical action in the game at the expense of the bigger strategic picture. For the military player especially, the learning moment seems to have been a pertinent one: the allure of cyber capabilities may be strong, but they are not necessarily the right tools to achieve desired outcomes. The example can also be viewed as testament to the game's ability to encourage self-reflection among players. By discussing *how* they played the game post hoc, players were able to realise nuances in their decisions and actions which they were not necessarily

[473] Frey et al (2017), p. 6
[474] Author fieldnotes, 18 April 2017
[475] Written player feedback, 15 May 2017

conscious of at the time. Such reflection is a key part of the decision-making experience which makes wargaming a powerful learning tool (discussed further in Section 6.3.2).

Knowledge of the adversary's objectives

In another game session with military players, the researcher observed decision-making processes completely devoid of consideration of the other team's Objectives. Although most of these were hidden, there was also a set of open Objectives visible to everyone. Towards the end of this game, the UK team had a seemingly difficult decision to make between two courses of action, but if they had simply paid attention to one of Russia's open Objectives it would have been clear that only one of the courses of action was appropriate.[476] In the post-game discussion, one player stated that their absolute key takeaway from the game was that you do not know what the other team's Objectives are.[477] This is a reflection of the real world in that publicly stated policies may only be partial guides to how an adversary or competitor is likely to act. The UK National Cyber Security Strategy, for example, leaves retaliatory options open, stating that responses to threats include 'the full range of government capabilities.'[478]

As a learning moment created, a player from a different military session wrote that it is "key to understand hostile cyber security strategy."[479] It is not clear whether this referred to published documents or an understanding based on observation of behaviour (or a combination thereof), but this player evidently thought that closely reading published material or thoroughly analysing an adversary's behaviour would provide some sort of guide to action. Although this may be true to some extent, this message was not deliberately propagated in the game design, because an accurate guide to enemy behaviour requires a much more detailed game model. In this case, the game design therefore introduced scope for an unintended learning moment based on what the game model lacked.

[476] Author fieldnotes, 24 January 2017
[477] Author fieldnotes, 24 January 2017
[478] HM Government (2016), p. 49
[479] Written player feedback, 15 May 2017

6.2.4 Resource management

As discussed in Section 4.3.2, the game was designed to tease out some of the tensions between resources available to a country and their strategic goals. Players were not given enough Resource to achieve all their Objectives, forcing them to make difficult decisions, and the Resource and Vitality concepts in the game were purposefully vaguely defined to encourage debate.

Economic models

Across all game sessions, the most popular discussion topic around Resource management was the inaccuracy of the game's economic model. For example, two players (one military and one civilian, in two different game sessions) remarked on the constant income teams received and suggested options for variable income game mechanics.[480] This would reflect the rise and fall in a country's economy, where industrial output and tax receipts will vary with time and affect the amount of money available to a government. In another game session with a civilian mix of participants it was noted that Rosenergoatom, UK Energy, and UK Plc are all revenue-generating, so Government income should be based on the Vitality of these.[481]

While such discussions held some merit for players to engage with high-level strategic concepts, they were limited in contributing to the learning moments the game design was intended to enable because of the scant relation to cyber security. On the other hand, the examples illustrate how the game was able to elicit unintended learning moments. By presenting players with basic representations of various concepts within resource management, the game encouraged players to apply their own expertise. In imagining more advanced economic models, for example, players critiqued the in-game representation using their knowledge and understanding of the real world. By vocalising the

[480] Author fieldnotes, 24 January 2017; 6 September 2017
[481] Author fieldnotes, 29 June 2017

critique during a game session, the expertise was propagated among the participants, thereby enabling learning moments for all players.

The case of India and Pakistan

The topic of Resource also provided one example of a player being able enlighten the whole participant group with their own knowledge. In a game session with a civilian mix of players from an Indian background, a very lengthy discussion was had about the fact that Russia had bankrupted itself to win the game, which was felt to be unrealistic as a country must continue to function beyond the game scenario. One player, however, interjected that "this is what Pakistan does against India", pouring money into ISI (Pakistan's intelligence service) at the expense of economic development. The player then charted, with gesticulation, China's and India's economic growth since the 1970s, versus Pakistan lagging and actually decreasing.[482] Again, the discussion was not directly relevant to cyber security, but it did begin to address some of the tensions governments face in deciding where to invest their resources, with concrete examples of how certain countries have made these decisions.

More importantly, the example is illustrative of the game providing impetus to learning moments with constructive debate and sharing of knowledge. Pieter Van den Heede et al's study of popular computer war-themed games concluded that, almost invariably, the representations of war in these games was idealised, morally unambiguous, and based on fictional scenarios as real post-1989 conflicts are mostly considered too controversial for commercialisation, thereby potentially reinforcing misconceptions about modern conflict.[483] By contrast, the previous example demonstrates how the game designed for this thesis was a catalyst for rival geopolitical imaginaries and practices, albeit different from the representational politics present in the game (as discussed in Section 4.2.1), prompting players to link game concepts to real-world conflicts. Rather than reinforce misconceptions, as popular computer games might, the game used in

[482] Author fieldnotes, 18 April 2017
[483] Van den Heede et al (2017), pp. 16-17

this thesis created learning moments where players could express their conceptions and share these with other participants.

6.2.5 Attack and defence dynamics

As detailed in Section 4.4, the game design included various components and mechanics intended to convey ideas about cyber attack and defence dynamics. Some specific learning moments are analysed in the following subsections, but it is also worth highlighting two broader themes which emerged across multiple game sessions. Firstly, there was division among players whether the game suggested attack held primacy over defence, or defence could withstand attack. One player, for example, stated that their takeaway from the game was that "it's crucial to have a counterattacking capability,"[484] while another noted that they had learned attack was stronger than defence, although they were able to accurately qualify this with "*if* the game setup is realistic."[485] In both cases, the game result would likely have affected the players' judgement: both were UK victories resulting from UK launching devastating attacks on Rosenergoatom.

Contrary to these views were players who thought defence would prevail. Feedback from one player stated that their lesson learned was about the "strength of defence"[486], while one military player thought there were two main takeaways from the game:

> "1. It is not a question of if, but when an attack will happen – it's a game, so people will *always* Attack.
> 2. How effective it is to invest in defensive measures."[487]

Again, these judgements followed the progress of the game. In the first example, the UK lost the game, but only through a spectacularly unsuccessful Attack – their own defence had withstood multiple Russian Attacks – and in the second example

[484] Author fieldnotes, 20 April 2018
[485] Author fieldnotes, 9 February 2017
[486] Written player feedback, 15 May 2017
[487] Author fieldnotes, 8 May 2017

the UK had recovered from an early near-disaster with a strong defence which stopped Russia from further Attacks.

There were no specific provisions within the game design commenting on the relative strength of attack and defence, only that both of these are important dynamics of cyber security. That players were able to make arguments for either case can therefore be taken as testament to the effectiveness of the game in promoting discussions, and thereby enabling learning moments, around this issue. It is important, however, to recall the warning issued by Dunnigan (as mentioned in Section 2.3.3) that a false prophet is usually only noticeable after it is too late. In the examples mentioned above, two players were able to temper their potential lessons learned with recognition of limitations of the game, but the other two took lessons more directly. With the first player in particular (who noted the importance of a counterattacking capability), the facilitator felt a need to intervene to add more nuance to this takeaway, for example that attribution is not always straightforward and the ethics around targeting CNI. (See Section 6.3 for further examples of wargaming theory applied to the conduct of this research.)

Secondly, Attacking held a very strong allure. As the quote above highlights, the fact that participants were playing a game (a safe environment, as discussed in Section 2.2.7) meant that Attacking was an attractive course of action and observations from other game sessions corroborated this finding. One military player noted, in semi-jest, that "if all you have is a hammer every problem looks like a nail,"[488] while another player, on finding out their team had no attacking remit exasperatedly exclaimed "What, UK can't Attack? That sucks!"[489] Another UK team (played by Australian civilian industry participants), ignoring their lack of offensive remit, reasoned that "attack is the best form of defence" and played aggressively from the outset.[490] Players clearly wanted to go on the offensive but, in most cases, it is unlikely this reflected their real-life aspirations. In one session with UK civil servants, however, the following exchange was observed:

[488] Author fieldnotes, 15 May 2017
[489] Author fieldnotes, 28 April 2017
[490] Author fieldnotes, 7 December 2017

P1: “Why has the UK only got one Attack Vector?”

P2: “Because we play fair.”

P3: “If we play at all…”[491]

The final remark could be interpreted as frustration with UK policy, so a desire for some more offensive latitude in the game may well have reflected a similar real-world desire. Similarly, one German military player complained that if the blue team represented Germany they could not have any Attack Vectors whatsoever and displayed clear frustration at this.[492] Taking the allure of the offensive to the extreme were the UK team of military players who admitted that the primary reason they had purchased the Attack Vector was to deny Russia having it, but figured that once they had it they may as well use it.[493] Despite a host of defensive capabilities available, and Objectives which rewarded defensive strategies, Attacking often proved too hard to resist.

It is noteworthy that these findings run counter to Jacquelyn Schneider’s conclusions from a series of strategic wargames in the US, where participants were largely reluctant to resort to offensive cyber capabilities.[494] However, two caveats temper the comparability of their findings with those of this thesis. Firstly, it is likely the purposes of Schneider’s games were different from the one used in this thesis. Whereas the latter is pedagogical, the former was likely intended to inform policy; this was the purpose of a 2017 wargame conducted by Schneider at the US Naval War College.[495] Secondly, public information about the games referred to by Schneider is limited (with the notable exemption of the previously cited report). It is therefore not known what they represented, how they were set up, or who the players were. Different designs lead to different outcomes – consider Sabin’s probability distributions from Section 6.1.3 – so without knowing the design details it cannot be known if the outcomes are comparable. Optimally, combining analysis from many different types of wargames would yield greater insights, but such an exercise is beyond the scope of this thesis.

[491] Author fieldnotes, 6 December 2016
[492] Author fieldnotes, 24 January 2017
[493] Author fieldnotes, 15 May 2017
[494] Schneider (2018)
[495] Schneider et al (2017), pp. 23-25

Capability development

The game design included a representation of cyber capability development primarily through a Black Market where players could purchase Assets which enhanced their in-game capabilities. Three aspects of this mechanic are noteworthy with regards to creating learning moments. Firstly, one of the most frequently mentioned suggestions for improvements to the game was some sort of representation of internal capability development. Players across the spectrum of military and civilian participants recognised that cyber capability acquisition is not restricted to purchasing tools off the shelf, but that GCHQ, SCS and other intelligence agencies are rapidly developing capabilities of their own. In one session with civilian academic participants, one player was able to link the discussion to the recently-released Vault7 documents on WikiLeaks, which detailed the CIA's efforts in this area.[496] Other players suggested gameplay mechanics which could be used to model internal capability development, including GCHQ investing Resource into a pot and eventually gaining an Asset[497], or a card drawn at random.[498] In all cases, the game fulfilled its purpose of prompting discussion around this important cyber security topic and guided participants in thinking about some of the nuances around it. Although players were not able to engage with these nuances through gameplay (because the game lacked appropriate mechanics) learning moments could still be created through debate and discussion where the game had enabled players to make insightful remarks

Secondly, the Black Market game mechanic created an opportunity for arms races. The Market functioned as an all-pay open auction; the teams could bid Resource on Assets during their turn, then during the subsequent turn the other team could counter-bid with a higher amount, and so forth until one team stopped bidding. In this sense an arms race dynamic could be created whereby the team willing to commit the most Resource would be better equipped in terms

[496] Author fieldnotes, 24 March 2017; Gallagher (2017)
[497] Author fieldnotes, 13 March 2017; 15 May 2017; 29 June 2017; and 6 September 2017
[498] Author fieldnotes, 15 May 2017

of capabilities, but likely at the expense of neglecting other Entities in the game – in real life some, like Robert Strayer[499] or Raymond Boudon[500], have argued this dynamic contributed to the collapse of the Soviet Union. The researcher observed numerous arms races in game sessions, yet the potential learning moments were largely missed. One player, for example, mirthfully noted in a post-game discussion how his team had "forced Russia to spend 19 or 20 Resource on the Attack Vector, but they could never use it because we put defences on all the targets," yet failed to link this comment to any real-world concepts despite the clear presence of both an arms race and deterrence.[501] The only instance of a participant creating a clear learning moment in this area was a military player who wrote that their lesson learned was the "threat to use Black Market led to defender behaviour in the market (threat of race versus actual race)."[502]

Academics like Jarno Limnéll[503] and Anthony Craig[504] have argued that cyber arms races are very real, so it is unfortunate that the game failed to promote more discussion around this topic. This is not necessarily a failure of imagination on the part of the players because emphasis on arms races had been significantly toned down during the game development process (see Section 4.3.1). However, given the importance of the topic, future cyber wargames that include arms race-like mechanics – such as markets for capability development – may want to consider explicitly including this as an educational outcome.

Lastly, one discussion around Black Market Assets resulted in a textbook example of players being enabled to ask the right questions. In a post-game discussion session with German military players, one participant made the following comment:

> P1 [no cyber expertise]: "This game is for decision-makers, yes? I think it's perfect for people who don't know what all these cyber things are to have a way of learning about this. For example, I had not heard of ransomware before but now I

[499] Strayer (1998), p. 80
[500] Boudon (2003), p. 4
[501] Author fieldnotes, 28 April 2017
[502] Written player feedback, 15 May 2017
[503] Limnéll (2016)
[504] Craig and Valeriano (2016)

> can go look it up or ask one of these guys [motioning to two cyber experts sitting adjacent]."[505]

In addition to fulfilling the primary purpose of wargames as tools to help ask the right questions – as defined by Peter Perla (quoted in Section 2.3.3) – the example demonstrates how the game enabled players to seek out 'reducible ignorance' (as stated by Hulse et al, see Section 2.1.2) and set up knowledge-exchange relationships. Ideally, these relationships lasted beyond the confines of the game session, extending the benefits of knowledge-sharing for a longer duration. However, follow-up studies to ascertain whether this is the case are not within the scope of this thesis.

Through the game, players were exposed to concepts they had not encountered before, could identify colleagues who possessed more expertise in these concepts, and knew what questions to ask these colleagues in order to enhance their own knowledge. In the previous case, the player identified ransomware, which was represented by a Black Market Asset, as a gap in their knowledge and could point to the players who would be able to bridge that gap. Therefore, this example is emblematic of the game's capability development mechanics enabling tangible cyber security learning moments.

Attack vectors

Attack Vectors were one of the game components which underwent drastic change as the game design was refined (see Section 4.4.3 for discussion). The final implementation of the Vectors was intended to convey both the constant threat posed by malicious actors and the UK's overtly defensive approach as outlined in the National Cyber Security Strategy. Across all game sessions, two themes emerged as the most prevalently discussed. The first was the lack of UK Attack Vectors at the start of the game. Many players decried this from a gameplay perspective (as previously discussed with regards to the allure of the offense), but some also suggested that the game would be more accurate if the UK had some offensive remit.

[505] Author fieldnotes, 24 January 2017

In a game session with UK military players, for example, no fewer than four participants deemed a UK Attack Vector as a crucial addition to the game.[506] These players, whose professional roles all involved military cyber operations or policy, seemingly brought knowledge of the UK's real-life approach and projected it onto the game model. Whilst certainly validating the game as a tool for spurring thought about an important cyber security topic, it was also a shame that these thoughts were projected into a veritable echo chamber. There were instances in other game sessions where players inquired about UK Attack Vectors – demonstrating the capacity of the game to enable players to ask the right questions – but the facilitator's explanation (following the rationale in Section 4.4.3) was accepted as gospel.[507] On these occasions, the participants' experiences would have been enriched if another player could have presented an alternative view point, challenging the facilitator's perceived authority.

Discussions around UK Attack Vectors created more successful learning moments when they considered intelligence gathering aspects. In two game sessions, both with civilians, players recognised the role of intelligence in establishing and maintaining Attack Vectors. One participant referred to the "persistent spying" which keeps Vectors open, thereby identifying the constant hostile activity in cyberspace the game design intended to convey.[508] In a similar discussion in a different session, one participant with a deeper technical understanding was able to elaborate further, stipulating that UK actions in this area would likely not amount to penetrations of Russian targets, but more probably some sort of scanning efforts to map networks.[509] Discussions like these can be deemed more successful from a pedagogical standpoint, such as that taken by Terence Mahoney or Stephen Downes-Martin (as quoted in Section 5.3), because the players themselves explored the nuances associated with Attack Vectors, rather than the facilitator dictating learning outcomes.

[506] Written player feedback, 15 May 2017
[507] Author fieldnotes, 25 April 2017; 8 May 2017
[508] Author fieldnotes, 6 September 2017
[509] Author fieldnotes, 24 March 2017

The second theme that emerged around Attack Vectors were discussions regarding strategic, legal, and moral limits on the UK's attacking remit. For example, in one game session with military players it was noted that Rosenergoatom would be viewed very differently from something like Rosneft (Russia's electrical distributor, equivalent to National Grid in the UK). Indeed, the laws of war prohibit targeting of civilian nuclear infrastructure but, said one participant, "it's a different question if we're just talking about the lights going off in Moscow."[510] Similarly, one civilian player thought that GCHQ attacking Rosenergoatom would not be "politically justifiable,"[511] while a player from an academic background thought UK companies 'hacking back' would be internationally illegal and amount to an act of war.[512]

Although the latter statement betrays an unrefined understanding of international laws on armed conflict as applied to cyberspace, another player was able to temper the assertion by saying that repercussions for a UK actor being caught on the offensive would be much greater than Russia. This sort of dialogue between players exemplifies the game's capacity to inspire debate and create learning moments around a key cyber security concept. That players recognised the importance of ethics and the rule of law in these matters is significant because it indicates an understanding that cyberspace is not bereft of a rules-based order. Cyberspace is often portrayed as a 'wild west' where laws and regulations have no credence, yet efforts to codify international law, such as the Tallinn Manual, should be recognised as important developments which can hopefully limit aggressive behaviour in cyberspace.[513]

Attack risk and reward

The game design intended to convey the risk and reward payoffs associated with cyber attacks through a combat results table mechanic. The more Resource players committed to an Attack the higher their chances of causing significant damage, but there was also a higher risk of the Attack failing and backfiring. In

[510] Author fieldnotes, 8 May 2017
[511] Author fieldnotes, 29 June 2017
[512] Author fieldnotes, 24 March 2017
[513] Schmitt and Vihul (2017)

most game sessions, players were observed conducting risk assessments on their Attacks, weighing up the costs and benefits. However, very few players seemed conscious of this act and it was not often covered in post-game discussions, meaning the game mechanic was largely unsuccessful at creating learning moments. Intriguingly, teams playing Russia were more likely to heed their own advice from these risk assessments, with the most common Attack strength being three Resource (although this observation is anecdotal, statistics were not collected). Contrarily, UK teams (once they had acquired the ability to Attack) tended to dispense with assessments and launch any Attack they could afford.[514] However, rather than reflect the respective countries' approach to cyber attacks, these dynamics are more a result of the game setup, the teams' Objectives, and the allure of the offense. Overall, the dynamics around attack risk and reward largely represent a missed opportunity for players to have insightful discussions

A more common discussion point arising from the game's risk-reward structure was the role of dice and luck, with some players highlighting that die rolls determined the outcome of the game. On one of these occasions the comments led a useful discussion about whether players would commit to high-risk, high-reward attacks in real life, to which the conclusion was that it all depends on context.[515] On another occasion, a player from a UK civil service background was very sceptical about the amount of randomness which determined the game outcome and did not accept the facilitator's assertion that "war is random." In this instance circumstances had dictated a severely stunted game session (only four turns), which would have increased the impact of die rolls and thereby distorted players' perception of their importance.[516] Notably, the Foreign and Commonwealth Office have also admitted an aversion to dice in gaming, so this may be a trend within the UK civil service.[517] These examples demonstrate some negative connotations of using dice, when players think about its impact too literally and fail to relate the game representation to a real-life concept (positive results of using dice for engagement purposes are analysed in Section 6.3.3).

[514] Author fieldnotes, 8 May 2017
[515] Author fieldnotes, 7 December 2017
[516] Author fieldnotes, 25 April 2017
[517] Elliot (2017)

More useful learning moments were created when players considered less the die itself and more what it represents: luck. Three pieces of written feedback from UK military players are emblematic of the levels of sophistication of questions players might be enabled to ask after playing the game. The first stated that "luck is a factor," the second that "you can't predict luck, but you can account for it," and the third noted the "precariousness *and* resilience of risk management [emphasis in original]."[518] We can see that the first merely recognises the role of luck, the second realises how luck plays into strategy, and the third relates luck to a real-world concept. The third assertion especially demonstrates that player's ability to link specific game mechanics to generic ideas, whereby the uncertainties of die rolls were interpreted to represent that all the risk management and planning a team does can be undone by one unpredictable factor ("precariousness"), and therefore it helps to have backup plans and failsafe strategies in place for these eventualities ("resilience"). It is notable that this level of sophistication was attained by a military player, whose modes of thinking are likely to be attuned to uncertainty of risk. After all, one of the most celebrated axioms of military strategy is Helmut von Moltke's (paraphrased) assertion that 'no plan survives contact with the enemy.'[519] The game can therefore be considered successful in eliciting a learning moment derived from this axiom, but unfortunately only for a very limited audience.

Attribution

Dynamics of attributing cyber attacks were represented in the game through the permanent Attack Vectors (a deliberately inaccurate portrayal of attribution as a certainty) and in the Attack mechanics where a failed Attack would result in additional effects for being attributed. These were the source of insightful debates among players, some of whom recognised the nuances around attribution and how the game's representation related to real-world concepts. In one session with military players, for example, an observer asked the UK team if their strategy or decisions had been influenced by "macro-level attribution" – the fact that they knew their opponent was Russia. Although no clear answer was

[518] Written player feedback, 15 May 2017
[519] Hughes (1993), p. 92

given, this instigated a discussion about how the game would be different if played blind, perhaps with a divider between the teams or in isolation from each other (see Section 6.2.7 for further analysis of visibility). There was also a suggestion to simply label the teams 'A' and 'B' to perhaps neutralise some of the prejudices which might taint gameplay when the teams have real-life identities, but this seemed unpopular because real-life actors were more engaging.[520]

As a learning moment, this example illustrates how the game's attribution mechanisms could be successful in terms of enabling players to explore aspects of anonymity in cyberspace. Understanding the dynamics of anonymity and attribution is important because many offensive cyber operations have been conducted under the auspices that attribution is difficult. When they know they can get away with it, criminals and other actors become more brazen in their actions. Thomas Rid has postulated that Russian covert action in 2017 and 2018 was used to test red lines and Western resolve.[521] The willingness of both the UK and US to publicly attribute certain operations to Russia, for example the NotPetya cyber attack, has subsequently demonstrated the limits to which Russia can operate anonymously.[522]

In other sessions, discussions concerned attribution at lower tactical and technical 'micro' levels. One civilian industry participant pointed out that the game does not account for Russian use of "proxy forces": in real life Russia could sidestep the attribution mechanism by getting someone else to launch Attacks on their behalf.[523] In a different civilian session one player, who overtly identified with the political left, related in-game Online Trolls attacks to "Blairites" hiring trolls but no one able to trace the money used to pay for them. Two other players built on this by discussing both the ease and difficulty of tracing Internet Protocol (IP) addresses to physical locations. In order to further enhance this particular learning moment, the facilitator also injected points about the difference between technical and political attribution, and that knowing where a computer is

[520] Author fieldnotes, 15 May 2017
[521] Rid (2018)
[522] National Cyber Security Centre (2018)
[523] Author fieldnotes, 6 March 2017

does not necessarily identify the person behind the keyboard.[524] These examples demonstrate how the game prompted exploration of topics which were not explicitly contained in the game itself, but to which players could contribute their own knowledge and understanding, thereby following the observation made by Peter Perla and Ed McGrady that 'great games capture meanings which have never been said' (quoted in Section 2.2.4). By designing deliberately provocative attribution mechanics, the game thereby successfully promoted learning moments around this topic.

Deterrence

Deterrence is a central facet of the UK National Cyber Security Strategy[525], but this concept was not overtly designed into the game as an educational point, largely due to the researcher's own scepticism of cyber deterrence.[526] Nonetheless, deterrent gameplay was observed by the researcher, for example in one game where the UK team piled Resource and Vitality into potential targets, effectively stopping Russia from Attacking them. However, despite the researcher expressing this observation to players, in this instance discussion did not progress further and the learning moment was not realised.[527] German military participants playing a UK team, on the other hand, were able to recognise when they were deterring the other team and consciously employed this strategy to limit Russian attacks.[528] In the post-game discussions a player from the opposing Russian team summarised the game and explicitly included deterrence, which they had perceived as UK opening the GCHQ-Rosenergoatom Attack Vector, forcing Russia to spend Resource to gain Vitality in this Entity.[529] Their experience with the game led one of the players to conclude that the UK is well-placed to achieve the objectives outlined in the National Cyber Security Strategy, including deterrence, because they had successfully done this in the game.[530] The researcher's impression of this group of players suggests that they were aware that the game is not intended as a

[524] Author fieldnotes, 6 September 2017
[525] HM Government (2016), pp. 46-52
[526] For further information, see Haggman (2018)
[527] Author fieldnotes, 28 April 2017
[528] Author fieldnotes, 24 January 2017
[529] Author fieldnotes, 24 January 2017
[530] Author fieldnotes, 24 January 2017

simulation, so this assertion was likely not achieved solely based on the game model, but the player's wider understanding of cyber security and the strategic landscape.

In another game session with civilian industry players, one participant recognised that UK investing in Education had deterred Russia from Attacking the Electorate (the Education Black Market Asset caused any Attacks on Electorate to inflict only half damage). Moreover, the player felt that this was a realistic depiction of how a more cyber security-aware populace can limit the disruptive or destructive capacity of malicious actors, and that it sent a good message to players about the value of education.[531] This was precisely what the Education Asset had been designed to convey, and in this instance, it was conveyed in the context of deterrence, thereby enabling two learning moments simultaneously.

Overall, despite not explicitly designing deterrence into the game, the fact that players were able to recognise and discuss this concept is testament to the game's flexibility as a cyber security learning tool.

Passwords

The importance of strong passwords is a mantra frequently touted as one of the simplest cyber security defences anyone can implement. However, because passwords are a very low-level concept it makes no appearance in the game – notice that it is not mentioned once in Chapter 4. Despite this, one UK civil service player participating in a mixed session was determined to discuss this topic, almost at the expense of everything else.[532] The game session took place shortly after the National Cyber Security Centre had updated its public advice on passwords, changing its recommendation from forcing regular password changes to instead monitoring logins and notifying users of attempted logins, so it is likely the player had recently been exposed to this advice.[533] This was the only recorded instance of passwords being mentioned by participants, but the example does

[531] Author fieldnotes, 6 March 2017
[532] Author fieldnotes, 6 October 2016
[533] National Cyber Security Centre (2016)

illustrate the game's capacity to create learning moments where players could contribute their own knowledge about cyber security topics, even when they had no representation in the game.

While the game represents strategic level cyber security, the example illustrates that learning moments could be achieved even at very tactical levels, in this case about an important defensive concept.

6.2.6 Geopolitical realities and landscapes

As detailed in Section 4.5, the game contained a deck of Event Cards which were drawn randomly to represent unpredictable events to which the players would have to react. The pedagogical reasoning behind this game mechanic was to introduce to players the idea that geopolitical realities, moods, and circumstances can impact cyber security agendas, even if an event does not immediately seem cyber-related.

Effectiveness of Event Cards

Intriguingly, there was some division among players as to the efficacy of the Cards. One military player suggested the Cards were a candidate for removal from the game, questioning whether "they add learning points beyond planning for random acts."[534] This comment is somewhat surprising because the Event Cards are one of the components which could be said to have the most thematic cyber security content, directly simulating real-life events which players would likely be aware of (for example civil servants misplacing laptops). Additionally, the "learning point" of planning for random acts is a crucial one and it seems odd to dismiss it. Other players were more positive, praising the Event Cards (in addition to the Black Market Assets) as the best source of learning and education in the game.[535] The military player's negative comment was the only one of its kind recorded, so can likely be viewed as an anomalous outlier. Furthermore, if we

[534] Written player feedback, 15 May 2017
[535] Author fieldnotes, 6 October 2016; 9 February 2017

accept that players did indeed find the Event Cards useful for education, they perhaps represent a missed opportunity to create further learning moments, because there was no guarantee that all the Cards would be seen by players in a game session (there were 16 Cards but only 12 game turns).

Given players' general approval of the Event Cards, a future version of the game might therefore place greater emphasis on these prevailing geopolitical realities and how players should deal with their effects in cyberspace. At the same time, the scepticism shown by one player indicates that there is scope for improvement of this game mechanic. In particular, questions about what might be seen as realistic or likely geopolitical realities need to be answered in order to ensure relevance and acceptance of the Cards.

Impact of quantum computing

One Event Card which created multiple learning moments was the Quantum Breakthrough card, which posited that Google rolled out quantum computing across all its devices and services, granting all Entities in the game one additional Resource and Vitality. In discussion, some players questioned whether quantum computing really was a benefit for society, as the Card entailed, and voiced concerns about negative consequences. One player from a mathematics background, for example, was able to talk about how quantum computing undermines many of the assumptions that enable modern cryptographic technologies.[536] Other participants in this session, who may not have been familiar with concepts such as Shor's Algorithm (discussed in Section 4.5.4), could therefore be said to have experience a learning moment where they were introduced to this idea. That players were able to highlight the inaccuracies of a game component and explain why reality might be different vindicates the design approach behind the game; learning moments could be achieved, in this case about quantum computing, by players discussing the game's representation of this topic.

[536] Author fieldnotes, 9 February 2017

President Donald Trump

The geopolitical reality which most frequently created learning moments was President Donald Trump. Multiple suggestions were made by players to add Trump to the game as an Event Card; often these suggestions had a humorous edge but were based on serious concerns about Trump's ongoing geopolitical impact.[537] In one game session, for example, a player jokingly asked where Trump was, to which another player responded "right here," pointing to the middle of the red Russia triangle on the game board.[538] In another session one player remarked that a "Trump Tweets" card was a "glaring omission", with another player suggesting "Trump misspells Prime Minister's name" as a candidate.[539] The frequency with which Trump was mentioned indicates that players considered his presidency an exceptionally notable event, but seldom did discussion progress beyond repetition of popular tropes (such as Trump's purported association with Russia or his social media habits) without deeper analysis. Learning moments around this topic were therefore more about recognition that the election of President Trump is an important event, but less about why it is important and its longer-term implications.

6.2.7 Visibility in and of cyberspace

In conflict results are not only unpredictable (as simulated by the game's use of dice), but decisions are often made based on incomplete information. The idea that policy- and decision-makers do not have complete visibility of a situation was designed into the game through hidden player Objectives and secret cyber capabilities (Black Market Assets). However, players did have a very good view of the operating environment in that the game board itself was entirely visible with perfect information (for example, if the players could see a number of counters on the board, this was a true representation of the number of counters available).

[537] Author fieldnotes, 6 March 2017; 7 December 2017
[538] Author fieldnotes, 30 March 2017
[539] Author fieldnotes, 29 June 2017

Transparency and openness

On numerous occasions learning moments were created where players recognised the representation of visibility in the game, especially the complete visibility of the game board, which was often highlighted as an inaccuracy.[540] Players from both military and civilian backgrounds were cognisant that cyberspace is a particularly opaque environment and could elaborate on the shortcomings of the game's model, especially the game board, in this regard. In one game session, however, players defended the game's representation of visibility in that real-life UK strategy is very transparent. One player specifically noted that the UK Government is subject to Freedom of Information requests which are prone to reveal more than what has previously been published on a given issue.[541] Where the game falls short is that it applies the same logic to Russia, whereas in real life the Russian Government lags behind the UK in openness and transparency. Despite its inaccuracies, the game model can be lauded for promoting frequent debate about visibility in cyberspace, thereby creating learning moments about this topic. These moments were strengthened when players could link the broader concept to specific policies (such as Freedom of Information), potentially informing players' understanding about the trade-offs facing an open, liberal democratic society.

Deception

Deception is a classic concept where an actor attempts to make an adversary believe they are doing something different to what they actually are, and it appeared as a theme in multiple game discussions. One player, for example, was keen to establish before the game began whether the information they could perceive was correct – if an Entity had a certain amount of Resource on the game board this represented the actual amount available to them.[542] The player's concern about hidden Resource can be used to build on the point about

[540] Author fieldnotes, November 2016; 24 January 2017; 6 March 2017
[541] Author fieldnotes, 29 June 2017
[542] Author fieldnotes, 29 June 2017

transparency trade-offs, because an open society like the UK could be considered handicapped in how far it can exercise deception. The secrecy required for successful deception may be incompatible with policies of transparency. For instance, the UK Government would find it more difficult to conceal economic factors which enable or hinder its ability to act, compared to the Russian Government (who have allegedly tampered with their Gross Domestic Product figures).[543] The game model did not enable such strategic deception, but most players seemed aware of this shortcoming and its implications, as reflected in comments about visibility.

Other players were able to discuss deception at a tactical level. One participant from the Swedish civil service suggested a modified combat results table where players could spend Resource to hide Attacks.[544] A UK military player looked at the issue from the defender's side, suggesting secret use of the Black Market so that the defender could acquire Assets that would only become known to the attacker once they Attacked.[545] Both these points reveal a sophisticated understanding of cyber attack and defence dynamics, highlighting how cyber security is a constant hostile process of attackers and defenders trying to hide their capabilities while discovering the other's.

The game model was clearly effective in prompting players to think about these dynamics of deception, thereby creating learning moments in this area in at least two game sessions.

Secret moves

A final component of visibility which was frequently discussed by players was the idea of secret moves. The game design enabled both teams to see each other's actions and they were therefore able more proactively adapt to the other team. In one session, for example, the teams noted that many of their actions were based on predicting what the other team had enough Resources to do (for example

[543] Ingraham (2018)
[544] Author fieldnotes, 9 February 2017
[545] Written player feedback, 15 May 2017

bidding on the Black Market), and the Russia team stated that they would not have concentrated their Attacks on the Electorate if they could not see that UK Plc were defended.[546] The learning moment here echoes the one from deception, in that players recognised that in real life an attacker may not be aware of defences until they come up against said defences. Similar discussion points were also brought up in other sessions, with suggested remedies including confidential turns[547] or simultaneously resolved moves.[548] Although either of these approaches would create a more realistic game model, they would also add overhead and complexity (see Section 4.4.1 for further analysis).

Ultimately, the design aim stated in Section 4.6 of forcing players to make decisions amid a Clausewitzian fog of war was not realised. By virtue of its openness, the game design was unable to generate sufficient stress and confusion to emulate the experience of making decisions with incomplete, inaccurate, and contradictory information. However, in terms of creating learning moments, the game design enabled players to recognise the limitations of the game's open moves and discuss why actions in cyberspace are made with less visibility. Therefore, dynamics around visibility serve as examples of the game enabling players to contribute their own knowledge and understanding to enhance the learning experience for all participants.

This is the final learning moment theme analysed in this chapter and discussion now moves on to how theories of wargaming were realised during the practice of the thesis.

6.3 Practicing wargaming theory

Previous chapters have analysed some of the theory which underpins both wargame design and use. Much of this theory is based on practice, but very little of the foundational theory – largely laid by Perla and Dunnigan (as frequently referenced in Chapter 2), or even modern scholars such as Sabin – is based on

[546] Author fieldnotes, 29 June 2017
[547] Written player feedback, 15 May 2017
[548] Author fieldnotes, 21 April 2016

cyber wargaming, partly because cyber security is a nascent field, and partly because of the dearth of cyber wargames (described in Chapter 3).

This thesis therefore presents an opportunity to assess the applicability of wargaming theory to the practice of cyber wargaming. Although the confines of the research prevent any wide generalisation beyond the experience of the researcher, future cyber wargaming practitioners may compare their experiences and future work could attempt to amalgamate these into a more profound contribution to the field. Such contributions might perhaps ascertain whether cyber wargaming is a fundamentally different challenge than other topics from a practical perspective (many differences with regards to design were discussed in Chapter 4).

The following sections highlight four theoretical aspects widely recognised in wargaming literature, taken from Chapters II and V, and how these materialised in the practice of wargaming for this research: realism versus complexity, human decision-making, the engagement value of games, and the benefits of using manual games.

6.3.1 Realism versus complexity

A game designer's difficulty in balancing the realism (accuracy) of a game with its complexity (playability) was discussed in Section 4.1. In the game used for this thesis, player engagement with the thematic content was valued above the realism of the game model. More particularly, the issue manifested itself in the length of the game rules, which were considered a potential barrier to engagement and therefore kept to a maximum length of one double-sided A4 sheet. Often game sessions included discussions around this topic and several players recognised the trade-off between realism and complexity.[549] Most often this was well-accepted, and players seemed supportive of the decision to limit the rule length. One player, who had some wargaming experience, suggested two rule sets could be produced: a simple version for lay players (the current two pages),

[549] Author fieldnotes, 24 January 2017; 6 March 2017

and an advanced version for more expert players (up to eight pages).[550] Whilst certainly compelling in terms of future developments, such an implementation falls outside the scope of this thesis.

Despite efforts to keep the game rules short and relatively simple, many instances of friction between the players and the rules were observed. Usually this was confined to the beginning of a game session; most of the time, within two or three turns most players had grasped the intricacies, or at least the basics, of the rules.[551] Clarification questions which appeared frequently included the possibility of moving Vitality, converting Vitality into Resource, or transferring Resource to multiple Entities. Occasionally these resulted in opportunities for discussion (the researcher liked to joke that converting Vitality to Resource might represent people selling their kidneys), but no learning moments were recorded as created in this way. In one game session the rule sheets had been distributed the day before (along with player dossiers), giving participants overnight to absorb the rules. However, when the facilitator explained the rules the following day, ostensibly just to reinforce what the participants should already have known, it became apparent that for most it was their first time hearing them. Only one player claimed to have read the rules beforehand, but also confessed that the facilitator's explanation had been helpful because the rule sheet on its own, without the various game components laid out at hand, had been confusing.[552] This suggests that there is both scope and requirement to further simplify the game design and rule set given a target audience of non-specialist participants; or that players are reluctant to engage with game material until they are in a game session, unless they already have an interest in games or wargaming.

The tension between realism and complexity can therefore be said to have been prevalent during both the game design and deployment phases of this research. Although the rules for the game were not very long by wargaming standards, they were sufficiently complicated to create moments of friction with many players. This may partly be a result of the rules being too complex for the target audience but could also reflect the designer's inexperience in writing rule sets. Jim

[550] Author fieldnotes, 29 June 2017
[551] Author fieldnotes, 6 December 2016; 18 April 2017; 7 December 2018
[552] Author fieldnotes, 28 April 2017

Wallman, an experienced wargame designer, has written about the ease of writing rules, yet simultaneously reported other designers' frustrations with the process.[553] Practical experience suggests that expressing game mechanics in simple terms is a profound challenge which should not be underestimated.

6.3.2 Decision-making experience

As elaborated in Chapter 2, particularly Section 2.2.5, one of the key benefits propounded in wargaming literature is that games enable players to actively make decisions. Rather than have a scenario relayed to them, players progress the scenario through their own actions, providing what Perla and McGrady called a 'story-living' experience (cited in Section 2.2.5) richer than other learning methods. Although the game designed for this thesis did not contain a narrative scenario, teams still had to progress the game by making decisions about which Objectives they would pursue and how to allocate and spend their Resource.

The game rules stipulated that teams were limited to three minutes per turn. This was partly to ensure the game could fit into a two-hour time slot, but also forced players to make decisions under pressure (any Actions not performed within the time limit were forfeit). It is noteworthy that as a general trend, teams playing UK far more frequently pushed the time limit than teams playing Russia. The researcher often observed what might be termed 'analysis paralysis' in teams who sought to evaluate every possible permutation.[554] One German military participant, who had played as Russia, remarked in post-game discussions that they certainly felt like they were playing against a democracy because UK's decision processes were so long.[555] Another player in the same session pointed out that UK have more Transfer options so naturally take longer to make decisions.[556] This can be seen as an accurate reflection of real life, where the UK's governance mechanisms are more decentralised than Russia's, and the economy is more diversified. The game's ability to replicate these dynamics should be

[553] Wallman (2007), p. 11
[554] Author fieldnotes, 6 December 2016; 30 March 2017; 29 June 2017
[555] Author fieldnotes, 24 January 2017
[556] Author fieldnotes, 24 January 2017

considered a success in terms of giving players a story-living experience where they could step into the shoes of a policymaker (on either side) and experience decision-making from their point of view, albeit an experience which can vary in scope and tone depending on the background of the players.

6.3.3 Engagement

An extension of the story-living experience is that wargames are a high-engagement activity. Because they require active participation and immersion rather than passive attention, games engender a higher level of engagement than other pedagogic methods such as traditional classroom teaching, educational videos, or online training modules.

Over the course of this research, the game's qualities could be analysed with reference to the role of emotion, roleplay, fun, and 'distractions'; themes which are prevalent in wargaming literature. The ability of games to 'challenge the competitive spirit,' as Hausrath wrote (cited in Section 2.2.4), refers to the presence of emotion during wargaming. The dangers of distractions, meanwhile, were alluded to both in the Boeing game report and by Wilhelmson and Svensson (cited in Section 5.4.2) who consider the possibility of evaluators disturbing games. The idea that wargames should be fun has a contentious status in professional wargaming. Graham Longley-Brown, for instance, has emphasised the fun qualities of gaming as critical to player engagement.[557] On the other hand, Stephen Downes-Martin has decried such a focus on enjoyment and instead promoted 'professionally satisfying and constructive' as the primary requirements of a wargame.[558] The analysis conducted in the following sections builds on this existing literature by supplementing the practical experience of conducting the research for this thesis.

[557] Longley-Brown (2015)
[558] Downes-Martin (2015), p. 8

The emotive power of dice

The game's use of dice changed during game development. As detailed in Section 4.4.4, feedback from an experienced wargamer resulted in adoption of a regular six-sided die rather than a four-side one and combat mechanics that rewarded high rather than low rolls. These changes were made to align the game with existing norms in board gaming and minimise friction for players unfamiliar with specialised wargaming approaches (such as irregular dice). Observations of player reactions to die rolls certainly suggests that the implementation of dice in the game was successful at eliciting emotional investment. Outbursts for successful rolls, and equally dejected reactions to unsuccessful ones, were observed in almost every game session, with some participants particularly emotive.[559]

The photograph in Figure 15 captures one die-rolling moment from a public game session run by the researcher. The player on the right (the roller) has drawn attention to the die rolling action with an exaggerated hand motion, signalling the significance of the roll. The player on the left, meanwhile, awaits the result with anticipation; the hands placed together could be interpreted as an unconscious prayer motion. It is here worth recalling Baumeister et al's insight about the power of anticipating emotion (Section 2.1.2).

[559] Author fieldnotes, 25 April 2017; 28 April 2018

Figure 15: A rolling moment, showcasing the emotive power of dice. (Image credit: NATO CCDCOE. Image source: CyCon Flickr (https://www.flickr.com/photos/133800821@N02/albums/72157697650970535). Image in public domain.)

These reactions were enhanced when rolls were potentially game-winning or game-losing. One session with UK military players was remarkable for the intensity of reactions, with the final die roll (a UK Attack rolling 1, resulting in UK Government knocking itself out) producing a very loud combination of jubilant hollers and despondent groans.[560] A still photograph could not do this dynamic justice, so the reader is instead recommended to view a promotional video of a game session which captured a similarly dramatic (though more muted) reaction, which can be accessed online.[561]

The physicality of the game should not be underestimated as a factor in eliciting these emotive responses. As argued by Marcus Carter et al, the material feel of the die and the sound it makes as it hits the board provide sensory feedback to players, both the roller and others around the table.[562] Indeed, given that such experiences are mostly lost in digital environments, many computer games incorporate sound effects of rolling dice, prompting players to recall the physical and emotional sensations attached to this action. In an online discussion

[560] Author fieldnotes, 15 May 2017
[561] Information Security Group (2017), the moment in question is around the 06:40 mark
[562] Carter et al (2014), pp. 18-21

regarding development of the virtual tabletop Fantasy Grounds, forum poster Aesir affirmed that 'the missing sounds from dice rolling is currently the only real thing I happen to notice.'[563] The act of rolling dice is entwined with the materiality of the object, and this aspect should not be discounted as a contributor to game engagement.

Roleplay and the suspension of disbelief

The final version of game was designed so that in-game teams had real-life identities (UK and Russia), rather than the anonymous blue and red teams of early game versions. This design decision paid dividends in terms of players identifying with the Entities represented in the game, often resulting in moments of roleplay. Russian characters in particular made frequent appearances. One player spoke of sending ineffective teammates to Gulags[564], while another awarded "medals to everyone" after a successful attack.[565] One player encouraged the Russia team to adopt an offensive mindset, saying "go on, be Putin." Later in the game this team considered 'turtling' for the Victory Points but decided this would be uncharacteristic so remained on the offensive.[566] One UK team complained that "they've got some radio frequency manipulator targeting your [facilitator's] watch," when the Russia team took too long during their turn[567], and a team of military players remarked that they "need some fur hats" to complete the Russian image.[568] Taking this roleplaying to the extreme was the civilian industry player who turned up in a full Russian military uniform costume, saying that he also had a British one but decided beforehand he wanted to play Russia. Multiple jokes from other players suggested a vodka bottle would have completed the picture.[569]

There was also some roleplaying on UK teams. One team complained about the leadership of their "Theresa May" (incidentally the only female player on that

[563] Aesir (2005)
[564] Author fieldnotes, 24 March 2017
[565] Author fieldnotes, 8 May 2017
[566] Author fieldnotes, 6 March 2017
[567] Author fieldnotes, 30 march 2017
[568] Author fieldnotes, 13 March 2017
[569] Author fieldnotes, 7 December 2017

team had ended up in the Government role).[570] In another game session the player taking control of UK Energy returned from the game after a short absence, only to discover their team had lost and the company was broken. Upon hearing this they exclaimed "Oh I don't care, I just want to know if I still have my pension."[571] Not only does this demonstrate that the player was able to identify with the character they had been assigned, but that they understood prevailing corporate attitudes to cyber security. Often the repercussions of a cyber security breach, in terms of lack of significant negative effect on companies' stock prices, means the problem has not been taken seriously.[572] The game successfully encouraged the participant to express this view in a roleplayed character which had strong resemblance to real life.

The participants who engaged in roleplaying can be described as achieving a 'suspension of disbelief' – the audience's 'tolerance of the fictionality of the media content.'[573] The game adheres to Eve Schaper's definition of a fiction where suspension of disbelief can take place: 'any works…in connection with which it makes sense to speak of characters appearing and events taking place in them.'[574] The game itself did not present individual characters, only amorphous Entities, yet players were keen to both identify and identify *with* important individuals such as Vladimir Putin and Theresa May.

Roleplaying in this way is a suspension of disbelief because the players were both willing and able to look past the game's shortcomings – both the representations made therein and its form as a board game – to engage with its thematic content.

Fun and entertainment and their role in pedagogy

Finally, comments and feedback from many players emphasised the fun and entertaining qualities of the game. When asked about their thoughts about the game, "fun" was the word which first sprung to mind among participants from the

[570] Author fieldnotes, 24 March 2017
[571] Author fieldnotes, 25 April 2017
[572] Jones (2016), p. 18; Wilcox (2017)
[573] Böcking (2008)
[574] Schaper (1978), p. 31

UK military[575] and Australian civilian industry[576], while one UK civilian academic stressed how they "really, *really*" enjoyed it [speaker's emphasis][577], and another UK civilian stated that "it really felt like a game" (in that they were actually playing against an opponent).[578] What can be judged as a more nuanced comment was made by a German military player, who thought the game had limited value in teaching cyber security, but emphasised the element of fun as key to making it a good general education tool.[579] In defence of the game's cyber security pedagogic potential, it should be noted that this player was already a cyber security expert so it is understandable why they derived limited learning moments from the cyber security content.

By way of illustrating these dynamics, Figure 16 captures participants in the middle of having fun; the players on the far right and far left are executing some gameplay action, while the two in the middle have shared some humorous observation with the other team. Everyone can be seen laughing and engaged with the game.

[575] Author fieldnotes, 13 March 2017
[576] Author fieldnotes, 7 December 2017
[577] Author fieldnotes, 24 March 2017
[578] Author fieldnotes, 6 September 2017
[579] Author fieldnotes, 24 January 2017

Figure 16: The fun and entertaining qualities of the game embodied in players. (Image credit: NATO CCDCOE. Image source: CyCon Flickr (https://www.flickr.com/photos/133800821@N02/albums/72157697650970535). Image in public domain.)

Perhaps the strongest indicators of the ability of the game to impress and captivate participants were when sceptics became adherents. As an emblematic example, consider the cyber security expert player who admitted that "at first I was like 'what the hell is this?' but after three turns I was like 'hell yeah, let's do this!'"[580] Some players may have initially doubted the value of a board game covering an inherently digital subject (also see Section 6.3.4), but the barriers to participation were lowered once they were exposed to the game's mechanics and drawn into its engaging qualities. The following exchange serves as a final testament to the overall capacity of the game to elicit enjoyment:

> Facilitator: [Wrapping up discussion] "Is there anything else outstanding?"
>
> P1: "The only thing outstanding here is this game."[581]

From a pedagogical perspective, the reactions, roleplay, fun, and entertainment indicate an emotional investment which can be capitalised on when eliciting learning outcomes. Although players' experience with the game does not quite adhere to what Jan Packer calls 'learning for fun' (valuing learning for its own

[580] Author fieldnotes, 29 May 2018
[581] Author fieldnotes, 29 June 2017

sake)[582], other academics such as Dan Rea et al have contested that fun 'provides opportunities for greater learning satisfaction and success.'[583] If participants feel connected to the activity they are more liable to positively receive the lessons contained therein.

A notable dissenting opinion on this matter comes from Erling Dastool who avers that fun 'has very little to do with deeper student satisfaction, or with real learning.'[584] Dastool's objections, however, are based largely on their own anecdotal observations, whereas later contributions to the field follow more thorough methodological approaches (such as Packer's use of surveys). It has also been recognised that 'fun' is a term fraught with contradictions. Marc Prensky notes a 'major duality' in the division between fun as amusement or ridicule and fun as enjoyment or pleasure.[585] Whereas the former is frivolous, the latter can be associated with serious activities, including pedagogy. Dastool infers that 'fun' mostly carries connotations of entertainment, but there is greater academic support for the view that fun can be harnessed to create engaging educational experiences.[586]

As a summative reference on this issue, Bob Stramba and Christian Bisson state that 'studies have demonstrated that using more engaging and experiential instruction strategies is yielding greater academic success and higher student satisfaction.'[587] Prensky, citing Ellen Langer, adds that active participation from students results in greater engagement and retention.[588] Although this thesis does not include measurement of the viscosity of learning outcomes achieved (such as longitudinal study of lessons learned), the high engagement value produced by the game lays the foundations for strong pedagogic retention.

[582] Packer (2006), p. 341
[583] Rea et al (2000), p. 24
[584] Daastol (1995), p. 15
[585] Prensky (2002), p. 7
[586] See Bisson and Luckner (1996)
[587] Stremba and Bisson (2009), p. 11
[588] Langer, Ellen J. (1997), *The Power of Mindful Learning* (Perseus Books: Cambridge) in Prensky (2002), p. 9

Distractions and failure to engage

Just as the best games achieve a 'suspension of disbelief', so it could be said that they also achieve suspension of belief – a temporary disconnect from reality and full immersion in the game world. In the interest of a balanced assessment, it should be recognised that the game was not always successful in engaging players to the extent of such a suspension of belief. On multiple occasions players were observed interacting with their smartphones, suggesting that the game was unsuccessful in distracting players from the reality of their job roles.[589] A more serious charge would be to claim that these players were bored, directly contradicting earlier assertions about the game's fun and entertaining qualities. Thankfully these moments were outnumbered by examples of high engagement, so on balance the game's fun factor can be adjudged as a positive element.

In other instances, distractions were directly disruptive to game proceedings. In a session with Indian participants, one player interrupted the game to announce "for all the Indians in the room" the just-broken news that a high-profile Indian had just been arrested in London.[590] In the same session, the 2017 UK 'snap election' was announced, and consequently the post-game discussions revolved largely around election wargames, which was off-topic from cyber security.[591] These examples demonstrate how real-world events can impinge on the game and cause players to lose focus. In another session, one non-participant twice came to observe the game, but instead of offering anything constructive waved their hands over the game board distractingly in a juvenile manner (possibly inebriated – the game was played in a bar).[592] Instead of real-world events providing mental distractions, here the real world provided a very direct physical distraction, although it could be argued that this is an added degree of realism – distractions of this nature arise in the real world. The solution to both these problems would be to isolate the game environment to minimise distractions, but in the course of this research the environment could not always be controlled in

[589] Author fieldnotes, 13 March 2017; 24 March 2017; 30 March 2017
[590] Author fieldnotes, 18 April 2017
[591] Author fieldnotes, 18 April 2017
[592] Author fieldnotes, 25 April 2017

this way, indeed it was rarely possible for the researcher to decide where a game took place (see Section 7.1.2 for further discussion).

6.3.4 Manual wargaming and advantages over computers

The benefits of using manual wargames over computerised games were lauded in Section 2.2.1, also justifying the decision to use a manual game for this research. Nonetheless, a popular point of inquiry from players directed at the researcher was why the game was not a computer game.[593] The frequency with which this question appeared suggests one of, or a combination of, three things: the cyber security subject matter was most associated with digital media and a board game was therefore not an intuitive method to interact with the subject (see Section 2.3.1 for related discussion of medium and fidelity); the advantages of manual games were not widely understood; or computer games contemporarily enjoy greater popularity than board games. Unfortunately, this thesis does not offer scope to interrogate which of these are true, other than to remark on the noteworthiness of the issue.

Sometimes discussions around a computerised version of the game took on more nuance. In one session, for example, the player who had originally asked the question was convinced by the facilitator's explanation and suggested a touchscreen table would be a great hybrid solution.[594] Some of the literature referenced in Section 2.3.3 also analyses such devices, and they may present future potential, but are currently prohibitively expensive (compared to personal computers or tablets).[595] In another session one of the players (a seasoned civilian wargamer) was able to field the question, outlining the advantages and disadvantages with computerised games.[596] This is another demonstration of players setting up temporary knowledge exchange relationships, though in this case the pedagogical outcomes concerned wargaming rather than cyber security.

[593] Author fieldnotes, 28 April 2017
[594] Author fieldnotes, 30 March 2017
[595] In the region of $10,000-$12,000 according to Paul Ridden (2013)
[596] Author fieldnotes, 6 September 2017

Intriguingly, but perhaps unsurprisingly, when computer scientists asked questions about computer games they also offered potential technical solutions. On two occasions, implementations of Monte Carlo simulations were suggested to attempt to find an optimal strategy to the game.[597] Although there is certainly value in such an approach (wargaming as operations research or systems analysis, as mentioned in Section 2.1), the suggestions also betray a naivety about the purpose of the game as designed for this research; the purpose was never to find answers, only enable players to ask questions. The person who took this initiative the furthest was an academic at Heriot-Watt University who placed computerisation of the game on their list of potential computer science MSc projects.[598] In this case the academic did understand the purpose of the game and only wanted a pure digital conversion, maintaining the original design principles and enhancing them with digital technology. In the end no student elected to pursue the project, so it will remain unknown whether the conversion would have been successful.

Modifiability

As discussed in Section 2.2.1, one specific advantage manual wargames offer over computerised games are their modifiability. Manual games can be modified a lot more easily in that they do not require any technical skills to edit, and changes can be made even during the progress of a game. Because of this accessible modifiability, players' wisdom can find its way into games – in wargaming parlance referred to as 'wizard wheezes.'[599] Wizard wheezes were successfully implemented on numerous occasions during the course of this research. Sometimes a game might finish earlier than anticipated when one team was knocked out; but players wished to keep going, so a justification was invented why the failing Entity could be granted some Vitality and the game could continue.[600] As long as the justification was realistic and reasonable the facilitator

[597] Author fieldnotes, 25 April 2017
[598] Draft specification at http://www.macs.hw.ac.uk/~hwloidl/MScProjects/MScCyberSecurityGame.html
[599] Phrase used in Past Perspectives (2016), p. 2 and Stone Paper Scissors (2018), p. 5
[600] Author fieldnotes, 6 October 2016

would allow it. This is similar to de Koven's advice that ability and willingness to modify a game can be crucial to keeping the game going (Section 2.1.4).

More advanced wizard wheezes occurred on two occasions when players suggested Event Cards which could be added. One, from a German military player, suggested that Energetic Bear control the Black Market for one turn, receiving all proceeds from bidding.[601] The other, from a UK civilian player, made a similar suggestion, but with the effect that Russia receive a discount on the Black Market for one turn.[602] In both cases the suggestions illustrated good understanding of the underlying cyber security topics, and the players' explanations warranted their immediate inclusion in the game by simply writing the details on a piece of paper (see Figure 17) and shuffling it into the Event Card deck.

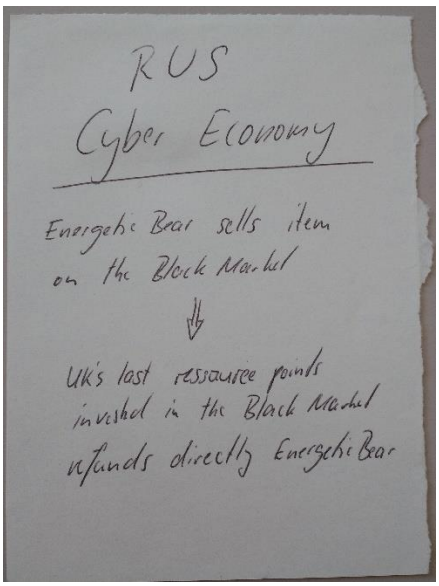

Figure 17: Wizard wheeze Event Card written by German military player (author's own image)

As Nick Luft has remarked, wizard wheezes can sometimes be negatively received by the team who it works against, even resulting in criticism of the umpire who allows it.[603] Although the facilitator did not experience any undue criticism regarding the above wizard wheezes, in the latter case there was some pushback from the UK team who felt there should be some reciprocal event advantaging

[601] Author fieldnotes, 24 January 2017
[602] Author fieldnotes, 29 May 2018
[603] Luft (2002), p. 5

them. This notwithstanding, the fact that the game both enabled players to imagine wizard wheezes and was flexible enough to accommodate the ideas is ample illustration of the modifiability advantage of using a manual game instead of a computer game.

The implication of this modifiability is that player engagement was increased. Because players realised they could make amendments to the game, they critically analysed game components and mechanics, rather than simply accept them as presented. In turn, such critical engagement led to opportunities for learning moments, especially when players applied their own knowledge and understanding of cyber security to the context of the game.

Chapter 6 conclusion

During the course of this research, a notable number of game sessions (33) with a wide range of participating organisations and individuals yielded both varied and insightful data. Analysis of the data has subsequently fallen into three distinct categories: uses of quantitative data, the game creating learning moments, and wargaming theory in practice.

Firstly, quantitative data about player demographics corroborated prior assertions about the ratio of gender participation. As discussed in Section 5.2.1, the military, cyber security, and wargaming are all male-dominated fields, and data from game sessions corroborates these findings. Encouragingly, however, the numbers also suggest that cyber wargaming may be a tool for increasing female participation. Other uses of quantitative game data demonstrated how alternative approaches to wargame analysis (Sections 6.1.2 to 6.1.4) can reveal insights about player performance, real-world outcomes, or the playing styles of different groups. These are legitimate uses of other types of wargames, such as ones focused on operations research (mentioned in Section 2.1) or policy formulation (such as the US Naval War College referenced in Section 6.2.5). In the scope of this thesis, however, the analysis was only intended to be indicative of these possibilities, not provide grounded conclusions.

Secondly, qualitative data based on the researcher's observations about player discussions show that a multitude of learning moments were created using the game. In Chapter 4, the design rationale for game components were analysed with regards to what cyber security concepts the components were intended to convey to players. This chapter has shown that most of the designs were successful: players were able to have discussions around the topics intended, ranging from key actors in cyberspace and their relationships, to cyber attack and defence dynamics, to geopolitical realities. More importantly, in some cases the game served as a catalyst for peer-didacticism, with players able to forge knowledge-exchange relationships during game sessions. Consider the German military player who had no cyber security expertise, yet after their experience with the game now knew what questions to ask and where to direct their questions in order to learn more (in this case about ransomware, see Section 6.2.5). In these instances, the game fulfilled Peter Perla's assertion that the primary purpose of wargames is to help 'ask the right questions' (cited in Section 2.3.3).

Lastly, the practical experience of the researcher in designing and deploying the game provided insights relating to wargaming theory. The tensions between realism and complexity, highlighted by Sabin and others (as referenced in Section 4.1), were prevalent both throughout the design process and the deployment phase. In particular, the researcher's difficulty with writing simple yet comprehensive game rules did not adhere to Wallman's claim that this is an easy task (cited in Section 6.3.1). The game also seemingly succeeded in providing what Perla and McGrady called a 'story-living experience' (referenced in Section 2.2.5) with a high level of engagement from players. Evidence of the emotive power of dice, roleplaying, and overall fun aspects of the game, as documented in Sections 6.3.1 to 6.3.3, amplifies the idea of the game as an experiential learning activity, which pedagogic scholars such as Stramba and Bisson assert are more conducive to effective education (cited in Section 6.3.3). As final notable examples, the prevalence of 'wizard wheezes' – a term used by Luft and others (referenced in Section 6.3.4) – during game sessions evidenced the modifiability

advantage of using a manual game over a computer game, as lauded by both Curry and Price, and Sabin (see references in Section 2.2.1).

The following chapter proceeds to analyse the researcher's experience of conducting the research, with close reference to methodological concerns outlined in Chapter 5.

Chapter 7: A wargaming practitioner's experience

In general, it could be said that there is dearth of critical scholarly work on the practice of wargaming. With notable exceptions, such as the previously referenced Sabin and Downes-Martin, or Rex Brynen[604], who have academic backgrounds, the wargaming corpus is largely written by practitioners for practitioners. Anecdotally, this researcher can attest that gatherings such as the Connections series of conferences (held annually in multiple locations around the globe) are more gatherings for wargamers to share ideas about games than to analyse more fundamental building blocks about wargaming practice. The researcher's impression from immersion in the wargaming community is that wargamers somewhat rely on a set of unspoken and unwritten assumptions about how wargaming is done.

Because of this, it is the researcher's assessment that progress in wargaming has, to some extent, stagnated and knowledge become stale. 'For a very long time,' say Pat Harrigan and Matthew Kirschenbaum (editors of the comprehensive anthology *Zones of Control*, a much-needed influx of literature in the field) 'there were only a handful of essential but well-worn texts on the subject of wargaming.'[605] Giants such as Perla and Dunnigan are rightly held aloft for their contributions, but neither of these have written anything ground breaking for at least a decade (even Perla's chapter in *Zones of Control* draws heavily on his own seminal 1990 book *The Art of Wargaming*[606]), and novel ideas or critique are not forthcoming at a rapid enough rate to keep the field fresh. Elizabeth Bartels[607] leads a small vanguard of nascent wargamers with academic credentials (also including the likes of Anders Frank[608], Johan Elg[609], and Ivanka Barzashka[610]), but there is ample scope for further contributors to make an impact.

[604] Brynen (2010; 2016)
[605] Harrigan and Kirschenbaum (2016), p. XIX
[606] Perla (2016)
[607] Bartels (2012; 2016)
[608] Frank (2014)
[609] Elg (2017)
[610] Barzashka (2017)

With this in mind, the present chapter seeks to make meaningful contributions to the practice of wargaming by relating some of the experiences the researcher encountered during the conduct of this thesis. The intention is to inject observations and analysis which seem to be lacking in wargaming literature, challenging unspoken assumptions and enriching the corpus by linking experiences to methodological aspects outlined in Chapter 5. Furthermore, the analysis draws on academic fields which might initially be considered far removed from wargaming, especially regarding participatory research, thereby introducing new intellectual capital which may help reinvigorate wargaming as a field of critique.

The chapter begins with an examination of the topic of positionality; both strategic positionality – covering the impact of the researcher's background on creating research opportunities – and tactical positionality – including subsections on challenges associated with facilitation, note taking, and game environments. Next, Section 7.2 contains analysis of classification and secrecy issues which were encountered during the course of the research and how they affected the progress of the research. Finally, Section 7.3 comments on the important role of humour during game sessions through two lenses: making fantasy of the familiar, and satirising those in power. A summary section then concludes the chapter.

7.1 The impact of the researcher's positionality

In Chapter 5, two dimensions of positionality were defined. The first is strategic positionality, inspired by Hammersley and Atkinson's 'background knowledge, social characteristics and circumstances' (cited in Section 5.2.1), which refers to aspects of the researcher's background that should be accounted for when conducting the research and analysing data. The second is tactical positionality, which refers to researcher behaviour during the conduct of the research and how this could affect data collection. Tactical positionality is further delineated to encompass two sets of tensions the researcher would encounter while running game sessions: the first, drawing on cautions issued by Dunnigan (cited in Section

5.3.1), is between the roles of game designer and facilitator/adjudicator; and the second, extending the work of Boeing, Wilhemson and Svensson, and Kainikara (all cited in Section 5.4.2), is between the roles of facilitator/adjudicator and researcher. While the definitions were largely theoretical and based on relevant literature, this section analyses how these dynamics materialised in practice.

7.1.1 Creating research opportunities

In traditional ethnographic studies, the researcher often embeds themselves in a location or a community to study it in-depth. Seminal anthropologist Mead lived with Samoan natives for nine months, while the influential Leach spent six years with the Kachin people in Burma (both referenced in Section 5.2). It should be noted that Mead's work has been the subject of much debate, including Derek Freeman's criticisms of bias[611], and Melvin Ember's subsequent charge that bias is also present in such criticisms.[612] For this thesis, however, the broad central research question meant that collecting data from a wide gamut of organisations was more suitable than a narrow subset, and the researcher would need to gain access to these organisations only for a relatively short amount of time – enough to run a game session; a matter of hours, rather than months or years, thereby setting the thesis apart from traditional ethnographic work.

Other researchers conducting participatory work within gaming have used differing strategies to garner participants. Frank (referenced in Section 5.3), for example, already had access to students on a military course he was involved in convening. An option frequently used in economic, psychological, and medical studies is to publicly advertise the research seeking volunteers. Bos used a variant of this, displaying recruitment posters on university campuses.[613] However, neither of these options were feasible for this thesis. The researcher did not have ready access to groups of students as Frank did, and while it may have been possible to publicly advertise the work, this is more conducive to recruiting

[611] Freeman (1983)
[612] Ember (1985)
[613] Bos (2016), p. 47

individual participants than the groups required to play the game, in addition to a number of ethical and methodological complications.[614]

Instead, the researcher secured the participation of organisations via direct contact, either through professional relationships, by meeting interested parties at events (such as conferences), or targeted contact via email. In the following sections, some successes and failures of this approach are analysed, with close attention to the researcher's personal, professional, and educational background (detailed in Section 5.2.1) as influencing factors.

Strategic positionality in networking, opportunism, and serendipity

When reflecting on the process by which organisations came to participate in the research, a common theme which underpins many examples is the role of serendipity and opportunism. Other academics have noted the importance of serendipity, Frank Pieke even going as far as calling it 'the essence of fieldwork research.'[615] The experience of this researcher certainly reinforces this notion because serendipity and opportunism were indispensable to the conduct of the research. Without meeting the right people, largely by accident, and helped by the researcher's strategic positionality, many of the game sessions might never have taken place.

As an example, the participation of UK government department B came about through the researcher meeting a department representative at an academic network meeting organised by a security and international relations think tank in March 2015. When talking to the representative, it appeared that a shared background as War Studies graduates (albeit some years apart) to some extent gave the researcher credibility. Further email contact eventually resulted in a game session at department's premises in London. In another case, German military education institution A became involved after the researcher gave a presentation at the ITEC 2016 conference in London. ITEC is organised by the

[614] For some considerations from various fields on volunteer recruitment, see Greiner (2015); Widerman (1999); and Shtasel et al (1991)
[615] Pieke (2000), p. 138

researcher's former employer, so the researcher had an advantage in that it was a familiar environment, inhibiting the onset of conference nervousness which many academics experience.[616] After the researcher's presentation, a German military officer approached the researcher for further discussions, which eventually, following further telephone and email contact, resulted in an invitation to visit the institution to run the game. Finally, consider the participation of Swedish military education institution A, whose involvement came about after the researcher met a Swedish military officer at the Connections UK conference in both 2015 and 2016. Although the officer was proficient in English, they seemed more at ease communicating in their native language, which the researcher was capable of. Discussions at the conference and subsequent email communication culminated in the researcher visiting the institution to run the game.

These examples illustrate how the researcher's strategic positionality – educational (King's War Studies), professional (events company), and personal (Swedish) background – was beneficial in establishing rapport with key gatekeepers who could ensure the participation of diverse organisations. In other ethnographic work, (potential) gatekeepers may be identified and a plan of contact drawn up as part of the research design; both Carla Reeves[617] and Morrill et al describe how their initial contact with organisations was through pre-identified top managers.[618] Importantly, unlike these authors, none of the meetings with the individuals in the previous examples were premeditated. In this sense, the characteristics of the research reflected those described by David Fetterman as the reality of ethnographic work: 'serendipity, creativity, being in the right place at the right or wrong time, a lot of hard work, and old-fashioned luck.'[619]

Serendipity was a notable omission from the methodology outlined Chapter 5, but purposefully so; after all, luck cannot be planned for. The thesis can therefore be said to adhere to what Isabelle Rivoal and Noel B. Salazar called 'good

[616] See Mills (2006); Haynes (2011); and 'Jan in the Pan' (2013)
[617] Reeves (2010), p. 318
[618] Morrill et al (1999), p. 55
[619] Fetterman (2010), p. 2

ethnographic work,' which 'can and should never be completely orderly.'[620] Just as wargaming is both an art and a science, combining the chaotic with the calculated, so was the practice of this thesis rife with research opportunities which began as unstructured and unplanned but were cultivated into meaningful experiences. The value of serendipity was therefore immense to this thesis, but owing to the role of strategic positionality, other researchers' experiences may vary and there can be no template to work from when taking advantage of unexpected opportunities.

The 'snowballing' effect

Serendipitous meetings like those outlined in the previous section were often instrumental in getting the fieldwork components of the research off the ground. However, as the project progressed, opportunities also arose without the researcher instigating contact with organisations. On several occasions the researcher was contacted by organisations who had heard about the game either via word of mouth or through social media.

The participation International military education institution A is emblematic of this process. A representative from the institution had seen a photo of the game on Twitter, originally posted by one of the players at German military education institution A.[621] This representative then contacted the German institution to find out more and was referred to the researcher. Further email exchanges led to an invite to run a game session at the international institution. In turn, this game session directly led to the involvement of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn. A CCDCOE representative was at international military education institution A at the same time as the researcher and was intrigued by the game. Further discussion eventually resulted in the game being run as a dedicated workshop at CCDCOE's annual CyCon conference in May 2018.[622] The chain of events outlined here therefore evidences the research spreading across three organisations in three separate countries (from a German

[620] Rivoal and Salazar (2013), p. 183
[621] Snellman (2017)
[622] https://ccdcoe.org/cycon/agenda.html

military education institution to an international military education institution to CCDCOE in Estonia), largely due to the efforts of key individuals within these organisations, but without advertising or recruitment actively done by the researcher.

The idea of fieldwork self-perpetuating in this way has not eluded other ethnographers. Jeffrey Sluka, for example, notes how such 'snowballing' was paramount during his fieldwork in the ghettos of Belfast at the height of the Troubles.[623] Moreover, Sluka's account is indicative of the importance of 'snowballing' in sensitive research areas. Once his work had been accepted by key gatekeepers in the community (a priest and a former IRA member), these individuals effectively became evangelists for the research, helping it become accepted by others.[624] Although this thesis was written at an unclassified level, NATO is nonetheless an organisation which handles sensitive information and many parts of the organisation require security clearance to access. By individuals on the inside championing the game internally within NATO at CCDCOE, the researcher did not have to contend with these barriers for the research to gain traction, thereby creating fieldwork opportunities (although see Section 5.2 for discussion of how security and classification hampered the research).

Meanwhile, both Catherine Palmer and Ian Alam relied on 'snowballing' as a methodological technique in order to gain access to more research subjects in Australian Rules football fandom[625] and corporate marketing respectively.[626] Although this thesis did not consider 'snowballing' in its methodology, practical experience indicates that this effect was crucial in developing new fieldwork opportunities. Because other researchers in gaming and wargaming recruited research participants in different ways (Bos' posters and Frank's students, as referenced previously), 'snowballing' does not appear to have been considered in wargaming literature. With this in mind, the researcher's experiences presented in this section can be considered an original contribution to the corpus.

[623] Sluka (2012), p. 288
[624] Ibid.
[625] Palmer (2010), p. 426
[626] Alam (2005), p. 100

Failures to gain traction

Despite a plethora of examples demonstrating how research opportunities could occur through both serendipitous meetings and 'snowballing', these cases were outnumbered by the amount of times the game failed to gain enough traction for a game session to the organised. Sometimes the researcher would contact an organisation who had been deemed as potentially interested in engaging with the game, only to receive a negative response, or no response at all. Other times information about the game might be positively received and inroads made into establishing a foothold in the organisation, only for communication to peter out. This could be caused by the point of contact leaving the organisation, or by imperatives outside the contact's control (see, for instance, example with legal barriers in Section 7.2.1), but often the reasons for communication ceasing remained unknown.

The following (anonymised) examples from the researcher's interactions with various organisations demonstrate different stages of failure. Representatives of a large cyber security company, for instance, were introduced to the researcher via email by a staff member at the researcher's university. However, after following up the introductory email with more information about the research and the game, no reply was received from the company. In another case, the researcher contacted a security-oriented intergovernmental organisation, which had been suggested by a German military game participant (though no point of contact was provided).[627] The initial response was surprisingly swift and positive given the unsolicited contact, but after providing more information about the game nothing was heard from them again. More progress was made with a representative from a large investment bank, who had originally learned of the research from seeing an academic poster displayed at a Royal Holloway open day. Email correspondence followed for the next six months, yet logistics proved a hindrance to organising a game session and communication eventually stopped. Finally, consider the examples of both a non-profit information security professionalisation organisation and an aerospace and defence company. In these cases, the researcher had made significant progress in establishing contact,

[627] Author fieldnotes, 24 January 2017

including telephone conversations with the professionalisation organisation and hosting a meeting with a representative from the defence company to showcase the game. Despite strong expressions of interest, however, no game sessions with either organisation materialised, and communication ceased.

Contextualising failures in academic literature

The researcher did not systematically record their interactions with organisations, so a complete breakdown of the failure rate is not attainable, but it can be estimated that failures outnumbered successes by around three to one. It is difficult to know how this compares to other academics doing fieldwork, particularly in gaming. In Bos' research he describes encountering 'indifferent or hostile' responses when attempting to recruit participants via online in-game communication but does not provide a number to quantify these failures.[628] Aforementioned Morrill et al state that their 'initial forays into polyarchies often met with failure', but without a reference point it is not known how 'often' compares to the experience of the present researcher.[629]

On the other hand, failures are not just statistical events, but also carry qualitative implications and offer opportunities for reflective practice. Failure can be a demotivational factor which stops the researcher progressing further or can affect how future fieldwork attempts are approached. Jo Lindsay, for example, writes that after her initial failures to recruit participants for survey research she herself 'felt like a complete failure' and that approaching the same organisation again went 'against her initial feelings', but she was then 'relieved' when an amended recruitment tactic was successful.[630] Although these extremes were not directly shared by the present researcher, the process of creating research opportunities was certainly an emotional experience. The elation and excitement of receiving assent from a high-profile organisation such as UK government department B or the German military education institution were memorable and can be contrasted with the disappointment of failures, though never to the point of causing despondence.

[628] Bos (2016), p. 46
[629] Morrill (1999), p. 65
[630] Lindsay (2005), p. 127

It is possible that the feelings of this researcher were tempered by the drawn-out process by which most participants were recruited (usually involving initial discussions followed lengthy email chains), while for other academics success or failure was more instant, thereby eliciting stronger emotional responses. However, another important facet to consider in this regard is the role of strategic positionality. The stereotype that males are less emotional will not be propagated here, but the researcher's experience outside academia may have contributed to why they received failure more stoically. Martin Schwartz has posited that 'students who are accustomed to getting the answers right' struggle with the idea that academia 'allows us to bumble along, getting it wrong time after time, and feel particularly fine as long as we learn something each time.'[631] Although writing specifically about science, the point can be made that students with a greater breadth of experience, either with other academic disciplines or generally outside academia, react less extremely to failure. In her study of international exchange students, Tracy Rundstrom Williams refers to this as 'emotional resilience' – the ability to 'face failures…and to continue working towards positive interactions' – as one of the key benefits of studying abroad.[632] Given that the researcher had both professional experience outside academia and personal experience living in different countries (as outlined in Section 5.2.1), these aspects should not be discounted when analysing the researcher's reactions to failed fieldwork opportunities.

7.1.2 Tactical positionality

In Chapter 5, tactical positionality was defined as distinct from strategic positionality. Where the latter can be said to encompass macro issues that influenced the research, the former concerns micro issues which had influence during game sessions. These micro issues were in turn classified into two types, the first of which concerned the tensions between the role of game designer and facilitator/adjudicator. Dunnigan (cited in Section 5.3.1) highlighted that 'false prophets' usually only become evident after it is too late, and this was taken to mean that game designers can sometimes become overzealous about the capacity

[631] Schwartz (2008)
[632] Rundstrom Williams (2005), p. 359

of their games to achieve their intended outcomes (in the case of this thesis: teach lessons). If players trust the designer's promise implicitly or uncritically, they may not recognise limitations of a game, thereby perhaps placing excessive faith in the game outcomes (in the case of this thesis: learning the wrong lessons).

The second type of tactical positionality concerned the tensions between the role of facilitator/adjudicator and researcher. The literature on wargaming is already conscious of these tensions, as highlighted by Wilhelmson and Svenson and Kainikara (all cited in Section 5.4.2). Here, difficulties can arise when one person attempts to simultaneously be in the thick of the game action to facilitate engagement or adjudicate on a game matter, whilst also being removed (sometimes physically) and invisible to players in order to make research observations and record notes. These dual roles can compromise each other, for example a researcher influencing a game with a biased adjudication decision in order to duplicate a previous research finding, rather than adjudicating impartially and fairly.

In the following sections, the tensions of tactical positionality are analysed through the researcher's experience of three themes: facilitation, note taking, and the game surroundings. As an example of the interdisciplinary nature of this research, these sections all draw on different strands of literature, though there is also overlap and cross references.

Experiences in game facilitation

It was noted in Section 5.4.2 that the researcher, in convening a wargame, would have to tread a careful balance between being facilitator who effectively encourages players to achieve learning objectives, and a good researcher who ensures proper data collection. This balance would encompass the physical presence of the researcher, their interventions in the game, and their interactions with the players. The researcher's practical experience of being a wargame facilitator, in the context of this thesis, are here analysed under four themes which became apparent as the researcher reflected on their experiences:

facilitator competency, game session control, facilitation mistakes, and physical energy.

It should be noted that the researcher had no prior experience or expertise in wargame facilitation. They had some awareness of the rituals and principles of facilitation through wargaming literature and participating in wargames facilitated by others, but these are no substitute for first-hand experience. The challenges of dealing with difficult players or situations, or making facilitation mistakes, were initially faced with improvisation, but over time the researcher became more accustomed and confident in facilitating the game. The account in this section partly captures the researcher's journey from a novice to becoming an accomplished wargame facilitator.

Facilitator competency

Something which became abundantly clear after running the game session at International military education institution A was that facilitator competency directly affected potential learning moments. In this session three games were run simultaneously in two separate rooms, but the researcher had trained three institution staff members to act as facilitators (by demonstrating the game and giving some basic facilitation advice), ostensibly freeing the researcher up to flit between games to make observations or assist when necessary. Unfortunately, out of the three staff members, only one proved to be an accomplished game facilitator (even improvising their own adjudication methods), while the other two lacked competency and one was reluctant to run the game without the presence of the researcher.[633] The researcher's impression was that in the games facilitated by the less competent staff members, the vast majority of players' attention was focused on grappling with the game rules rather than the thematic content, thereby limiting the potential learning moments that could be created. In the game facilitated by the accomplished staff member it is likely less friction with the rules enabled greater engagement with the cyber security aspects of the game; however, because the researcher was forced to spend a disproportionate amount

[633] Author fieldnotes, 28 April 2017

of time with the other games they were limited in what observations they could make.[634]

The effect of the competency of the facilitator on learning moments was also prevalent in a game session with students at UK military education institution B. Here, only one game was run, facilitated by the researcher, with an institution staff member assisting. This staff member's competency as a facilitator became prevalent in the post-game discussion, where their pedigree as an educator came to the fore. The staff member was able to lead the discussion along paths that clearly illuminated learning moments, for example with an exercise using Post-It notes.[635] The structure of the discussion forced participants to vocalise and rationalise their thoughts about the game in such a way that the lessons learned could be shared among the whole group, thereby maximising the pedagogic potential of the game. The staff member's competency as a facilitator was key in enabling this. These examples illustrate what other wargaming practitioners like Mahoney, Wiggins, and Burns (all referenced in Section 5.3) have advised with regards to facilitation. The institution staff member was adept at drawing out opinions, creating feedback loops, and driving the discussion towards game objectives.

The researcher's own proficiency in this facilitator role is difficult to judge without external assessment. However, if the amount of learning moments created can be used as a guide (Chapter 6), the researcher should be considered a successful wargame facilitator within the remit of this thesis. Being a good facilitator both is and is not a requirement for this research. In one sense, good facilitation was crucial to ensuring player engagement with the game (see Section 6.3.3), without which players might not have learned as many lessons. But such facilitation need not have been done by the researcher; for example, the game could have been designed to be playable without a facilitator, in the vein of popular board games such as Monopoly. In such a setting, the researcher could have retreated into an observational role, thereby perhaps capturing more detailed analysis of players behaviour and discussions (see next section for discussion of fieldnotes). The

[634] Author fieldnotes, 28 April 2017
[635] Author fieldnotes, 15 May 2017

point here is that the researcher's proficiency as a facilitator shaped the outcome of the research, but that does not preclude less competent facilitators from pursuing similar work.

Controlling game sessions

Another facet of facilitator competency is the ability to control a game session, both to ensure frictionless flow of the game and to create learning moments. In the same way that a Dungeon Master in Dungeons & Dragons is tasked with conjuring a game world, progressing the game's story, and adjudicating on players' actions, all while ensuring player enjoyment – as wonderfully described by John Eric Holmes – so must a wargame facilitator lead a game session, often in challenging situations.[636] During the course of this research several instances of difficult player behaviour were encountered that pushed the researcher's ability to control a game session.

In a post-game discussion at German military education institution A, the topic of anonymity in cyberspace and proxy actors was the source of intense debate between several of the participants. What started out as good observations by two people grew into a heated (though cordial) argument, with other participants joining in on either side. Eventually the discussion reached an impasse too far from cyber security and the researcher felt a need to intervene to bring it back on topic.[637] The challenging component of this was that every participant was a military officer between Major and Lieutenant Colonel on a strategic leadership course; people with exceptionally strong influence and command skills. Despite them being perfectly friendly and welcoming to the researcher, there was nevertheless an intimidating element to interjecting in the debate given the researcher's clear status as an outsider in this environment. In the end the interruption successfully brought the discussion back on track, but the researcher's experience is noteworthy from a wargaming practitioner's perspective.

[636] Holmes (1980)
[637] Author fieldnotes, 24 January 2017

On other occasions the researcher ceded control of the game session to more capable facilitators. Most prominently this occurred during both the International academics A and B sessions, where a British military officer was present and able to assert control of discussions.[638] Both sets of participants were unruly (see examples from Section 6.3.3), often interrupting each other or vying for attention. The researcher wrote in their fieldnotes that "it was very lucky [officer] was there (in combats) as his authority helped keep players in check (as they themselves acknowledged)."[639] The presence of a uniformed military officer created structure in the game session, which the researcher is unlikely to have been able to conjure on their own. This structure could be considered a positive atmosphere (as attributed to Wilhelmson and Svensson in Section 5.3) where the point of authority was neutral, thereby not inhibiting discussion. Indeed, despite their unruliness, many learning moments were successfully created in these game sessions, which must be at least partially attributed to the officer's capacity to control the sessions.

Finally, the researcher's experience at one edition of the Connections UK wargaming conference (London, September 2017) stands out as an example of challenging participant behaviour. In this game session, all players were strangers to each other, and on the Russia team this resulted in huge personality clashes. From the outset, one of the team members found themselves isolated and unable to argue for their preferred course of action. By the second game turn the player had sourly relegated themselves to a spectator and in turn three, following a final argument with their team, stood up and left the game.[640] At the time, the situation was enormously awkward, and the researcher was unsure how to proceed. Ultimately it was decided to ignore the situation and complete the game, which was done successfully, but the researcher felt compelled to offer an apology to the player the next day, which was well-received. The player, an experienced wargamer, also provided a note of caution about strong personalities in central roles; other wargamers have similarly testified that 'personality conflicts, over-competitiveness, and anger' can be features of game sessions.[641]

[638] Author fieldnotes, 18 April 2017
[639] Author fieldnotes, 4 May 2016
[640] Author fieldnotes, 7 September 2016
[641] Johnson (1988), p. 6

This may be counterintuitive if we consider stereotypical wargamers as a more reserved characters – Jim Dunnigan himself admits to being 'a shy person by nature'[642] – yet it also makes sense in the context of socialisation: the process which 'establishes common definitions in the way a situation is perceived.'[643] Terri Toles-Patkin has written that 'should the socialisation process prove unsatisfactory, the [player] can remove himself from the situation,' which is precisely what happened in this game session.[644] As an experience of facilitating wargames this is perhaps an extreme example, but one which embodies the difficult challenge of game session control.

Facilitation mistakes

In addition to challenges created by participants, the researcher also made unforced errors when facilitating games. In one game session, for example, the UK team had accidentally been allowed to place the Software Update Asset on the Electorate, which is not possible according to the restrictions of the Asset. The UK team brought this to the researcher's attention and the Asset was quietly swapped out for the Education Asset, with the effects carried over. Russia did not notice the swap and the researcher decided it would have been more complicated to explain than let the game progress.[645] The error was inconsequential to the result of the game but did illustrate that human wargame facilitators are not infallible. The capacity of facilitators to make mistakes has been recognised in related literature[646], and in the wargaming context by Craig Orme, who emphasises the objectivity of simulators (computers) in adjudication.[647] On the other hand, the modifiability of a manual game (as discussed in Sections 2.2.2 and 6.3.4) was also showcased in this example.

Facilitation mistakes were more serious when they compromised the impartiality of the researcher and impacted gameplay. In one session the researcher inadvertently advised Russia against transferring Resource for an Attack because the UK target was protected by an Asset. The UK team did voice a complaint at

[642] Dunnigan (1992), p. 148
[643] Toles-Patkin (1986), p. 5
[644] Ibid., p. 7
[645] Author fieldnotes, 6 September 2017
[646] For example Kirk and Broussine (2000), p. 18; Schwartz (2002), p. 301
[647] Orme (2013), p. 1

this but did not harbour further ill feelings.[648] Nonetheless, the researcher had clearly intervened in the game in a way which did not adhere to the neutrality and impartiality advocated by Kainikara (referenced in Section 5.4.2). In another session such impartiality was impossible to maintain owing to player availability. For long periods of a game with civilian industry participants, the UK team was left with only one player owing to team members leaving for phone calls and meetings. The game contains too much material for one player to manage, so at these points the researcher stepped in to offer advice, though was careful to always let the player make the final decision on any actions.[649] This was less of an unforced error than it was a conscious intervention by the researcher, but it did jeopardise the fairness of the game's competition because the researcher, in also being the game designer, could provide knowledge imparting an unfair advantage.

The takeaway from these paragraphs is that while manual wargames benefit from human knowledge and ingenuity, they are also fraught with human frailties. As the previous examples illustrate, facilitation mistakes can impact the course of the game and players' experiences. This problem is exacerbated when the facilitator simultaneously undertakes multiple roles – in the case of this thesis also game designer and researcher – placing additional stress on the facilitator's faculties.

The physical and mental energy drain

One final issue which was a central aspect of the researcher's experience, but is remarkably absent from wargaming literature, is how facilitating wargames was physically and mentally taxing. Warren Wiggins has noted that facilitators may need some mental resilience when delivering contentious adjudication decisions[650], while Solomon Smith warns that 'it is important to mentally prepare for various scenarios,' although he is more concerned with the context of the classroom than wargaming in general.[651] Neither of these, however, give any indication as to the high cognitive load a facilitator is liable to experience. With regards to the physicality of facilitating, wargaming literature only concerns maintenance of positionality (as discussed in Section 5.4.2), but not how the role

[648] Author fieldnotes, 6 September 2017
[649] Author fieldnotes, 6 March 2017
[650] Wiggins, p. 5
[651] Smith (2013), p. 571

can be draining. The researcher's experience, as recounted in the following paragraphs, can therefore be considered an original contribution to the wargaming corpus.

The researcher is not an unfit individual, but even a regular two-hour game session with a single game would often leave the researcher exhausted. This condition was amplified if multiple games were run simultaneously within one session or multiple sessions run sequentially.[652] The cause of this was likely a combination of physical and cognitive factors. As a central focal point, the facilitator would usually stand at the end of the table between the seated teams, able to reach all parts of the game board. Sitting down was normally not an option as it limited the researcher's reach, but in order to become more immersed in the game and be able to talk *with* players rather than *down at* them, the researcher spent long periods of time stooped over table. Despite not involving a great deal of movement, this position was nonetheless physically demanding.

In addition to the physical dimension, mental taxation was also a significant factor. As facilitator, the researcher would have to pay close attention to every move in the game to ensure no rules were broken (either inadvertently or purposefully) as well as address questions or comments from players. Meanwhile, in their role as a researcher they would also have to make mental notes about the conduct of the game, players' engagement, and discussions (see Section 7.1.2 for further analysis of notetaking). Given that a single game could have up to ten participants, these cognitive processes would need to be running in multiple instantiations concurrently. Doing this for two hours or more, in combination with the physical exertions, often resulted the researcher being exhausted after a game session.

That physical and mental strain is mostly absent from wargaming literature is likely due to the majority of the corpus being written by gamers for gamers. One of the unwritten assumptions in the wargaming community, as mentioned in the introduction to this chapter, may be that facilitation is taxing, but no one has taken time to further critically reflect on this, or report it in writing. This is to the

[652] Author fieldnotes, 6 September 2017

community's detriment, because if we consider honest, reflective contributions on these aspects in other fields, we see that these fields are richer for it. In, ethnography, for instance, Samantha Punch recounts the strain of striving to interact positively with research participants, speaking a foreign language, and 'behaving in culturally appropriate ways.'[653] Writing through the lens of public health, Virginia Dickinson-Smith et al are cognisant that academics are socialised against speaking of their emotions, thereby suppressing them.[654] Meanwhile, Michael Wilkinson, coming from a general facilitation perspective (such as training seminars) analyses the importance of high energy to energise topics, engage participants, and elevate the facilitator.[655] From a broader anthropological standpoint, Lynne Hume and Jane Mulcock issue the warning that during fieldwork 'the possibility of experiencing physical and emotional trauma is frequently unavoidable.'[656] Although the researcher's experience as a wargame facilitator was far from traumatic, there was nevertheless noteworthy physical and mental strain, as outlined in the preceding paragraphs. It is hoped that the present contribution is valuable to wargaming, much in the same way that Punch's account is valuable to ethnography, in writing openly about the realities of fieldwork.

Experiences with fieldnotes

Fieldnotes are one of the most rudimentary techniques for recording observations during fieldwork. There is no shortage of analysis of the role of fieldnotes in anthropology and ethnography, and guides on how to take them[657]; a chapter by Roger Sanjek even outlines specialist vocabulary associated with fieldnotes.[658] Fieldnotes were the primary means by which the researcher's observations of game progress and players' behaviour and discussions were recorded, but this technique was not used uncritically. In Section 5.4.1 some methodological considerations around notetaking were identified, including drawbacks outlined

[653] Punch (2012), p. 90
[654] Dickinson-Smith et al (2009), p. 66
[655] Wilkinson (2004), pp. 239-240
[656] Hume and Mulcock (2004), p. xxii
[657] As an example, see Emerson et al (2011)
[658] Sanjek (1990)

by Hammersley and Atkinson. Of these, a particularly prevalent aspect experienced by the researcher was that the character of notes changed as the research progressed. In early stages of the fieldwork the researcher attempted to take handwritten notes during the game sessions. This proved untenable as the demands of facilitating games left no time to make substantive notes. As the research progressed, it became clear that these notes would not provide sufficient data to meet the research objectives, and a decision was instead made to write up notes after the conclusion of a game session, which was a significant improvement; consider the difference in the following examples:

Table 4: Comparison of fieldnotes as the research progressed

21 October 2016	29 June 2017
“[Player] comment about visibility”[659]	"The idea of blindness was raised early on by [player], but I parked it and returned to it in the post-game discussion. - Asked if teams would have played differently if they couldn't see what the other team were doing; answer was unanimously yes. -- Lots of actions were taken on basis of predicting what other team had Resources to do (e.g. bidding) -- Russia in particular said they would not have known to concentrate attacks on Electorate if they could not see UK Plc were defended."[660]

The note on the left is from a game session early in the fieldwork, made during the game, and is characterised by its brevity. Although it alludes to a learning moment, in this case visibility (discussed in Section 6.2.7), the note does not capture any specifics about what players said, when they said it, or how it was

[659] Author fieldnotes, 21 October 2016
[660] Author fieldnotes, 29 June 2017

said. The note on the right, on the other hand, made after a game session later in the fieldwork, demonstrates the comparative richness of these notes. Here, the note contains information not only about specific comments regarding a learning moment, but also the timing of those comments and the structure of the discussion (researcher-moderated). Fieldnotes made after the conclusion of a game session were invariably more detailed than those made during games, making them more valuable in terms of providing research data. The pictures in Figure 18 illustrate the differences in early and later fieldnotes in practice.

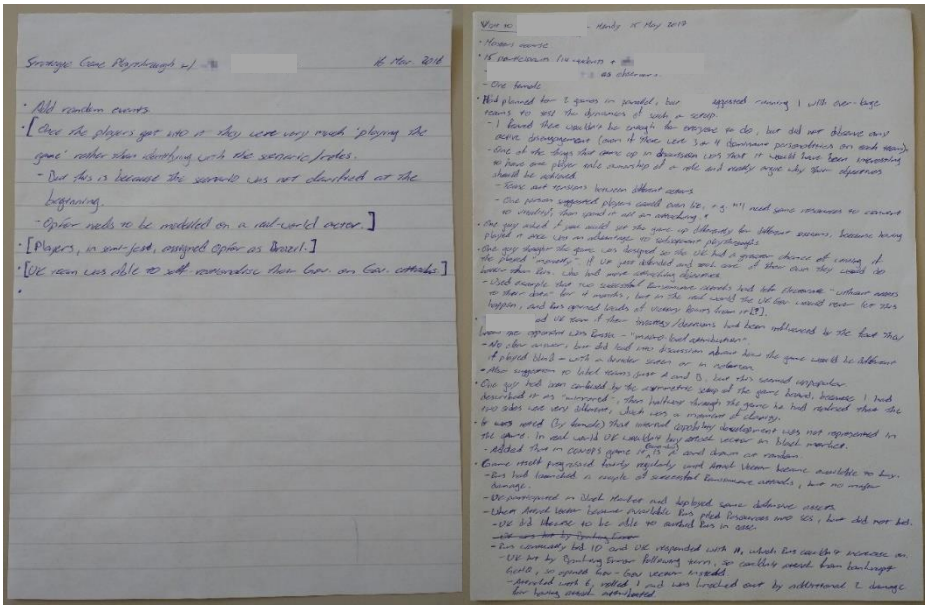

Figure 18: Comparison of early (left) and later (right) fieldnotes. Note paucity of detail in the earlier note, as well as its brevity; earlier note is A5 paper, later note is A4 and continues for multiple pages (author's own photograph, participant details obscured for anonymity.

The approach of writing fieldnotes after game sessions meant relying on the researcher's memory for notes, as no other recording mechanisms were employed (as justified in Section 5.4.1). With the pressures on the researcher's cognitive faculties analysed in the previous section, it is perhaps understandable that the quality of the notes was sometimes affected. The following examples demonstrate lapses in the researcher's memory which negatively impacted data gathering:

> "[Player] (?) said something profound in pre-game discussions, but have forgotten what.

- Maybe about China."[661]

"[Player] said something about relationships changing through the course of the game, e.g. Russia Government-Rosenergoatom breaking down after first quarter (can't remember details or context)."[662]

In both cases participants contributed something valuable but the researcher failed to adequately capture it. Without excusing the researcher's notetaking performance on these occasions, the context of the game sessions should be expounded because they influenced notetaking capacity. In the first example, logistical contingencies meant that the note was made two days later. It may therefore be understandable that some details of the game session escaped the researcher's mind in the intervening time between the session and the note being made. In the second example the note was made after a double game session, with two games having been run sequentially, thereby providing more data to memorise and note, as well as multiplying the physical and mental strains on the researcher.

In Robert Emerson et al's overview of the literature on fieldwork, they observe that strategies on timing and organisation of fieldnotes differ; however, the researcher's approach of writing notes immediately after a game session seems to be accepted practice in ethnography.[663] In the researcher's experience, this practice also resulted in nearly all fieldnotes being written under less than ideal circumstances. A large portion were written on trains travelling back from game sessions, when the researcher's memories were still fresh, while others were written in conferences (where a game had been run) or hotel rooms. In the past, 'travel writers' were often considered 'superficial', largely because their association with movement intimated that in-depth observations could not be made.[664] In modern ethnography, however, James Clifford has contested that with increased global mobility '"the field," seen as a place of writing, leaks,' and its boundaries 'begin to blur.'[665] The "field" today is not contained to the site of

[661] Author fieldnotes, 25 April 2017
[662] Author fieldnotes, 6 September 2017
[663] Emerson et al (2007), p. 354
[664] Clifford (1997), p. 201
[665] Clifford (1990), p. 64

study, but permeates the entire research journey. The point here is that fieldnotes for this thesis really were *field*notes, recorded away from the comforts of the researcher's office. The experience of the researcher certainly corroborates Clifford's assertion about the malleability of the "field", while, despite dips in quality as outlined previously, the researcher's notes provide sufficient depth to demonstrate that writing on the move can be a successful notetaking strategy.

Challenging game surroundings

Just as the act of taking fieldnotes had to be adapted to circumstances, so did the researcher have to adapt to the challenge of different game surroundings. Because the majority of game sessions took place away from the researcher's institution, they had little control over the setting for the game. Most organisations were accommodating by asking about requirements, for example table size. Usually the game took place in a classroom or boardroom of appropriate size with few external distractions, which meant running the session was relatively straightforward. Occasionally, however, challenging situations materialised, forcing the researcher to adapt facilitation of the session. In this section, challenges are delineated and analysed according to three types: physical, environmental, and atmospheric.

Physical challenges: multiple games in one session

In sessions where the researcher had to facilitate multiple games simultaneously, efforts were made to place tables close together to minimise physical movement required, as illustrated in Figure 19. Although players may have been more liable to be distracted by what was going on in the adjacent game(s), it was necessary to ensure the researcher had quick access to all games in order to effectively facilitate them.

Figure 19: The researcher (standing centre) explaining the game rules to three tables being run simultaneously at CyCon 2018. An assistant facilitated the game on the left with occasional input by the researcher, while the researcher facilitated the two games on the right, which had been placed close together for ease of access. (Image credit: Nick Robinson. Image source: Nick Robinson on Twitter (https://twitter.com/nickdr92/status/1001440409825013760). Image in public domain.)

In one case, at International military education institution A, three games were split across two rooms, making it impossible to place all tables in close proximity. Here, facilitator competency (discussed in Section 7.1.2) was used to determine the setup, with the more competent facilitator taking charge of one game in one room and the other two games being placed in the other room where the researcher could easily supervise both.

Environmental challenges: informal settings and social spaces

Some settings were more informal, with games being run in social spaces. In these situations, the players' attention was not always committed to the game, meaning player engagement might differ from that discussed in Section 6.3.3. On the other hand, these settings created a relaxed atmosphere conducive to player enjoyment, even if the presence of food and drink was at times unnerving for the researcher given the risk of spillage damaging game material.[666] In these social

[666] Author fieldnotes, 9 February 2017

spaces the provision of appropriate tables was not always guaranteed, forcing the researcher to improvise by using whatever surfaces could be found.

Atmospheric challenges: overbearing superiors

A different type of challenging environment, directly counter to the relaxed atmospheres of the social settings, was the presence of an imposing superior. This was only encountered in one game session with Australian civilian industry participants, where players had entered the room and divided themselves into teams (including the aforementioned enthusiast in Russian uniform). However, before play began another participant joined and promptly assigned teams to all players, resulting in four of the players swapping sides.[667] At the time this seemed like a manager throwing their weight around and the researcher later confirmed that the participant in question was a Partner at the firm. The Partner was not present for the duration of the game session, but the times they were in the room there was a palpable change in atmosphere with several players reticent to voice opinions. Recall from Section 5.3 that Wilhelmson and Svensson, and Burns all warned that the presence of an overbearing superior may stifle player participation. In this case, although an isolated one, the experience of this researcher attests to this possibility being realised.

Flexibility as a trait of tactical positionality

The previous examples demonstrate that the game surroundings, both material and affective, could not always be controlled by the researcher and sometimes posed challenges. The ability of the researcher to adapt to situations was therefore paramount to conducting game sessions and the researcher's tripartite role of designer, facilitator/adjudicator, and researcher was important in enabling this adaptability.

With regards to the designer-facilitator nexus, Perla et al identified creativity is a core trait of wargame designers, and it can be posited that adaptability of facilitators is an extension of this.[668] With the researcher in this thesis assuming both the roles of designer and facilitator, it makes sense that the creativity which

[667] Author fieldnotes, 7 December 2017
[668] Perla et al (2002), p. 21

underpinned game development was also applicable during game deployment. As for the facilitator-researcher junction, the researcher adopted a simplified version of Sabin's assertion (cited in Section 4.1), that it is better to play than not to play. This stance posited that learning moments could still be created even in less optimal game surroundings, so the researcher could be flexible about how a game was set up and run, optimistic that useful research data could still be collected.

In the vein of flexibility, it is also pertinent to link the researcher's experience to the advantages of using a manual game. Because the game was not dependent on any electronic hardware (an advantage propounded by Curry and Price in Section 2.2.1) or precise environmental configuration (for example separating the teams) it was possible to use it in a wide variety of settings, adapting the layout according to the environment. The flexibility of both the game and the researcher therefore enabled challenges associated with game surroundings to be overcome.

7.2 Secrecy, security, and classification of information

It was noted in Section 5.2.2 that both cyber security and wargaming can carry heavy classification labels, even more so in the case of cyber wargames such as exercises ELIGIBLE RECEIVER and LOCKED SHIELDS. Issues around secrecy were encountered multiple times during the course of this thesis research, both in terms of access (to participants and other games) and participant contributions during game sessions. However, classification did not prove a hindrance to the thesis as ample alternative unclassified sources were accessed and player contributions were substantial, as elucidated in Chapter 6. While the following sections outline some of the researcher's more frustrating experiences at the fringe of classified environments, the takeaway for others in the cyber wargaming field is that it is worth persevering with unclassified work because very good results can be achieved even without access to closed doors and secret information.

7.2.1 Access denied

Only persons with relevant security clearances can access classified information and environments. The researcher did not hold a clearance during the time of the thesis, although in the design of the research this was inconsequential because the work was intended to be entirely unclassified. Nonetheless, the topics of cyber security and wargaming, combined with the researcher's institutional affiliations and professional networking, resulted in the research having close proximity to government, security, and military establishments where classified work took place. Two instances of the researcher encountering classification barriers are worth exploring; one demonstrating restrictions on participation and one hinting at inaccessible work.

First, through a mutual acquaintance (who had taken part in one of the game sessions), the researcher was introduced to a staff member at a US military-affiliated academic institution. Over initial email exchanges the institution appeared very interested in the research and the game, asking insightful questions and providing an outline of some of their own efforts in cyber wargaming. However, when the researcher offered to organise a game session, either in person or by sending a copy of the game, they were met with the following response:

> "With much regret, [institution] can't be directly involved with game play testing and feedback, according to our lawyers. There are some sticky legal wickets which would make it problematic."[669]

There was no further elaboration on what these 'sticky wickets' were, but the underlying premise could be interpreted as one of classification. If the institution participated in a game session and provided feedback about the game, they might inadvertently reveal information about their own cyber wargames, which were classified. Such inadvertent revelation has been considered by Lenore Manderson et al in their introduction to a dedicated anthropology journal supplement on secrecy and disclosure. They conclude that seemingly innocuous descriptors and

[669] Author email correspondence with US institution, 7 February 2017

actions like 'names, body language, and strategic silence' can all reveal secrets.[670] From the institution's point of view, limiting all interaction and communication was likely the most effective way to prevent inadvertent revelation of classified material.

The international aspect may have played an additional role, with US military-affiliated researchers being restricted in how much they could interact with UK-based civilians. Furthermore, there may have been issues with the institution's official affiliation, which might have been considered the institution endorsing the game as a US government representative. This problem could be understandable given some of the contentious geopolitical events depicted in the game. Whatever the exact legalities, the example illustrates how classification-related barriers could prevent potential participants from playing the game.

Second, the researcher had been introduced to the person responsible for Cyber Skills and Education within UK government department C. After initial contact via email and a meeting hosted by the researcher, the person was very keen to see a game session in action and rallied a few interested people. The session was organised at the UK military education institution B, but on the day of the game, everyone attended apart from the person who had been the primary driver behind organising it. The researcher was informed that the person had instead decided to participate in a cyber wargame at UK government department C's offices in London.[671] The game session was a success regardless, but the experience highlighted that much work in this field goes on behind closed doors. The nature of UK government department C's wargame was not divulged to the researcher, so nothing is known about its design or intended outcomes. It is also reasonable to assume that further cyber wargames have been conducted by UK government department C and in other classified organisations, both in the UK and overseas. The corpus of cyber wargaming is therefore much bigger than that explored in Chapter 3, but without access to classified spaces this researcher was only able to analyse the tip of a presumed iceberg.

[670] Manderson et al (2015), p. S189
[671] Author fieldnotes, 8 May 2017

These examples demonstrate how classification and secrecy can introduce a degree of ambiguity to research. In the researcher's experience, there were agendas hidden shrouded by classification markings which were often hinted at but never revealed. Some participants' interest in the research, for example the UK government department C person in the previous example, was unclear, and it is largely unknown what they did with the information they received. In this respect, Celso Castro has testified that 'being classified as "friends" or "enemies" by the military' can be fundamental to the success or failure of research.[672] During the course of this thesis, the researcher's successes with the likes of the German military education institution, the International military education institution, and UK military education institution B suggests that individuals from these organisations categorised the researcher as a 'friend'. Other times, notably the example from UK government department C in the following section, the researcher's lack of security clearance clearly put them in the 'enemy' category. Extrapolating this notion further, it could be posited that the failures outlined in Section 7.1.1 were also symptomatic of the researcher being categorised as an 'enemy', despite these not being military organisations.

In the researcher's experience, managing the uncertainty associated with classification can be a challenge because there may not be clear indicators whether another party would see the researcher as 'friend' or 'enemy'. Furthermore, initial categorisation may not be final, and a researcher can flip between 'friend' and 'enemy', periodically granted or denied access.

7.2.2 Stifled participants

Issues around classification did not just affect what the researcher could access, but also restricted what some players could contribute. Participants with knowledge of secret information were not able to share this, even if would have been conducive to creating learning moments where knowledge could be shared, because all game sessions were unclassified. The starkest example of the constraints of classification occurred in a meeting the researcher had with UK

[672] Castro (2013), p. 13

government department C, where they had been invited to showcase the game to a number of interested parties. When all attendees had assembled, but before the meeting had begun, one person asked what classification level the meeting was at and seemed disappointed to learn it was an unclassified level. The person later admitted that to build an accurate game model for use in a decision-making game, the designer would need access to classified data concerning both the blue and red teams.[673] Their disappointment at an unclassified meeting suggests the person had insights to share – perhaps data to create a more accurate game model – but were unable to do so.

Additionally, their stated requirement for classified data emphasises the difficulty of designing an accurate cyber wargame. With traditional, especially historical, wargames a wealth of data is available to the designer (for example rifle calibres, artillery ranges, or aircraft speeds) on which they can model game mechanics.[674] In cyberspace the characteristics of offensive and defensive capabilities are more difficult to measure; partly because of the lack of physical manifestation, but largely because of the amount of secrecy surrounding these topics. This vindicates the design philosophy behind the game used in this thesis: create a stimulating representation rather than an accurate simulation. Attempting to create an accurate simulation would have been futile in an unclassified research environment, whereas a stimulating representation could be created based solely on publicly available information.

As a final example of tensions around classification, a notable incident occurred during a game session with a mixed civilian participant group. During this session the players discussed transparency on the Russian side, noting that Government and Rosenergoatom are reasonably transparent, whereas SCS and Energetic Bear are very opaque. At this point the discussion was punctuated by the following exchange observed between two participants:

> [UK civil servant 1, player]: "As if we don't have good insight into these [pointing to Russia Government and Energetic Bear]."

[673] Author fieldnotes, 14 April 2017
[674] Dunnigan (1992), p. 47

> [UK civil servant 2, observer]: "[UK civil servant 1]'s views do not necessarily reflect those of their employer."[675]

Although conveyed with a strong sense of humour (more on which in Section 7.3), UK civil servant 2's assertion nonetheless carries serious undertones. The game session took place at an unclassified academic conference and UK civil servant 1's participation in the game was not in an official representative capacity. The researcher's interpretation of the exchange was therefore that any statements should be taken as personal assertions and any inferences about the UK's intelligence capabilities are merely conjectures which are not endorsed by the UK Government.

Since the game session, information has become public to suggest UK civil servant 1's assertions had realistic grounding – Dutch intelligence agency AIVD had infiltrated and monitored the networks of Russian hacking group Cozy Bear since 2014.[676] Whether UK civil servant 1 was alluding to these operations cannot be known, but the example illustrates how the secrecy which permeates much of cyber security can be stifling for participants who have classification clearances but are unable to share their insights.

7.3 Humour as a pedagogical tool

Despite the seriousness of the subject matter in the game, the importance of humour to the conduct of game sessions and to creating learning moments should not be understated. The role of humour has been recognised in various pedagogical fields, for example Heather Baird and Nicky Lambert's study of nursing and midwifery education[677], or Phyllis Guthrie's analysis of teaching developmental readers.[678] These studies show that humour enables stronger participant engagement and lesson retention by bridging divisions between

[675] Author fieldnotes, 29 June 2017
[676] Modderkolk (2018)
[677] Baird and Lambert (2010)
[678] Guthrie (1999)

students themselves and between students and teachers, while also making participants emotionally identify with the subject matter.

No formal analysis of the role of humour exists in wargaming literature, in fact the word 'humour' does not appear at all in key books by Perla[679], Dunnigan[680], or Sabin[681], nor the authoritative anthology edited by Harrigan and Kirschenbaum.[682] This is perhaps a consequence of wargaming's historical roots as a military activity distanced from frivolity, but the topic has been given attention in other ludological fields, particularly video games. Claire Dormann and Robert Biddle, for instance, attest that humour 'enables the mediating process between player and object.'[683] Humour can help break down barriers between player and games, heightening immersion and engagement. A cautionary note, however, is provided by Ivan Lombardi who writes that 'excessively reiterated use of humour in teaching materials is very likely to interfere with the learning process itself, for humour has the tendency to monopolise the attention and being associated with frivolousness.'[684]

Because of the lack of treatment in wargaming literature, neither the methodological approach of the thesis nor design of the game consciously considered the use of humour (note the absence of this in Chapters IV and V). However, the game did incorporate a few humorous elements uncritically, mostly contained in the Event Cards. The Clumsy Civil Servant card exemplifies this (as seen in Chapter 4, Figure 9), using an image from the popular British sitcom *Yes, Minister* to invoke comedic associations. However, humour was not a design principle and it appeared sparingly in game components, striking the balance iterated by Lombardi largely by accident. The amount of fun and entertainment elicited by players, as outlined in Section 6.3.3, should therefore not necessarily be attributed to manufactured humour, but instead to the game's ludic qualities which encouraged players to create their own humour.

[679] Perla (1990)
[680] Dunnigan (1992)
[681] Sabin (2012)
[682] Harrigan and Kirschenbaum (2016)
[683] Dormann and Biddle (2006), p. 416
[684] Lombardi (2012), p. 154

Many instances of player-originated humour have been cited in previous chapters and sections, but these are only a small subset of all humour encountered during game sessions. The author's fieldnotes contain 38 notes labelled 'humour', but even this number is likely not a true reflection of the amount of jokes and humorous inferences made by players, given the shortcomings of the fieldnotes as discussed in Section 7.1.2. By way of meaningfully analysing players' use of humour we can employ lenses provided by Klaus Dodds and Philip Kirby, who suggest two interpretations: 'how humour makes the familiar seem fantastical', and 'the role of humour in satirising those in power.'[685]

7.3.1 Elevating mundanity through humour

When viewed through the lens of fantasticating familiarity, humour can be said to take a reality, sometimes mundane, and elevate it to something entertaining and engaging. In this way, jokes could be an important tool for players to convey a serious message by less serious means. Consider the following examples:

- One player suggested that the game needed a "potato harvest" Event Card for a Russian economic boom. The suggestion was made in jest but was grounded in the observation that in-game Russia was a lot poorer than its real-life counterpart.[686]
- GCHQ's poor cashflow was the butt of multiple jokes from both civilian and military players, with one player asserting "this is a familiar situation" when the in-game Entity was reduced to one Resource, having previously been well-off.[687] In reality GCHQ's finances are not available for public scrutiny, other than a budget for all UK's security services and intelligence agencies (also including MI5 and MI6) for 2016 which totalled £2.8 billion.[688] These humorous outbursts may therefore reveal players' frustration with GCHQ's funding.
- One German military player, in summarising the Russian team's strategy, noted their use of "General Winter" to launch Attacks at the beginning

[685] Dodds and Kirby (2013), p. 56
[686] Author fieldnotes, 29 June 2017
[687] Author fieldnotes, 8 May 2017; 29 June 2017
[688] HM Government (2016), p. 10

and end of the game, with quiet seasons in the intervening period.[689] This was a historically-aware joke, referring to Russia's strategic use of their harsh winters to resist and repel invaders (Sweden in 1708-09, France in 1812, Nazi Germany in the Second World War).

- When an observer in a game session with civilian industry participants asked how fake news could influence the Electorate, a player injected with "this is post-Brexit, they have already been influenced."[690] A similar joke was made in another session, where the Russian team admitted that their approach of targeting the Electorate was to "get at them through the Sun," referring to the tabloid newspaper.[691] These players were attuned to the contentious role of news media in subverting democratic processes.
- Finally, in a game session with military participants, a joke was made about PA Consulting being the new Universal Exports. PA Consulting is a real-life consultancy firm, while Universal Exports is a fictional company in the James Bond novels and films, serving as cover for the British Secret Service.[692] PA Consulting does serve the defence and security sector, but it is not clear if the joke was grounded in a reality inaccessible to the researcher (classified information).[693]

These remarks illustrate that humour could serve as an outlet for players to express views or provide insight about a range of issues without compromising themselves or the enjoyable environment created by the game. A discussion about the finer points of GCHQ's financing could certainly have been mundane, but through some well-timed wit the player referenced above made a sharp point without dragging the discussion towards dullness. Additionally, by turning reality into something fantastical, humour perhaps enabled some players to say things they otherwise could not have. Whatever business PA Consulting does with the UK intelligence community might not be public information, but a joke about this relationship may have provided a cathartic outlet to the utterer, whereas anyone

[689] Author fieldnotes, 24 January 2017
[690] Author fieldnotes, 30 March 2017
[691] Author fieldnotes, 29 June 2017
[692] James Bond Wiki website
[693] PA Consulting website

without inside knowledge would likely consider it to be based in fantasy. In other words, players could get away with saying things because they were just jokes.

7.3.2 Poking fun at Presidents

When viewed through the lens of satirising the powerful, humorous moments in game sessions often concerned overplaying individuals' characteristics and national stereotypes. The two most notable subjects of such satire were Presidents Vladimir Putin and Donald Trump. Players' discussions surrounding Putin and Trump were analysed in Sections 6.3.3 and 6.2.2, and 6.2.6 respectively, but they are worth revisiting to focus on the role of humour.

In real life, both Putin and Trump have engineered personas that set them apart from the political mainstream. Putin has carefully curated an image of masculinity, depicting himself as an avid outdoorsman and promoted his physical and sporting prowess.[694] Trump, meanwhile, built part of his 2016 election campaign on the slogan 'drain the swamp', emphasising his candidacy as an outsider to a corrupt and dysfunctional political system in Washington, and has not shied away from controversial outbursts, often using social media platform Twitter to attack opponents (and allies).[695] While evidently successful (both men are currently in power), in portraying themselves as different from the dull greyness of politics, they have also made themselves targets of lampooning. Through the Internet and the rise of 'meme culture', satirical and ridiculing images spread quickly, sometimes purely as humour but often with critical or subversive motives.[696] In the Russian context in particular, Anastasia Denisova has noted how the 'humorous and seemingly harmless form' of memes have been 'instrumental in overcoming censorship.'[697]

Memes about Putin and Trump have also proliferated offline, making their way into discussions during game sessions conducted for this thesis. One player, for

[694] CBS News
[695] BBC (2016)
[696] Zittrain (2014), p. 388
[697] Denisova (2017), pp. 979-980

example, joked about Putin riding bears[698] – a popular memetic adaptation of Putin horseback riding – while others mocked Trump's Twitter antics, suggesting him misspelling someone's name could have geopolitical ramifications (as referenced in Section 6.2.6). Humorous assertions of this nature also had more serious undertones. The player joking that "we know where your children live" (see Section 6.2.1) may have been referencing Putin's history as a KGB agent, and the player who placed Trump "right here" in the middle of the Russian side of the game board (see Section 6.2.6) was likely referencing the popular trope that Putin can influence or even control Trump.

As with the idea of fantasticating familiarity, where humour provided a veil behind which observations or criticisms could be made, so did humour enable players to make disparaging comments about world leaders without becoming embroiled in political debates. In this sense, humour might be considered a 'safety valve' by which political tension and frustration could be released in a harmless way.[699] The game environment encouraged players to make use of humour as a satirical outlet, allowing them to make useful contributions towards learning moments where knowledge was shared while enhancing their enjoyment of the game activity.

7.3.3 Using humour to engineer affective atmospheres

Despite humour originally not being a methodological or design consideration, as the fieldwork progressed, the researcher came to realise the important role of humour in player engagement and for eliciting learning moments. The researcher therefore adopted humour as a deliberate tactic when facilitating game sessions in order to engineer the affective atmospheres of the sessions. The concept of 'affective atmospheres' has primarily gained traction in human geography, where a seminal paper by Ben Anderson describes atmospheres (moods, feelings, ambiences, tones) as 'perpetually forming and deforming, appearing and disappearing, as bodies enter into relation with one another.'[700] Other

[698] Author fieldnotes, 24 March 2017
[699] Ziv (1988), p. 360
[700] Anderson (2009), p. 79

geographers have applied this concept to diverse subjects such as surveillance[701], passenger mobilities[702], and nationalism.[703] The idea that atmospheres could be 'engineered' was first suggested by Derek McCormack, who traced Salomon Andrée's 1897 balloon expedition from its use of technology to manipulate material atmospheres, to the effect the expedition had on public consciousness and perception.[704]

In the context of this thesis, engineering affective atmospheres refers to the researcher's attempts to set the tone of a game session, particularly through the use of humour to create a relaxed ambience and lighten the mood. For instance, when explaining the background to the game and why the game board is set out in the way it is, the researcher would say:

> "And on this side of the game board is Russia. Their setup mirrors that of the UK with the same five Entities. Now, I haven't read the Russian cyber security strategy, partly because it's classified and partly because I don't read Russian, but these five Entities nonetheless exist in their society, so it is fair to model it in this way."

Although not initially intended as humorous, the parts about the Russian cyber security strategy being classified and the researcher not being able to read the language almost always resulted in a ripple of laughter among players. As such, this spiel was repeated more or less verbatim every game session, thereby setting the tone from the outset.

Most humour which appeared in game sessions, either from the researcher or from players themselves, was successful, but sometimes the humour missed the mark. In his exploration of teacher strategies, Robert Stebbins writes that 'subjects and audience also define the humorous situation' and 'jokes may fall flat' if they do not take the audience into account.[705] A prime example of this occurring during the thesis was with the aforementioned *Yes, Minister* image; a

[701] Adey et al (2013)
[702] Bissell (2010)
[703] Closs Stephens (2016)
[704] McCormack (2008)
[705] Stebbins (2012), p. 91

reference which was lost on most non-British audiences. In addition to limited international airtime, it might also be said that *Yes, Minister* is quintessentially British, requiring an understanding of both Britishness and the quirks of the British civil service to fully appreciate. In a doctoral thesis examining the challenges of translating *Yes, Minister* into Catalan, Patrick Zabalbeascoa suggests four categories of humour in the show that are particularly difficult to translate: 'national-culture-&-institutions' jokes, 'national-sense-of-humour' jokes, 'language-dependent' jokes, and 'national-&-language-dependent' jokes [sic].[706] Given these challenges, it is perhaps understandable why non-British audiences failed to relate to the humour in the Event Card.

Overall, in this researcher's experience as a wargaming practitioner, the role of humour was of great importance and deserves further attention, both as a methodological consideration and in wargaming design and analysis.

Chapter 7 conclusion

Although this thesis has solid theoretical foundations, both within research methodology and within wargaming, it was to a large extent a practical endeavour. Having spent significant time out in the field as a wargaming practitioner, it would be remiss not to reflect on this experience, partly with a view to filling the void in wargaming literature identified in this chapter's introduction. The researcher's experiences allow some of the unspoken assumptions which seemingly underpin the practice of wargaming to be queried, or at least brought into the public domain for further debate. This chapter has contributed to the wargaming corpus in four main areas. Firstly, there is a lack of explanation in wargaming literature about how wargames occur and are organised. The starting point for much wargaming advice already assumes the existence of a 'sponsor' who has requested (and paid for) a game, and then proceeds to outline ways of designing or delivering the game to meet the sponsor's objectives (although as a notable exception, Downes-Martin has outlined cases where it would be useful to design a game which deceives the

[706] Zabalbeascoa (1993), pp. 322-325

sponsor[707]).[708] In reflecting on the researcher's experience of garnering interest in the game and arranging game sessions, this chapter has drawn on ethnographic literature which recognises both the role of serendipity (such as Pieke, cited in Section 7.1.1) and 'snowballing' (for example Sluka, cited in Section 7.1.1), while also taking into account the researcher's strategic positionality – personal, educational, and professional background – in shaping game deployment opportunities. In this way, one valuable contribution of this thesis can be considered its analysis of a stage of the wargaming process, what might be called a pre-sponsor stage, which is not widely covered in existing wargaming literature.

Secondly, issues around tactical positionality – the tensions between roles of designer, facilitator/adjudicator, and researcher – are not covered in wargaming literature from an experiential point of view. Ample warnings exist about how designers can become overzealous proponents of their games (Dunnigan, cited in Section 5.3.1) or the careful balance that researchers need to tread to simultaneously be close enough to observe a game but also not interfere in its progress (Wilhelmson and Svenson, and Kainikara, all cited in Section 5.4.2). However, other than to provide methodological advice, simply reading wargaming literature, even thick descriptions such as Holmes' (cited in Section 7.1.2), will not prepare a facilitator for the rigours of wargame facilitation. Here, the researcher's experiences, as recounted in Section 7.1.2, can be considered instructive. The researcher's experience of dealing with difficult players and awkward situations, for example, can be considered more insightful than generalised warnings such as that provided by Johnson (cited in Section 7.1.2). Similarly, in other fields, authors have not shied away from writing about physical and mental strains experienced in the field, and the researcher's contribution to wargaming on this topic might mirror that of Punch to ethnography (cited in Section 7.1.2).

In other ways, the researcher's experience corroborated literature advice regarding tactical positionality issues. Regarding notetaking analysed in Section 7.1.2, Hammersley and Atkinson's assertion (cited in Section 5.4.1) that the character of fieldnotes can change over time certainly rang true during this

[707] Downes-Martin (2016)
[708] Such as Weuve et al (2004), p. 13

thesis; consider the differences between the notes illustrated in Figure 18. Attempting to multitask by taking notes while facilitating games also proved wholly ineffective but could be remedied by either monotasking (take notes afterwards, as the researcher did), or having dedicated observers as most large professional games do (for example the Boeing game referenced in Section 5.4.1). Of the variety of challenges posed by game surroundings – physical, environmental, and atmospheric – the researcher encountered one example of an overbearing superior dramatically affecting the conduct of players. This experience provided evidence attesting to Wilhelmson and Svensson, and Burns' warnings that players can be stifled by the presence of superiors (cited in Section 5.3). In providing an experiential account of being a wargame practitioner, this thesis therefore provides a relatable contribution that goes beyond the generalised advice usually encountered in wargaming literature.

Thirdly, one of the problems the wargaming community is currently grappling with is how to wargame cyber security, operations, or warfare in unclassified environments. The researcher was present at a workshop session on this topic led by Downes-Martin at the 2018 Connections US conference in Washington DC, which led to some ideas for future progress.[709] However, a recurring theme (in this workshop and others at the same conference) was a fear of 'retroactive classification' – that games may become too close to reality that the government would classify them, despite only using unclassified information.[710] The experience of the researcher in conducting this thesis should be considered a positive sign in this regard. Despite encountering a few issues where classification denied access to potential game participants, or stifling what participants were able to contribute during game sessions, as analysed in Sections 7.2.1 and 7.2.2 respectively, overwhelmingly the results of the research have been successful. A game has been designed based only on unclassified information (Chapter 4), played only in unclassified settings, and generated many useful learning moments for players (Chapter 6). The wargaming community should therefore be encouraged about the possibility of wargaming cyber at unclassified levels.

[709] Downes-Martin (2018)
[710] Abel (2015), pp. 1038-1058

Finally, Perla and McGrady's article 'Why Wargaming Works' (cited in Section 2.2.5) has become the de-facto reference point for explaining how the 'story-living experience' makes wargames engaging. Others, such as Longley-Brown (referenced in Section 6.3.3), have added that fun is an important element to the success of wargames. What the wargaming literature lacks, however, but which has been recognised elsewhere, for example Guthrie in teaching or Dormann and Biddle in video games (both referenced in Section 7.3), is analysis of the role of humour. Using lenses provide by Dodds and Kirby (cited in Section 7.3), the researcher's experience showed that humour was a paramount tool for creating learning moments by elevating mundanity and satirising those in power. Furthermore, as a game facilitator, the researcher was able to use humour's affective qualities to engineer the atmosphere of game sessions, ensuring they were relaxed and conducive to discussion. Humour may not be suitable for every wargame, for example analytical decision-making games, but for games where the primary outcome is to generate engagement and discussion, the researcher's experience has demonstrated that humour should not be discounted as a pedagogic tool.

Overall, the researcher's experience as a wargaming practitioner was varied and challenging, but above all enjoyable. Despite the shortcomings of the literature, particularly in preparing for the trials and tribulations of the facilitator role, wargaming is an exceptionally rewarding activity because it entertains and enlightens players. For this research especially, being able to create real learning moments, as analysed in Chapter 6, made it meaningful and worthwhile to pursue. In overcoming the multitude of challenges explored in this chapter, the researcher has made a detailed and personal experiential contribution to the body of knowledge on wargaming practice.

Chapter 8: Conclusions

This thesis has explored the use of tabletop wargames for cyber security education. Cyber security has become a paramount challenge in modern societies at national, organisational, and personal levels. At the same time, cyber security is often viewed as a niche, perhaps even mysterious, field accessible only to computer scientists or technology enthusiasts. Wargaming, this thesis has posited, may be an effective way to introduce non-specialist people to key cyber security concepts and terminology in an interactive setting. The central thesis objectives were:

- *Create a wargame for cyber security education.*
- *Analyse the capacity for the game to create learning moments and enable players to share knowledge and ask the right questions.*
- *Reflect on the researcher's experience as a wargaming practitioner.*

By increasing awareness and understanding of cyber security, the barriers to engaging with the subject are lowered and the perception of cyber security is altered from a niche problem for technologists to solve, to one which everyone can contribute to. Ultimately, increased and more effective engagement with cyber security should result in increased awareness of cyber threats and adoption of mitigation tools and techniques, leading to more secure and resilient societies.

The primary means of investigation for the research was the creation of an original wargame based on the UK National Cyber Security Strategy (both 2011 and 2016 versions). The game pitted the UK against Russia, the most combative of the UK's near-peer adversaries. The two sides were divided into five Entities representing government, business, individuals (a core trinity found in the Strategy), military/intelligence, and critical national infrastructure. Players took control of these Entities to achieve conflicting Objectives using limited Resources at their disposal. The purpose of the game was to expose players to a wide range of cyber security concepts, from key actors in cyberspace and their relationships, to cyber attack and defence dynamics, to geopolitical realities. By fostering

discussion and debate around these topics, players would create learning moments, thereby addressing the central thesis objectives (see Chapter 4 for game design process and analysis).

The game was deployed to a range of organisations, from military establishments and government departments to private companies and academic institutions, both in the UK and abroad. Qualitative (and some quantitative) data was gathered, in the form of fieldnotes, about player discussions and their engagement with the game to determine its pedagogic efficacy. It has been found that the game was successful in stimulating debate about a multitude of cyber security topics; players were able to contribute their own knowledge of issues to enhance the understanding of other players. To a succinctly address the central thesis objective, it can be stated that the game successfully created many learning moments. But perhaps more importantly, the game fulfilled Peter Perla's assertion that the primary purpose of wargames is to help players 'ask the right questions' (cited in Section 2.3.3). Even if players did not come away from the game having learned concrete lessons, they were armed with knowledge that would help them learn lessons in the future (see Chapter 6 for game data analysis).

By way of summarising the results of the thesis, research findings are here discussed according to three themes: how the findings corroborated or diverged from wargaming literature, the key original contributions of the thesis and their importance, and some suggestions for the way ahead.

8.1 Research findings compared to the literature

Despite wargaming not being an academic discipline in and of itself, there is ample academic literature analysing wargames and their uses. This thesis has taken heed of this literature, including standard works in the field such as those from Perla and Dunnigan, and more specialised publications from the likes of Downes-Martin and Wilhelmson and Svensson. Being a highly practical research project, it has been possible to compare the theories expressed in the literature to the researcher's experience with wargaming. Most notably, this has manifested

itself in four ways: the story-living experience, the modifiability of manual games, realism versus complexity, and the difficulty of writing game rules.

8.1.1 Corroborating the story-living experience

One of the most critical features of wargaming that make them effective learning tools is that they provide participants with what Perla and McGrady called a 'story-living experience.'[711] Compared to more passive learning experiences, such as reading a book, watching a video, or taking an online course, wargames are highly interactive, forcing players to make decisions and experience the consequences of those decisions. In this way, wargames are a more experiential and therefore more impactful learning method.

The game designed for this thesis seems to have been successful in evoking such "story-living experiences" for players. For example, as remarked in Section 6.3.2, one player noted that it *felt* like the opposing team – in this case the UK – had been a democracy, given their long decision-making processes. The game was able to conjure a feeling as if the player had stepped into the shoes of a policymaker and experience decision-making from their point of view. This reinforces Perla and McGrady's assertion that wargames provide story-living experiences.

8.1.2 Corroborating the modifiability advantage of manual games

As lauded by Dunnigan, one of the advantages of manual games over computer games is their accessible mechanics, where rules, procedures, numbers, and probabilities are fully transparent to players.[712] This enables games to be easily modified, either by designers or players themselves, even while a game is being played. Moreover, where modifying a computer game would require coding and graphics skills, making modifications to a manual game requires no technical proficiencies, merely imagination (and perhaps some basic arts and crafts abilities).

[711] Perla and McGrady (2011), p. 112
[712] Dunningan (1992), pp. 64 and 174

During the course of this research, the modifiability advantage came to the fore numerous times. When the facilitator made a mistake, as detailed in Section 7.1.2, it was simple to rectify without interrupting the flow of the game. More prominently, the advantage of modifiability manifested itself in wizard wheezes. On two occasions, players made suggestions for new game components (Event Cards) which they felt would help the game more accurately represent the real world. Creating these components was a simple as writing the suggestions on pieces of paper and inserting them into the Event Card deck mid-game (illustrated in Figure 12). The ease with which these modifications were made could not be replicated in a computer game environment.

8.1.3 Corroborating the balance between realism and complexity

The tensions between realism and complexity, also characterised by Sabin in terms of accuracy versus simplicity or realism versus playability, must be tackled by every game designer.[713] The closer a game models the real world, the more realistic it is, but such realism also increases the complexity required to play the game. A more complex game may be able to impart more accurate lessons to players but may also require significantly more time to understand the game rules, thereby inhibiting participation.

The difficulty of balancing realism and complexity was encountered multiple times during the game design process of the research. It can be seen, for instance, in the development of the combat results table (Section 4.4.4) which started out based on a very simple formula but ended up being expanded into a more nuanced table representing real-world risk and reward payoffs. The final version of the combat results table (Figure 11) has 36 possible results, whereas the first version (Figure 10) only had 16. A more realistic game would likely have an even larger matrix, such as the 360 possible outcomes for calculating casualties in George Gush's set of rules for wargames covering the fifteenth to seventeenth centuries.[714] The game designed for this thesis was therefore relatively simple (by an order of

[713] Sabin (2012), p. 19
[714] Gush (1979), p. 46

magnitude compared to Gush), but this was a conscious decision made to encourage playability rather than attempt to accurately model the real world.

8.1.4 Game rules are not easy to write

As elaborated in the game design process (Section 4.1.1), a decision was made to limit the length of the game rules, erring on the side of simplicity and playability over complexity and realism. The justification for this was that the researcher wanted to maximise the time players spent engaging with the thematic cyber security content of the game, rather than grapple with the game mechanics. The rules were capped at one double-sided A4 page, which players would be able to read in ten minutes, minimising the time spent not interacting with the main game material. For comparison, the latest rules for *World in Flames* amount to 88 pages, not including campaign guides and additional spreadsheets for game setup.[715]

Despite a relatively short rule set (by wargaming standards), moments of friction between players and rules were encountered during game sessions. Particularly at the beginning of game sessions, players often asked clarifying questions or attempted to do Actions prohibited by the game rules, suggesting the rules were not as simple as intended. Jim Wallman, cited in Section 6.3.1, has opined that writing wargame rules is easy, yet the experience of the researcher contradicts this. Writing game rules is by no means easy, especially when constrained by length and targeting a generalist non-gaming audience. On this point, the findings of the research therefore diverge from the view in the literature.

8.2 Novel takeaways for wargamers

As a contribution to the wargaming corpus, in addition to comparing findings to extant literature, this thesis generated two pieces of evidence of potential value to wargamers (and others) seeking to delve into the field of cyber wargaming. In merging distant literature and creating a catalogue of best-practice in cyber

[715] Australian Design Group (2018)

wargame design, the thesis has created resources that wargamers can draw on both for justifying their choice of manual games and for guiding design choices when developing cyber games.

8.2.1 Merging distant literature

Astute observers may query the decision to use a manual game over a computer game, especially considering that the subject matter may seemingly closer fit a digitised environment – after all, the cyber domain would not exist without computers. Extant wargaming literature already makes a compelling case why manual games hold many advantages over computer games (see Section 2.2.1), but by consulting literature from other fields, this thesis has been able to strengthen these claims.

Research in computer science, specifically interface design and human-computer interaction, has shown paper prototyping and scenarios were equally or more effective than computerised methods for generating ideas in the early stages of systems development (see Section 2.3.1). To generalise these findings, it can be said that low-fidelity tools are effective for promoting high-level thinking. This is something which wargamers have been cognisant of for decades, perhaps even centuries, but which can now be backed with data from "hard" science. Studies merging wargaming with computer science literature have not been done before and therefore constitutes useful evidence for wargamers who seek to justify the use of manual games over computer games.

8.2.2 A catalogue for best-practice in cyber games design

Although this thesis is inspired by a dearth of cyber wargames, some games in this genre do exist, and a comprehensive review was conducted in Chapter 3. The analysis evaluated the design of the games as well as their pedagogic potential, seeking to ascertain what constitutes best practice in the field which other designers should take heed of. Across games that varied hugely by style and quality, some aspects appeared recurrently in the best games: including ludic

components, having an adversarial nature, utilising cards, simulating unpredictability, and marketplaces.

The value of this chapter to the wargaming community is in critiquing key cyber games to establish a catalogue of best practice in cyber game design. Although the website boardgamegeek.com is a sprawling repository of games, it is not necessarily always an informative source for theme-specific design principles. The results when searching for "cyber", for example, includes the game *Scooby-Doo! Cyber chase*, which is of no relevance to people interested in wargames or educational games.[716] From the researcher's experience, especially at the Connections US 2018 conference, other wargamers are not always aware of existing games in the field, and the catalogue of best practice provided in this thesis therefore serves as a reference point which can be consulted and learned from.

8.3 Key original contributions of the research

The thesis can be said to have made three original contributions to the field of cyber wargaming: developing a novel game, relating a practitioner's experience, and positive answering the central thesis question. These were summarised in Section 1.5 but are worth restating for readers who have skipped to the end or struggle to recall what they read some 250 pages ago.

8.3.1 Development of a novel cyber wargame

Given the dearth of educational cyber wargames, especially looking at cyber security from a strategic national policymaking angle, this thesis presented an opportunity to create a new game to fill this void. The game design analysis conducted in Chapter 4 took into account many of the standard challenges faced by wargame designers, including gameplay phases, visibility, victory conditions, and the aforementioned balance between realism and complexity. Moreover, these challenges were discussed with regards to cyber security concepts which

[716] BoardGameGeek listing for *Scooby-doo! Cyber chase*

were designed into the game in order to elicit learning moments from players. The game design therefore drew not only on wargaming literature, but also cyber security literature to ensure game components and mechanics could be related to the real world.

Unlike other games in the genre, such as *[d0x3d!]* which is based on *Forbidden Island* (see Section 3.1.1), the game designed for this thesis was created from scratch. Although it borrowed concepts from other games, such as *Privacy*'s event cards or *Decisions & Disruptions*' marketplace (Sections 3.4 and 3.5 respectively), every game component was original, and many were entirely unique. The game artefact itself therefore constitutes an original contribution to cyber wargaming.

8.3.2 A wargaming practitioner's experience

Existing wargaming literature is largely written by wargamers for wargamers. That is to say, there is ample material presenting new game ideas or describing how a game has been used, but there is very little critical reflection on the practice of wargaming. A novice reading the standard textbook works from Perla and Dunnigan would not learn much about what it is like to run wargames, and it is the researcher's impression that much of wargaming practice is based on unwritten assumptions in the wargaming community.

In Chapter 7, the researcher sought to challenge, or at least bring attention to, some of these assumptions by relating their experiences as a wargaming practitioner. By analysing the process by which game sessions were organised, including the important element of serendipity, it has been possible to shed light on what might be called the pre-sponsor stage in wargame deployment. Subsequently, the physically and mentally taxing nature of facilitating wargames was exposed through candid reflection on the researcher's experience in running game sessions. Since wargaming literature is largely devoid of such experiential accounts, the researcher's contributions should be considered both original and valuable.

8.3.3 Addressing the central thesis objective

Perhaps the most crucial contribution of the research is in positively addressing the central thesis objective: the game *did* create learning moments where players could share knowledge and were enabled to ask the right questions. These moments were outlined in Chapter 6 and broadly aligned with the intended game design, including key actors in cyberspace and their relationships, cyber attack and defence dynamics, and geopolitical realities. However, because of the flexibility of the game (another advantage of manual gaming, as per Section 2.2.6), unintended learning moments were also achieved, for example regarding the rivalry between India and Pakistan, password guidance, and President Donald Trump. What players can learn from a game for cyber security education and awareness training therefore depends on what lessons are designed into the game and what opportunities the game makes for player contributions. In this thesis, the game had a wide variety of lessons built in and offered ample scope for players to provide their own input.

In addition to enabling cyber security learning moments, the game also proved to be an effective pedagogical tool. Players exhibited very high engagement behaviours during game sessions, including emotive reactions, role playing, humour, and a sense of fun – all of which lays strong foundations for pedagogic retention. Whilst this is not in itself an original claim, the wealth of data used to back it up far supersedes previous studies; Rieb and Lechner only ran *Operation Digital Chameleon* once[717], Frey et al played *Decisions & Disruptions* with 43 participants[718], while Barnard-Wills and Ashenden tested *Privacy* with 130 players – this research had over 250 participants across 33 very varied game sessions.[719] The research therefore shows, with greater weight of evidence than previously published, that wargames should be part of the toolkit for cyber security educators.

[717] Rieb and Lechner (2016), p. 8
[718] Frey et al (2017), p. 9
[719] Barnard-Wills and Ashenden (2015), p. 153

8.4 The way ahead

No research endeavour is ever complete and can always be further refined, developed, or extended. This research is no different and two avenues for future work are suggested herein. First, there is scope to make a computerised or hybrid version of the game. As discussed in Section 6.3.4, some players with technical nous already suggested this approach and even offered to make digital versions of the game. The researcher is of course cognisant that computerising the game would forego many of the advantages of manual gaming, but at the same time computers offer capabilities that could enhance the game in certain ways. As an example, a computer could easily keep track of scores and game histories, enabling deeper analysis of quantitative data. Additionally, one of the main shortcomings of the game was its lacklustre representation of attribution because players had complete visibility of the game board. Digital games offer more options for manipulating graphics including hiding information or parts of the game board. By computerising the game designed for this thesis, new modes of play could be created to achieve a greater range of learning moments.

Second, a public version of the game should be produced. Every game component is available in Chapter 4 and Appendices A and B, but it would be difficult to piece these together into a complete product. Given that the game is both engaging and useful, it would be a shame if the game, as an artefact, was lost at the completion of the research. Instead, it would be more valuable to produce a distributable version of the game and making this available in an online repository together with instructions for running a successful game session. Interested parties could simply download all the material and print their own copy of the game to be used as they see fit, perhaps even modified for specific contexts and depending on the learning moments desired. Since this research is publicly funded this material could be provided free of charge, or for a small contribution towards upkeep of the online repository. In this way, the successes of the game do not stop with the research but continue with the wargaming community.

Wherever the game ends up, even if it does not spread beyond this thesis, the researcher is confident that wargaming is an effective tool for cyber security

education and awareness training, and the work presented herein has had a tangible impact on the participants who contributed to it.

Appendices

Appendix A: Player Dossiers

UK Government

Cyber Security Wargame Dossier

UK Government

Player overview

You are playing the UK Government.

The Government plays a central role in the exercise. It is the point to which all new resources flow at the beginning on each turn, and you are therefore responsible to doling these out to the other Entities on your team. The Government is also directly connected to all other Entities, so is any damage you sustain will reverberate across your entire team. Likewise, any damage taken elsewhere will also impact you.

You may have the possibility of opening one attack vector, targeting Russian Government. This reflects the UK's stature in international organisations and its economic power, through a combination of which you can mount attacks that damage the vitality of the Russian Government. This would be a one-way vector, so you cannot be retaliated against in this way.

Player objectives

You have two main objectives:

1. Election time – buy popular support ahead of 2021 elections by making sure the people prosper.
   +1 Victory Point for every month Electorate ends with 4 or more Resource

2. Aggressive outlook – drive home a strong anti-Russia rhetoric.
   +5 Victory Points if Russia Government ends the game with less Vitality than it started (4).

Cyber Security Wargame Dossier

Electorate

Player overview

You are playing the Electorate.

The Electorate represents the people of the UK. According to the UK Cyber Security Strategy, the people are one of the key constituents (along with government and business) ensuring the UK's prosperity and security in cyberspace. You are responsible for holding the Government accountable for their actions, as well as maintaining your current quality of life, which largely depends on keeping the UK's critical infrastructure intact. You may therefore want to balance your demands of the Government with recognition that they have other priorities.

Although you have no outgoing attack vectors, you may be subject to direct attack from Russian Online trolls, seeking to undermine political, cultural, and social cohesion.

Player objectives

You have one main objective:

1. Resist the drain – avoid having your wealth taken away from you.
   -1 Victory Point every time Resource is transferred away from Electorate.

Cyber Security Wargame Dossier

UK Plc

Player overview

You are playing UK Plc.

UK Plc represents UK businesses, which in the UK Cyber Security Strategy, along with government and people, form the key components of the UK's prosperity and security in cyberspace. Your interest lies not only in growing your business, but also in supporting the military and intelligence apparatus with your products and expertise.

Although you have no outgoing attack vectors, you may come under direct attack from Energetic Bear conducting commercial espionage.

Player objectives

You have one main objective:

1. Weather the Brexit storm – build a cash flow buffer to deal with Brexit uncertainties
   +2 Victory Points for 3 or more Resource at the end of April
   +3 Victory Points for 6 or more Resource at the end of August
   +4 Victory Points for 9 or more Resource at the end of December
   (Cumulative)

Cyber Security Wargame Dossier

GCHQ

Player overview

You are playing GCHQ.

GCHQ represents the UK military and intelligence communities. You are supporting the UK's offensive cyberspace operations. In this role, your primary aim is to ensure the UK's superiority in cyber capabilities, while denying those capabilities to your adversaries.

Player objectives

You have one main objective:

2. Recruitment drive – swell your staff numbers by increasing Vitality every quarter (end of March, June, September and December).
   +1 Victory Point for single quarters
   +3 Victory Points for two consecutive quarters
   +5 Victory Points for three consecutive quarters
   +7 Victory Points for the entire year
   (Not cumulative)

Cyber Security Wargame Dossier

UK Energy

Player overview

You are playing UK Energy.

UK Energy is one of Britain's largest energy providers. It produces electricity from a range of sources, including coal, gas, solar, wind, and nuclear. In this last regard it plays a pivotal role as the sole operator of nuclear power plants in the UK, spread over seven locations, generating about one sixth of the UK's electricity. You must ensure this critical function is maintained by not only keeping up the production of energy, but also keeping your main customer – the Electorate – a viable market by guaranteeing its electricity supply.

Player objectives

You have one main objective:

1. Grow capacity – increase the energy output of your power plants.
   +2 Victory Points if you have 6 or more Vitality at the end of June
   +3 Victory Points if you have 9 or more Vitality at the end of December

Cyber Security Wargame Dossier

Russia Government

Player overview

You are playing the Russian Government.

The Government plays a central role in the exercise. It is the point to which all new resources flow at the beginning on each turn, and you are therefore responsible for doling these out to the other Entities on your team. The Government is also directly connected to all other Entities, so any damage you sustain will reverberate across your entire team. Likewise, any damage taken elsewhere will also impact you.

You have no outgoing attack vectors, but may be directly attacked by the UK Government if such a vector is open. This reflects a greater economic and diplomatic clout enjoyed by the UK.

Player objectives

You have two main objectives:

1. Some animals are more equal than others – keep a slice of your income for yourself.
   +1 Victory Point every month you end with 3 or more Resource

2. Control the Trolls – don't let the trolls get overconfident.
   -1 Victory Point every time Online Trolls launch a 3 or 4 Resource attack
   -2 Victory Points every time Online Trolls launch a 5 or 6 Resource attack

Cyber Security Wargame Dossier

Online trolls

Player overview

You are playing Online trolls.

Russia is well-known for employing an army of online trolls to run honey pot social media accounts, propagate pro-Russian news, and make inflammatory comments on news stories and message boards. The role of the trolls is to undermine the UK people's confidence in their government and shift negative attention away from Russia.

You have one outgoing attack vector targeting the UK Electorate through which you can mount direct attacks.

Player objectives

You have one main objective:

1. Success breeds confidence – small-scale harassment is beneath your capabilities.
   +4 Victory Points every time you launch an attack with 3 or more Resource and the Ransomware asset.

Cyber Security Wargame Dossier

Energetic Bear

Player overview

You are playing Energetic Bear.

The use of the Internet for industrial espionage has become part and parcel of offensive cyber operations, and Russia is no exception to this. Energetic Bear is the code name for one of the many espionage groups that seek to further Russian business prosperity at the expense of the UK's.

You have one outgoing attack vector targeting UK Plc with which you can launch direct attacks.

Player objectives

You have one main objective:

2. Those who can't, steal – grow your business by whatever means possible.
   +1 Victory Point for having more Vitality at the end of April than the start of the game
   +3 Victory Points for having more Vitality at the end of August than April
   +5 Victory Points for having more Vitality at the end of December than August
   (Cumulative)

Cyber Security Wargame Dossier

Special Communications Service (SCS)

Player overview

You are playing the Special Communications Service (SCS).

The SCS is responsible for signals intelligence, communications security, and cryptology. You are supporting Russia's offensive cyberspace operations. In this role, your primary aim is to ensure Russia's superiority in cyber capabilities, while denying those capabilities to your adversaries.

Player objectives

You have one main objective:

2. Win the arms race – have a better cyber arsenal than the UK.
   +2 Victory Points every month you end with more Attack assets than the UK's defence assets

Cyber Security Wargame Dossier

Rosenergoatom

Player overview

You are playing Rosenergoatom.

Rosenergoatom is Russia's nuclear power stations operator. The organisation is responsible for running 10 nuclear power plants, a number which is planned to expand drastically. You must ensure this critical function is maintained, while also preparing for expansion.

Player objectives

You have one main objective:

1. Grow capacity – increase the energy output of your power plants by growing Vitality every quarter (end of March, June, September and December)
   +1 Victory Point for single quarters
   +3 Victory Points for any two consecutive quarters
   +5 Victory Points for three consecutive quarters
   +7 Victory Points for the entire year
   (Not cumulative)

Appendix B: Game Rules

Setup:

The game pits two sides, the UK and Russia, against each other. Each side is divided into five Entities:

UK	Russia
Government	Government
Electorate	Online Trolls
UK Plc	Energetic Bear
GCHQ	Special Communications Service
UK Energy	Rosenergoatom

Each Entity has two sets of counters it must manage: Resource (yellow, representing wealth) and Vitality (blue, representing well-being).

Rules of play:

Basics:

How to win the game:

- Earn more Victory Points than the opposing team.

How the game is played:

- The game lasts 12 turns: January-December 2020.
  - A turn consists of one team performing Actions with all their Entities, after which the other team performs Actions with all their Entities.
- Each turn, each Entity may perform one of five courses of Action:
  - Distribute: transfer Resource to any single connected Entity
  - Revitalise: spend Resource to gain Vitality
  - Attack: spend Resource to attack along an attack vector
    - Note: Teams may not attack in January
  - (GCHQ/SCS ONLY) Access Black Market: bid on black market goods
  - Abstain: do nothing this turn

Details:

Turns:

- At the start of every Month a card is drawn from the Event Cards pile and its effects implemented immediately.
- At the start of each team's turn, the Government Entity is granted 3 Resource.
- There is a time limit of 3 minutes per team each turn. Any actions not performed within this limit are forfeited.
- At the end of each turn, teams must fill in their respective Record Keeping Sheets.

Distribute:

- Resources can be transferred between Entities connected by thin black lines.
- Arrows denote one-way transfer relationships.
- The maximum number of Resource that can be transferred in one Action is 5.
- There is no limit on how much Resource an Entity can possess.

Revitalise:

- Cost of Vitality goes up with the amount converted:

Vitality	Cost (Resource)
1	1
2	2
3	4
4	5
5	6
6	7

- There is no limit on how much Vitality an Entity can possess.

Attack:

- An Entity can attack along the attack vector attached to it – purple for UK, orange for Russia.
- The attacking Entity must spend Resource to perform at attack: minimum 1, maximum 6.

- The attack result is calculated by rolling one six-sided die and consulting the Combat Resolution table below.
    - In the event of a negative result, the attack backfires and the attacker suffers damage to their own Vitality.
- Additionally, such a poorly executed attack can be **attributed** by the defender to the attacker, with repercussions detailed in the Attribution table below.

		Die Roll					
		1	2	3	4	5	6
Resource spent	1	0	1	1	1	1	2
	2	0	1	1	1	2	2
	3	-1	0	1	2	2	3
	4	-1	0	1	2	3	4
	5	-2	-1	2	3	3	4
	6	-2	-1	0	3	5	6

		Attribution Level	
		-1	-2
Attacking Entity	Energetic Bear	UK gains Software Update asset.	UK gains Software Update and Recovery Management assets.
	Online Trolls	UK gains Education asset.	UK gains Education asset, Online Trolls cannot launch attacks for 2 turns.
	SCS	UK gains Software Update asset, SCS cannot bid on Black Market for 2 turns.	UK may choose to open up GCHQ-Rosenergoatom or UK Government-Russia Government attack vector at no cost.
	GCHQ	GCHQ cannot launch attacks for 2 turns.	GCHQ cannot perform any actions for 2 turns, UK Government loses 1 Vitality.
	UK Government	Russia gains Bargaining Chip asset.	Russia gains Bargaining Chip asset, UK Government lose additional 2 Vitality and 2 Resource.

- **Residual damage** is also suffered by any Entities directly connected to the damaged Entity.
    - This is calculated in the ratio of 1:2.
    - This also applies to backfire damage.

Access Black Market:

- GCHQ or SCS can spend Resource they have to bid on items in the Black Market.
    - If a team bids on an item and the other team does not increase on that bid in their immediately following turn, the bid winner receives the item on their subsequent turn.
    - Multiple items can be bid on in one turn.
    - It is an all-pay auction, meaning Resource used for all bids is considered spent – losing bids do not get refunded and do not count towards subsequent re-bids.
- Items can be hoarded for later use or played with immediate effect.
- All items can be bought by either team.

End of game:

- If an attack results in any Entity being reduced to 0 Vitality, the attacker is awarded 10 Victory Points and the game immediately ends.
    - Remaining Victory Points up to that point are tallied up after full effects of attack have been finalised (i.e. residual damage).
- Note: It is possible to launch a successful game-ending attack and still lose the game.
  At the end of December each team states their Objectives and Victory Points are tallied up. The team with the most Victory Points is declared the winner.

Appendix C: Game Sessions

This appendix lists all 33 game sessions which were used for data collection for the thesis, including information about session types, settings, participants, and game results. Note that some records are incomplete as the relevant data was not collected or changes were made to the methodology; for example, game results using early versions of the game are not included because the game used different rules, so the results are not comparable. Indeed, all sessions using earlier versions of the game were effectively playtest sessions which often resulted in major changes to game design (as elaborated in Chapter 4), whereas the design remained stable once the final version was produced. Nonetheless, qualitative data was collected from the earlier sessions which informed the analysis in Chapter 6.

Session name	Description	Type	Sub-type	Setting	Male	Female	Result	UK score	Russia score
UK technology company A1	Large computer technology company with global presence, players from a variety of technical and business roles.	Civilian	Industry	Boardroom	7	1			

UK academics A1	University, players from postgraduate social science courses.	Civilian	Academia	Office	3	1			
UK academics A2	University, players from postgraduate technical courses.	Civilian	Academia	Office					
International Academics A	International education programme hosted at a UK military education institution, Indian players from senior roles in government and industry.	Civilian	Mix	Classroom	5	1			
Connections UK 2016 1	Conference for the UK wargaming community hosted at King's College London, players from a range of backgrounds.	Civilian	Mix	Large room	5	1			

Connections UK 2016 2	Conference for the UK wargaming community hosted at King's College London, players from a range of backgrounds.	Civilian	Mix	Large room	6	0			
UK media company A + UK government department A	Small interactive media company and a central government department, players from industry and technical civil service roles.	Civilian	Mix	Meeting room	4	2			
UK academics A3	University, players from postgraduate social science courses.	Civilian	Academia	Meeting room	4	2			
UK government department B	Central government department, players from policy roles.	Civilian	Civil Service	Meeting room	3	1	UK win	10	5

UK academics A4	University, players from technical postgraduate courses.	Civilian	Academia	Meeting room	6	2	Russia win	-2	3
German military education institution A1	Officer training institution, players at OF-2 to OF-4 grades from all service branches.	Military		Classroom	7	1	Russia win	15	17
German military education institution A2	Officer training institution, players at OF-2 to OF-4 grades from all service branches.	Military		Classroom	8	0	UK win	19	16
Swedish military education institution A1	Officer training institution, players from a range of military and government roles.	Mix		Officers' mess	9	1	UK win	32	14

Swedish military education institution A2	Officer training institution, players from a range of military and government roles.	Mix		Officers' mess	5	3	UK win	21	12
UK technology company B	Large technology and engineering company with strong ties to defence, players from a range of business roles.	Civilian	Industry	Meeting room	4	0	Russia win	22	26
UK military education institution A	Specialist training school for all ranks, players at OF-2 to OF-3 grades from multiple service branches.	Military		Office	4	2	UK win	22	16
UK academics B	University, undergraduate players from technical courses.	Civilian	Academia	Classroom	8	2	Russia win	11	29

UK technology company A2	Large computer technology company with global presence, participants from a variety of technical and business roles.	Civilian	Industry	Meeting room	7	2	UK win	34	30
International academics B	International education programme hosted at a UK military education institution, Indian players from senior roles in government and industry.	Civilian	Mix	Classroom	6	1	Russia win	13	17
UK government department C	Central government department, participants from policy and procurement roles.	Civilian	Civil Service	Meeting room	5	3	(No gameplay, discussion only)		

CDT Advisory Panel	Internal Royal Holloway conference, players from central government, industry, and academia.	Civilian	Mix	Bar	5	2	UK win	4	3
International military education institution A1	Specialist training institution for officers and senior government representatives, players from OF-2 to OF-4 grades, policy, and analyst roles.	Mix		Classroom	7	3	UK win	36	31
International military education institution A2	Specialist training institution for officers and senior government representatives, players from OF-2 to	Mix		Classroom	10	0	UK win	29	13

	OF-4 grades, policy, and analyst roles.								
International military education institution A3	Specialist training institution for officers and senior government representatives, players from OF-2 to OF-4 grades, policy, and analyst roles.	Mix		Classroom	9	1	UK win	47	18
UK military education institution B1	Officer training institution, players from OF-2 to OF-4 grades.	Military		Office	6	0	Russia win	14	19
UK military education institution B2	Officer training institution, players from OF-2 to OF-4 grades.	Military		Classroom	14	1	Russia win	7	23

ACE-CSR conference	Conference for UK academic cyber security community, players from academic, industry, and central government roles.	Civilian	Mix	Classroom	6	4	Tie	22	22
Connections UK 2017 1	Conference for the UK wargaming community hosted at King's College London, players from a range of backgrounds.	Civilian	Mix	Large room	6	2	Russia win	27	31
Connections UK 2017 2	Conference for the UK wargaming community hosted at King's College London, players from a range of backgrounds.	Civilian	Mix	Large room	4	2	Russia win	25	28

International military education institution A4*	Specialist training institution for officers and senior government representatives, players from OF-2 to OF-4 grades, policy, and analyst roles.	Mix		Classroom	9	1	Russia win	7	28
International military education institution A5*	Specialist training institution for officers and senior government representatives, players from OF-2 to OF-4 grades, policy, and analyst roles.	Mix		Classroom	9	0	Russia win	10	18
International military education institution A6*	Specialist training institution for officers and senior government representatives,	Mix		Classroom	9	1	UK win	26	14

	players from OF-2 to OF-4 grades, policy, and analyst roles.								
Australian professional services firm	Large firm with global presence, players from a range of business roles.	Civilian	Industry	Boardroom	6	4	Tie	16	16
CyCon Conference 1-6	International cyber security conference, players from a range of government, industry, and academic roles.	Civilian	Mix	Large room	(Not formally recorded as these six sessions were not officially part of the field work and are not included in the total of 33 sessions)				

*Game sessions conducted in author's absence

Bibliography

[d0x3d!] (http://d0x3d.com/d0x3d/about.html)

Abel, Johnathan, 'Do You Have to Keep the Government's Secrets – Retroactively Classified Documents, the First Amendment, and the Power to Make Secrets out of the Public Record', *University of Pennsylvania Law Review*, Vol. 163, Issue 4 (March 2015), pp. 1037-1098

Abuhamdeh, Sami and Mihaly Csikszentmihalyi, 'Attentional involvement and intrinsic motivation', *Motivation and Emotion*, Vol. 36, Issue 3 (September 2012), pp. 257-267

Adair, Bill, 'Did the Army Get Out-Gamed?', in *Tampa Bay Times*, 20/02/2005 (available at http://www.sptimes.com/2005/02/20/Worldandnation/Did_the_Army_get_out_.shtml)

Adams, Eldridge S. and Michael Mesterton-Gibbons, 'Lanchester's attrition models and fights among social animals', *Behavioural Ecology*, Vol. 14, No. 5 (2003), pp. 719-723

Adams, Vincanne, Michelle Murphy and Adele E. Clarke, 'Anticipation: Technoscience, life, affect, temporality', *Subjectivity*, Issue 8 (2009), pp. 246-265

Adey, Peter, Laure Brayer, Damien Masson, Patrick Murphy, Paul Simpson and Nicolas Tixier, '"Pour votre transquillité": Ambiance, atmosphere, and surveillance', *Geoforum*, Vol. 49 (October 2013), pp. 299-309

Aesir, post on *Fantasy Grounds* online forum, 15 February 2005 (https://www.fantasygrounds.com/forums/showthread.php?2723-Dice-rolling-sounds)

Alam, Ian, 'Fieldwork and data collection in qualitative marketing research', *Qualitative Market Research: An International Journal*, Vol. 8, Issue 1 (2005), pp. 97-112

Allianz, 'Allianz Risk Barometer: Top Business Risks for 2018' (2018)

Ananthaswamy, Anil, 'Chinese satellite beats distance record for quantum entanglement', *New Scientist*, 15 June 2017 (https://www.newscientist.com/article/2134843-chinese-satellite-beats-distance-record-for-quantum-entanglement/)

Anderson, Ben, 'Security and the future: Anticipating the event of terror', *Geoforum*, 41 (2010), pp. 227-235

Applegate, Scott D., 'The Principle of Maneuver in Cyber Operations', in C. Czosseck, R. Ottis and K. Ziolkowski, eds., proceedings of the 4th International Conference on Cyber Conflict, 2012 (NATO CCD COE: Tallinn), pp. 183-195

Arce, Ivan, 'The Weakest Link Revisited', *IEEE Security & Privacy*, March/April 2003, pp. 72-75

Aristotle (2004), *The Nicomachean Ethics*, trans. J. A. K. Thompson, 3rd ed. (Penguin: London)

Association for Finance Professionals, '2018 AFP Risk Survey Report' (2018)

Australian Design Group, 'World in Flames Collector's Edition Living Rules', 17 July 2018 (https://cdn.shopify.com/s/files/1/0714/3419/files/WiF_CE_Rules_17_Jul_2018.pdf?5855005331441860712)

Axelrod, Robert and Rumen Illiev, 'Timing of cyber conflict', *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 111, No. 4 (January 2014), pp. 1298-1303

Bagley, Tennent H. (2007), *Spy Wars – moles, mysteries, and deadly games* (Yale University Press: New Haven, CT)

Baird, Heather and Nicky Lambert, 'Enjoyable learning: The role of humour, games, and fun activities in nursing and midwifery education', *Nurse Education Today*, Vol. 30 (2010), pp. 548-552

Baker, Peter and Andrew Morgan, 'Resilience of the Food Supply to Port Disruption', DEFRA Project FO0108, Final Report, September 2012

Barbara, Jonathan, 'Measuring User Experience in Multiplayer Board Games', Games and Culture, Vol. 12, Issue 7-8 (2015), pp. 623-649

Barlow, John Perry, 'A Declaration of Independence of Cyberspace', 8 February 1996 (https://www.eff.org/cyberspace-independence)

Barnard-Wills, David and Debi Ashenden, 'Playing with Privacy: Games for Education and Communication in the Politics of Online Privacy', *Political Studies*, Vol. 63, Issue 1, 2015, pp. 142-160

Bartels, Elizabeth, Margaret McCrown and Timothy Wilkie, 'Designing Peace and Conflict Exercises: Level of Analysis, Scenario, and Role Specification', *Simulation & Gaming*, Vol. 44, Issue 1 (2012), pp. 36-50

Bartels, Elizabeth M., 'Inhabited Models and Irregular Warfare Games: An Approach to Educational and Analytic Gaming at the US Department of Defense', in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge), pp. 503-512

Barzashka, Ivanka, 'Designing a Missile Defence and Nuclear Risk Strategic Decision Game', presentation given at Connections UK 2017 conference, King's College London, London, UK, 7 September 2017 (http://www.professionalwargaming.co.uk/MissileDefenceWargame.pdf)

Baumeister, Roy F., Kathleen D. Vohs, C. Nathan DeWall, Liqing Zhang, 'How Emotion Shapes Behavior: Feedback, Anticipation, and Reflection, Rather Than Direct Causation', *Personality and Social Psychology Review*, Vol. 11, No. 2 (2007), pp. 167-203

BBC News, 'Previous cases of missing data', 25 May 2009 (http://news.bbc.co.uk/1/hi/uk/7449927.stm)

BBC, '"Cyber war games" to be staged by UK and US', 16 January 2015 (http://www.bbc.co.uk/news/uk-politics-30842669)

BBC, 'Hacker group Anonymous declares war on Orlando, Florida', 28 June 2011 (https://www.bbc.com/news/world-us-canada-13952864)

BBC, 'How might Trump "drain the swamp"?', 18 October 2016 (https://www.bbc.com/news/election-us-2016-37699073)

Beaumont, Roger, 'Maskirovka: Soviet Camouflage, Concealment and Deception', Stratech Studies SS82-1 (November 1982)

Becker, Katrin, 'Studying Commercial Games: Justifying Choices', *Journal of Game Design and Development Education*, Issue 1 (2011), pp. 48-53

Bedwell, Lance E., 'Developing Environmental Education Games', *The American Biology Teacher*, Vol. 39, No. 3 (March 1977), pp. 176-177, 192

Berenstein, Daniel, Johannes Buchmann and Erik Dahmen (2009), *Introduction to post-quantum cryptography* (Springer)

Berreman, Gerald D., 'Ethics versus "Realism" in Anthropology', in Antonious C. G. M. Robben and Jeffrey A. Sluka, eds. (2012), *Ethnographic Fieldwork: An Anthropological Reader*, 2nd ed. (John Wiley & Sons: Chichester), pp. 331-352

Berry Bertram, Kerry, 'The Sea Ice Board Game', *Science Scope*, Vol. 32, No. 2, Earth Materials, Features, and Processes (October 2008), pp. 20-24

Betz, David, 'Cyberwar is Not Coming', Infinity Journal, Vol. 1, Issue 3 (Summer 2011), pp. 21-24

Bissell, David, 'Passenger Mobilities: Affective Atmospheres and the Sociality of Public Transport', *Environment and Planning D: Society and Space*, Vol. 28, Issue 2 (January 2010), pp. 270-289

Bisson, Christian and John Luckner, 'Fun in Learning: The Pedagogical Role of Fun in Adventure Education', *Journal of Experiential Education*, Vol. 19, Issue 2 (August 1996), pp. 108-112

Board Game Geek, 'World in Flames' (https://www.boardgamegeek.com/boardgame/1499/world-flames)

BoardGameGeek, search for ‘Waterloo’ (https://boardgamegeek.com/geeksearch.php?action=search&objecttype=boardgame&q=waterloo&B1=Go)

BoardGameGeek, cyberpunk games (https://boardgamegeek.com/boardgamefamily/5611/cyberpunk)

BoardGameGeek listing for *Scooby-doo! Cyber chase* (https://boardgamegeek.com/boardgame/20380/scooby-doo-cyber-chase)

Böcking, Sarah, ‘Suspension of Disbelief’, *The International Encyclopedia of Communication*, 5 June 2008 (https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781405186407.wbiecs121)

Bonk, Curtis J. And Vanessa P. Dennen, ‘Massive Multiplayer Online Gaming: A Research Framework for Military Training and Education', Technical Report 2005-1, Advanced Distributed Learning Initiative, March 2005

Bos, Daniel, ‘Answering the Call of Duty : the popular geopolitics of military-themed videogames’, Doctoral thesis, Newcastle University, 2016

Boudon, Raymond, ‘Beyond Rational Choice Theory’, *Annual Review of Sociology*, Vol. 29 (2003), pp. 1-29

Bowcott, Owen, ‘Dispute along cold war lined led to collapse of UN cyberwarfare talks’, *The Guardian*, 23 August 2017 (https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges)

Brangetto, Pascal, Emin Çalişkan and Henry Rõigas, ‘Cyber Red Teaming – Organisational, technical and legal implications in a military context', NATO Cooperative Cyber Defence Centre of Excellence, 2015

Brewer, Garry D. and Martin Shubik (1979), *The War Game: A Critique of Military Problem Solving* (Harvard University Press: Cambridge, Massachusetts)

Brynen, Rex, ‘(Ending) Civil War in the Classroom: A Peacebuilding Simulation’, *PS: Political Science and Politics*, Vol. 43, No. 1 (January 2010), pp. 145-149

Brynen, Rex, ‘Gaming the Nonkinetic’, in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge), pp. 485-502

Buchanan, Ben (2017), *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press: New York, NY)

Buckley, Thomas and Ruth David, ‘Kraft Heinz Spurned in $143 Billion Unilever Takeover Bid’, *Bloomberg*, 17 February 2017 (https://www.bloomberg.com/news/articles/2017-02-17/kraft-heinz-says-unilever-rejected-approach-on-combination)

Burns, Shawn W., 'War Gaming as Reflective Practice', United States Naval War College (publication details unknown)

Burns, Shawn, ed. (2013) *War Gamers' Handbook – A Guide for Professional Wargamers* (United States Naval War College: Newport, RI)

Cambridge Dictionary, 'troll' (http://dictionary.cambridge.org/dictionary/english/troll)

Campbell, Martin, dir. (1995), *GoldenEye* (Eon Productions)

Carter, Marcus, Mitchell Harrop and Martin Gibbs. 'The Roll of the Dice in Warhammer 40,000', *Transactions of the Digital Games Research Association*, Vol. 1, No. 3 (2014), pp. 1-28

Castro, Celso, 'Anthropological methods and the study of the military: the Brazilian experience', in Helena Carreiras and Celso Castro, eds. (2013), *Qualitative Methods in Military Studies: Research experiences and challenges* (Routledge: London) pp. 8-16

CBS News, 'Vladimir Putin doing manly things' (https://www.cbsnews.com/pictures/vladimir-putin-doing-manly-things/)

Centre for Protection of National Infrastructure (https://www.cpni.gov.uk/critical-national-infrastructure-0)

Chau, Brian, 'Anti-Hack! Demonstration of a Board Game introducing Information Security', YouTube, 14 April 2016 (https://www.youtube.com/watch?v=icSx8hZf7Xg)

Chekan, Brig Gen Robert J., 'Schriever Wargame 2010 – A Coming of Age', *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 7, No. 1 (November 2010), pp. 16-18

Clancy, Tom (1984), *The Hunt for Red October* (Naval Institute Press: Annapolis)

Clausewitz, Carl von (1997a), *On War*, trans. Michael Howard and Peter Paret (Oxford University Press: Oxford)

Clausewitz, Carl von (1997b), *On War*, trans. J. J. Graham (Wordsworth: Ware)

Clifford, James, 'Notes on (Field)notes', in Roger Sanjek, ed. (1990), *Fieldnotes: The Makings of Anthropology* (Cornell University Press: Ithaca), pp. 47-70

Clifford, James, 'Spatial Practices: Fieldwork, Travel, and the Disciplining of Anthropology', in Akhil Gupta and James Ferguson, eds. (1997), *Anthropological Locations: Boundaries and Grounds of a Field Science* (University of California Press: Berkeley), pp. 185-222

Closs Stephens, Angharad, 'The affective atmospheres of nationalism', *Cultural Geographies*, Vol. 23, Issue 2 (2016), pp. 181-198

Cohn, Carol, 'Sex and Death in the Rational World of Defense Intellectuals', *Signs*, Vol. 12, No. 4, Within and Without: Women, Gender, and Theory (Summer 1987), pp. 687-718

Collins, Kathleen M., Carolyn J. Griess, Kristine Carithers and Danielle Michaelis Castillo, 'It's All in the Game: Designing and Playing Board Games to Foster Communication and Social Skills', *YC Young Children*, Vol. 66, No. 2 (March 2011), pp. 12-19

Cone, Benjamin D., Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, 'A video game for cyber security and awareness training', *Computers & Security*, No. 26 (2007), pp. 63-72

Convertino, Sebastian M. II, Lou Anne DeMattei, Tammy M. Knierim, 'Flying and Fighting in Cyberspace', Air War College Maxwell Paper No. 40, July 2007 (Air University Press: Alabama)

Cozine, Keith, 'Thinking Interestingly: The Use of Game Play to Enhance Learning and Facilitate Critical Thinking Within a Homeland Security Curriculum, *British Journal of Educational Studies*, Vol. 63, No. 3 (2015), pp. 367-385

Craig, Anthony and Brandon Valeriano, 'Conceptualising Cyber Arms Races', *Proceedings of 8th International Conference on Cyber Conflict* (2016), pp. 141-158

Crawford, Chris, 'The Future of Computer Wargaming', *Computer Gaming World*, Vol. 1, No. 1 (November-December 1981), pp. 3-7

Cryptomancer (http://cryptorpg.com/)

Ctrl+Alt+Hack (http://www.controlalthack.com/activities.php)

Ctrl+Alt+Hack game rules (available at http://www.controlalthack.com/downloadrules.php)

Cumming, Douglas, Tak Yan Leung, and Oliver Rui, 'Gender Diversity and Securities Fraud', *Academy of Management Journal*, Vol. 58, No. 5 (2015), pp. 1572-1593

Curry, John and Tim Price (2013), *Dark Guest: Training Games for Cyber Warfare Volume 1 –Wargaming Internet Based Attacks*, 2nd ed.

Curry, John, ed. (2011) *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists* (The History of Wargaming Project)

'Cyber Defence Exercise Locked Shields 2013 After Action Report' (2013) (available at https://ccdcoe.org/multimedia/cyber-defence-exercise-locked-shields-2013-after-action-report.html)

Dahm, Werner J. A. and Col Eric Silkowski, 'Science Supporting Space and Cyber: Insights From Schriever Wargame 2010', *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 7, No. 1 (November 2010), pp. 38-40

Dallaway, Eleanor, 'Closing the Gender Gap in Cyber Security', CREST, 2016 (https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf)

Darken, Rudolph P. and Curtis L. Blair, 'The Uniformed Military Modeling and Simulation Professional', in Andreas Tolk and Tuncer Ören, eds. (2017), *The Profession of Modeling and Simulation – Discipline, Ethics, Education, Vocation, Societies, and Economies* (Wiley: Hoboken) pp. 151-166

Dastool, Erling, 'One Person's Opinion: Should School Be Fun?', *The English Journal*, Vol. 84, No. 2 (February 1995), pp. 15-16

de Kloet, Jeroen and Liesbet von Zoonen, 'Fan Culture – Performing Difference', in Eoin Deveraux, ed., *Media Studies: Key Issues and Debates* (SAGE: London), pp. 322-341

de Koven, Bernard (2013), *The Well-Played Game* (MIT Press: Cambridge, MA)

Dean, Richard (2003), *Imperial Brotherhood: Gender and the Making of Cold War Policy*, first published 2001 (University of Massachusetts Press: Amhurst)

Decisions & Disruptions (http://www.decisions-disruptions.org/)

Decisions & Disruptions game rules (available at http://scc-research.lancs.ac.uk/sites/decisions-disruptions.org/assets/dd_rules_final_nb.pdf)

Defence, Concepts and Doctrine Centre (2017), *Wargaming Handbook* (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf)

Deloitte, 'Independent Review of RTGS Outage on 20 October 2014', 23 March 2015 (http://www.bankofengland.co.uk/publications/Documents/news/2015/rtgsdeloitte.pdf)

Dempsey, Joel, 'UK Defence Personnel Statistics', House of Commons Library Briefing Paper, Number CBP7930, 29 June 2017

Denisova, Anastasia, 'Democracy, protest and public sphere in Russia after the 2011-2012 anti-government protests: digital media at stake', *Media, Culture & Society*, Vol. 39, Issue 7 (2017), pp. 976-994

Denning, Dorothy E., 'The Ethics of Cyber Conflict', in Kenneth Einar Himma and Herman T. Tavani, eds., *The Handbook of Information and Computer Ethics* (John Wiley & Sons: Hoboken, NJ), pp. 407-428

Denning, Tamara, Adam Lerner, Adam Shoshtack and Tadayoshi Kohno, 'Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security

Awareness and Education', Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13), 2013a, pp. 915-928

Denning, Tamara, Batya Friedman, Tadayoshi Kohno, 'The Security Cards: A Security Threat Brainstorming Toolkit', 2013b (http://securitycards.cs.washington.edu/assets/security-cards-information-sheet.pdf)

Department of Justice, 'Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets', 27 June 2013 (https://www.justice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets)

Department of War Studies (https://www.kcl.ac.uk/sspp/departments/warstudies/about/index.aspx)

Department of War Studies Employability (https://www.kcl.ac.uk/sspp/departments/warstudies/employability.aspx)

Dicheva, Darina, Christo Dichev, Gennady Agre and Galia Angelova, 'Gamification in Education: A Systematic Mapping Study', *Journal of Educational Technology & Society*, Vol. 18, No. 3 (July 2015), pp. 75-88

Dickinson-Smith, Virginia, Erica L. James, Sandra Kippen and Pranee Liamputtong, 'Researching sensitive topics: qualitative research as emotion work', *Qualitative Research*, Vol. 9, Issue 1 (2009), pp. 61-79

Dodds, Klaus and Philip Kirby, 'It's Not a Laughing Matter: Critical Geopolitics, Humour and Unlaughter', *Geopolitics*, Vol. 18, Issue 1 (2013), pp. 45-59

Donaldson, Mike, 'What is hegemonic masculinity?', *Theory and Society*, Vol. 22 (1993), pp. 643-657

Downes-Martin, Stephen, 'Adjudication – The *Diabolus in Machina* of War Gaming', *Naval War College Review*, Vol. 66, No. 3 (Summer 2013), pp. 67-81

Downes-Martin, Stephen, 'How can we credibly wargame cyber at an unclassified level?', Game Lab, Connections US conference, 18 July 2018 (https://paxsims.files.wordpress.com/2018/08/game-lab-unclassified-cyber-gaming-20180814.pdf)

Downes-Martin, Stephen, 'Wargaming as a Catalyst for Innovation', presentation given at Connections US conference, 27 July 2015 (https://connectionswargaming.files.wordpress.com/2015/06/wargaming-as-a-catalyst-for-innovation-20150828.pdf)

Downes-Martin, Stephen, 'Wargaming to Deceive the Sponsor – How and Why?', speaker's notes from presentation given at Connections UK conference, King's College London, 4 September 2016 (http://www.professionalwargaming.co.uk/WargamingToDeceivePaper.pdf)

Dunnigan, James F. (1992), *The Complete Wargames Handbook: How to Play, Design, and Find Them*, 2nd. Ed. (Quill William Morrow: New York)

Elg, Johan, 'Wargaming in Military Education for Army Officers and Officer Cadets', Doctoral Thesis, King's College London, September 2017

Eisenack, Klaus, 'A Climate Change Board Game for Interdisciplinary Communication and Education', *Simulation & Gaming*, Vol. 44, No. 2-3 (2012), pp. 328-348

Elliot, Owen, '?gaming in the FCO', presentation given at Connections UK 2017 conference, 6 September 2017 (http://www.professionalwargaming.co.uk/17-FCOGaming.pdf)

Ember, Melvin, 'Evidence and Science in Ethnography: Reflections on the Freeman-Mead Controversy', *American Anthropologist*, Vol. 87, No. 4 (December 1985), pp. 906-910

Emerson, Robert M., Rachel I. Fretz and Linda L. Shaw (2011), *Writing Ethnographic Fieldnotes*, 2nd ed. (University of Chicago Press: Chicago)

Emerson, Robert M., Rachel I. Fretz and Linda L. Shaw, 'Participant Observation and Fieldnotes', in Paul Atkinson, Amanda Coffey, Sara Delamont, John Lofland and Lyn Lofland, eds. (2007), *Handbook of Ethnography* (SAGE: London)

Englund, Peter (1991), *Förflutenhetens landskap: Historiska essäer*, 3rd ed. (Atlantis: Stockholm) [Translated title: *The landscape of the past: Historical essays*]

ENISA, 'Cyber Europe 2014 – Questions and Answers', October 2014 (https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2014/cyber-europe-2014-information/briefing-pack/cyber-europe-2014-2013-questions-and-answers)

ENISA, 'NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies', November 2016

European Commission, 'Commission Guidance note on implementation of certain provisions of Regulation (EU) No 833/2014', 25 September 2015 (https://europa.eu/newsroom/sites//newsroom/files/docs/body/1_act_part1_v2_en.pdf)

Everett, Cath, 'Ransomware: to pay or not to pay?', *Computer Fraud & Security*, April 2016, pp. 8-12

'Executive Order 13687 – Imposing Additional Sanctions With Respect To North Korea', Federal Register, Vol. 80, No. 3, 6 January 2015 (https://www.gpo.gov/fdsys/pkg/FR-2015-01-06/pdf/2015-00058.pdf)

Fabricatore, Carlo, Miguel Nussbaum and Ricardo Rosas, 'Playibility in Action Videogames: A Qualitative Design Model', *Human-Computer Interaction*, Vol. 17, Issue 4 (2002), pp. 311-368

Falliere, Nicolas, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier', Version 1.4 (February 2011)

Farwell, James P. and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival*, Vol. 53, No. 1 (February-March 2011), pp. 23-40

Ferrara, Emilio, 'How Twitter bots played a role in electing Donald Trump', *Wired*, 9 November 2016 (http://www.wired.co.uk/article/twitter-bots-democracy-usa-election)

Fetterman, David M. (2010), *Ethnography: Step-by-Step*, 3rd ed. (Sage: Thousand Oaks, CA)

Fifield, William (1982), *In Search of Genius* (William Morrow & Co.: New York)

Fine, Gary Alan, 'Strategy and Sociability - The Mind, the Body, and the Soul of Chess', *American Journal of Play*, Vol. 6, No. 3 (Spring 2014), pp. 321-344

FireEye, 'Spearphishing Attacks: Why They are Successful and How to Stop Them', Whitepaper (2016)

'FM 3-38 Cyber Electromagnetic Activities', Headquarters, Department of the Army, February 2014 (https://fas.org/irp/doddir/army/fm3-38.pdf)

Foley, Meraiah, Linda Dewey, Sue Williamson, Deborah Blackman, Alison Creagh, Lisa Davidson, Meng Zhu and Jill Slay, 'Women in Cyber Security Literature Review', Australian Department of the Prime Minister and Cabinet, June 2017

Foresman, Hon. George W., 'The Complexities of American National Security: Enabling A New Generation of Leadership', *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 7, No. 1 (November 2010), pp. 5-8

Foxall, Andrew, 'Constructing, Practicing, and Narrating Russian Geo(Political) Identity, *Geopolitics*, Vol. 17, Issue 1 (2012), pp. 235-241

Frank, Anders, 'Gamer mode – Identifying and managing unwanted behaviour in military educational wargaming', Doctoral Thesis, KTH Royal Institute of Technology, 2014

Freedman, Lawrence (2013), *Strategy: A History* (Oxford University Press: Oxford)

Freeman, Derek (1983), *Margaret Mead and Samoa: The Making and Unmaking of an Anthropological Myth* (Harvard University Press: Cambridge, MA)

Frey, Sylvian, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, Sayed Asad Naqvi, 'The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game', in *20th International Conference on Software Engineering (ICSE 2018)*, 2018, Association for Computing Machinery (ACM)

Gady, Franz-Stefan, 'New Snowden Documents Reveal Chinese Behind F-35 Hack', *The Diplomat*, 27 January 2015 (http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/)

Gallagher, Sean, 'WikiLeaks publishes docs from what it says is a trove of CIA hacking tools', *Ars Technica*, 7 March 2017 (https://arstechnica.com/information-technology/2017/03/wikileaks-publishes-what-it-says-is-trove-of-cia-hacking-tools/)

Galloway, Alexander R., 'Debord's Nostalgic Algorithm', *Culture Machine*, Vol. 10 (2009), pp. 131-156

Game of Threats (https://www.pwc.co.uk/issues/cyber-security-data-privacy/game-of-threats.html)

Garretson, Lieutenant Colonel Peter, 'Wargaming in 2015', address to the Air War College class of 2015

Gerden, Eugene, 'New cyber defence doctrine approved by Russian government', *SC Media*, 6 January 2017 (https://www.scmagazineuk.com/new-cyber-defence-doctrine-approved-by-russian-government/article/630032/)

Ghamari-Tabrizi, Sharon, 'Simulating the Unthinkable: Gaming Future War in the 1950s and 1960s', *Social Studies of Science*, Vol. 30, No. 2 (April 2000), pp. 163-223

Gibson, William (1995), *Neuromancer* (first published 1984) (Voyager: London)

Gilbert, David, 'Cost of Developing Cyber Weapons Drops from $100m Stuxnet to $10k IceFrog', *International Business Times*, 6 February 2014 (http://www.ibtimes.co.uk/cost- developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451)

Gondree, Mark and Zachary Peterson, 'Valuing Security by Getting [d0x3d!]: Experiences with a network security board game', 6th Workshop on Cyber Security Experimentation and Test (CSET), 2013 (https://www.usenix.org/system/files/conference/cset13/cset13-gondree.pdf)

Gondree, Mark, Zachary Peterson and Portia Pusey, 'Talking about Talking about Cybersecurity Games', *;login:*, Vol. 41, No. 1 (Spring 2016), pp. 36-39

Gondree, Mark, Zachary Peterson and Tamara Denning, 'Security Through Play', *IEEE Security and Privacy*, May/June 2013, pp. 64-67

Gray, John (2003), *Straw Dogs: Thoughts on Humans and Other Animals*, 2nd ed. (Granta: London)

Greenberg, Andy, 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits', *Forbes*, 23 March 2012

Gregory, Derek, 'The Everywhere War', *The Geographical Journal*, Vol. 177, No.3 (September 2011), pp. 238-250

Greiner, Ben, 'Subject pool recruitment procedures: organizing experiments with ORSEE', *Journal of the Economic Science Association*, Vol. 1, Issue 1 (July 2015), pp. 114-125

Gross, Joseph Michael, 'A Declaration of Cyber War', *Vanity Fair*, April 2011 (http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104)

Guilbeaut, Douglas and Samuel Woolley, 'How Twitter Bots Are Shaping the US Election', *The Atlantic*, 1 November 2016 (https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/)

Gush, George (1979), *Wargames Rules for Fifteenth to Seventeenth Centuries (1420-1700)*, 2nd ed. (Wargames Research Group: Goring-by-Sea)

Guthrie, Phyllis, 'Knowledge Through Humour: An Original Approach for Teaching Developmental Readers', paper presented at the Annual Meeting of the National Institute for Staff and Organizational Development, International Conference on Teaching and Leadership Excellence (Austin, TX, 23-26 May 1999)

Haggman, Andreas, 'Cyber Deterrence Theory and Practice', in M. Lehto and P. Neittaanmäki, eds. (2018) *Cyber Security: Cyber Power and Technology* (Springer), pp. 63-81

Haggman, Andreas, 'Clausewitz and cyber security: towards a new Trinity?', *Strife Blog*, 13 February 2014 (https://strifeblog.org/2014/02/13/clausewitz-and-cyber-security-towards-a-new-trinity/)

Haggman, Andreas, 'Cyber risks to governance, Part I – Silk Road: resisting and reshaping governance', *Strife Blog*, 20 August 2015 (http://www.strifeblog.org/2015/08/20/cyber-risks-to-governments-part-i-silk-road-resisting-and-reshaping-governance/)

Haggman, Andreas, 'Training day: Joint UK-US cyber exercise tests preparedness', *Jane's Intelligence Review*, August 2016, pp. 52-53

Halter, Ed (2006), *From Sun Tsu to Xbox: War and Video Games* (New York: Thunder's Mouth Press)

Hammersley, Martin and Paul Atkinson (2007), *Ethnography – Principles in practice*, 3rd ed. (Routledge: Abingdon)

Harrigan, Pat and Matthew G. Kirschenbaum, 'Editors' Introduction', in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge), pp. XV-XXX

Hawkins, Harriet, 'Creative geographic methods: knowing, representing, intervening. On composing place and page', *cultural geographies*, Vol. 22, Issue 2 (2015), pp. 247-268

Haynes, Kathryn, 'Tensions in (re)presenting the self in reflexive autoethnographical research', *Qualitative Research in Organizations and Management: An International Journal*, Vol. 6, No. 2 (2011), pp. 134-149

Helms, Maj Gen Susan J., 'Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain', *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 7, No. 1 (November 2010), pp. 12-15

Herman, Mark, Mark Frost and Robert Kurz (2009), *Wargaming for Leaders: Strategic Decision Making from the Battlefield to the Boardroom* (McGraw Hill: New York)

Herr, Andrew, 'Will Humans Matter in the Wars of 2030?', National Defense University Press, 1 April 2015 (http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581875/jfq-77-will-humans-matter-in-the-wars-of-2030.aspx)

Herring, Cedric, 'Does Diversity Pay?: Race, Gender, and the Business Case for Diversity', *American Sociological Review*, Vol. 74, Issue 2 (2009), pp. 208-224

Hildreth, Steven A., 'Cyberwarfare', CRS Report for Congress, June 2001

Hinshaw, John and Peter N. Stearns (2014), *Industrialization in the Modern World: From the Industrial Revolution to the Internet Volume 1: A-P* (ABC-CLIO: Santa Barbara, CA)

HM Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (HM Stationery Office)

HM Government (2016), *National Cyber Security Strategy 2016-2021*

HM Government, 'Security and Intelligence Agencies – Financial Statement 2015-16', HC 363, 14 July 2016

Holmes, John Eric, 'Confessions of a Dungeon Master', *Psychology Today* (November 1980), pp. 84-94

Hook, Nathan, 'Grounded Theory', in Petri Lankoski and Staffan Björk, eds. (2015), *Game Research Methods: An Overview* (ETC Press), pp. 309-322

Hopkirk, Peter (2006), *The Great Game: On Secret Service in High Asia* (John Murray: London)

Horowitz, Jason, 'Will Russia Meddle in Italy's Election? It May Not Have To', *New York Times*, 1 March 2018 (https://www.nytimes.com/2018/03/01/world/europe/italy-election-russia.html)

Howard, Admiral Michelle, 'Leadership and Technology Change – Implications, Opportunities and the Operational Perspective', keynote at 9th International Conference on Cyber Conflict, 30 May 2017 (available at https://www.youtube.com/watch?v=btqmd8gHP4Y)

Hughes, Daniel, ed. (1993), *Moltke on the Art of War: Selected Writings* (Presidio Press)

Huizinga, Johan (1949), *Homo Ludens: A Study of the Play-Element in Culture* (Routledge: London)

Hulse, David, Allan Branscomb, Chris Enright, Bart Johnson, Cody Evers, John Bolte and Alan Ager, 'Anticipating surprise: Using agent-based alternative futures simulation modeling to identify and map surprising fires in the Willamette Valley, Oregon USA', *Landscape and Urban Planning*, 156 (2016), pp. 26-43

Hume, Lynne and Jane Mulcock, 'Introduction: Awkward Spaces, Productive Spaces', in Lynne Hume and Jane Mulcock, eds. (2004), *Anthropologists in the Field: Cases in Participant Observation* (Columbia University Press: New York), pp. xi-xxxvii

Huntemann, Nina B. and Matthew Thomas Payne, 'Introduction' in Nina B. Huntemann and Matthew Thomas Payne (2010), *Joystick Soldiers: The Politics of Play in Military Video Games* (Routledge: Abingdon), pp. 1-18

Hutchinson, Sally A., 'Education and Grounded Theory', *Journal of Thought*, Vol. 21, No. 3 (Fall 1986), pp. 50-68

'Hype and Fear', *The Economist*, 8 December 2012 (available at http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may)

ICS-CERT, 'Cyber-Attack Against Ukrainian Critical Infrastructure', Alert (IR-ALERT-H-16-056-01), first published 25 February 2016 (https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01)

Information Security Group (2017), 'Visualisation of Security via Gameplay', *YouTube* (https://www.youtube.com/watch?v=sPwZKB8ZLyM)

Ingraham, Christopher, 'Satellite data strongly suggests that China, Russia and other authoritarian countries are fudging their GDP reports', *The Washington Post*, 15 May 2018 (https://www.washingtonpost.com/news/wonk/wp/2018/05/15/satellite-data-strongly-suggests-that-china-russia-and-other-authoritarian-countries-are-fudging-their-gdp-reports/)

Jackson, Patrick, 'Who killed Russia opposition politician Boris Nemtsov?', *BBC News*, 7 March 2015 (http://www.bbc.co.uk/news/world-europe-31693234)

Jackson, Steve (1992), *Hacker - The Computer Crime Card Game*, rulebook

Jacobsen, Jeppe Teglskov, 'The Cyberwar Mirage and the Utility of Cyberattacks in War - How to Make Real Use of Clausewitz in the Age of Cyberspace', DIIS Working Paper 2014:06 (Danish Institute of International Studies: Copenhagen)

James Bond Wiki (http://jamesbond.wikia.com/wiki/Universal_Exports)

Johansson, Maria and Mattias Arvola, 'A Case Study of How User Interface Sketches, Scenarios and Computer Prototypes Structure Stakeholder Meetings', in Linden J. Ball, M. Angela Sasse, Corina Sas, Thomas C. Ormerod, Alan Dix, Peter Bagnall and Tom McEwan (eds.), *People and Computers XXI - HCI...but not as we know it: Proceedings of HCI 2007* (British Computer Society)

'Jan in the Pan', 'Surviving Academic Conferences without Crying', *The brain that wouldn't die: a tenure track blog*, 30 July 2013 (https://brainthatwouldntdie.wordpress.com/2013/07/30/surviving-academic-conferences-without-crying/)

Johnson, Grant, 'Letter to the editor', *Spearpoint: The Official Newsletter of The North American Society of Ancient and Medieval Wargamers*, Vol. 3, No. 1 (February 1988), p. 6

Jones, Aime, 'Cybercrime Effects on Stock Prices', Honors College Thesis, Murray State University (2016) (http://digitalcommons.murraystate.edu/cgi/viewcontent.cgi?article=1004&context=honorstheses)

Jones, Sam, 'Energy companies hit by cyber attack from Russia-linked group', *Financial Times*, 30 June 2014 (https://www.ft.com/content/606b97b4-0057-11e4-8aaf-00144feab7de)

Jones, Sam, 'Nato holds largest cyber war games', *Financial Times*, 20 November 2014 (http://www.ft.com/cms/s/0/9c46a600-70c5-11e4-8113-00144feabdc0.html#axzz3jqH31uUj)

Kainikara, Sanu (2003), 'Effective Wargaming: Impact of the Changing Nature of Warfare', Aerospace Centre Paper Number 13 (Australian Department of Defence)

Kashibuchi, Megumi and Akira Sakamoto, 'The educational effectiveness of a simulation/game in sex education', *Simulation & Gaming,* Vol. 32, No. 3 (September 2001), pp. 331-343

Kappos, David J. and Pamela Passman, 'Cyber Espionage Is Reaching Crisis Levels', *Forbes*, 12 December 2015 (http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/)

Kaspersky Lab, 'Energetic Bear – Crouching Yeti', July 2014 (https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf)

Kaspersky Lab, 'Vulnerable System Update Statistics. General Electric', 19 June 2017 (https://ics-cert.kaspersky.com/reports/2017/06/19/industrial-system-component-updates-general-electric/)

Kelley, Tanya M. and Erik Johnston, 'Discovering the Appropriate Role of Serious Games in the Design of Open Governance Platforms', *Public Administration Quarterly*, Vol. 36, No. 4 (Winter 2012), pp. 504-554

Kiesling, Eugenia C., 'On War Without the Fog', *Military Review*, September-October 2001, pp. 85-87

Kiravuo, Timo, Seppo Tiilikainen, Mikko Särelä and Jukka Manner, 'Peeking Under the Skirts of a Nation: Finding ICS Vulnerabilities in the Critical Digital Infrastructure', *Proceedings of the 14th European Conference on Cyber Warfare and Security*, 2015, 137-144

Kirk, Phil and Mike Broussine, 'The politics of facilitation', *Journal of Workplace Learning*, Vol. 12, Issue 1 (2000), pp. 13-22

Klein, Jonathan H. and Dale F. Cooper, 'Cognitive Maps of Decision-Makers in a Complex Game', *The Journal of the Operational Research Society*, Vol. 33, No. 1 (January 1982), pp. 63-71

Knight, Peter, 'A simple learn-as-you-play board game', *Teaching Geography*, Vol. 19, No. 1 (January 1994), pp. 19-21

Kriz, Willy Christian, 'A Systematic-Constructivist Approach to the Facilitation and Debriefing of Simulations and Games', *Simulation & Gaming*, Vol. 41, Issue 5 (2010), pp. 663-680

Kurian, George Thomas, 'Lanchester strategy', in George Thomas Kurian, The *AMA dictionary of business and management* (2013) (available online: https://search.credoreference.com/content/entry/amadictbm/lanchester_strategy/)

Kux, Dennis, 'Soviet Active Measures and Disinformation: Overview and Assessment', *Parameters*, Vol. 15, No. 4 (Winter 1985), pp. 19-28

Leach, Edmund (1964), *Political Systems of Highland Burma – A Study of Kachin Social Structure*, first published 1954 (G. Bell and Sons: London)

Ledeneva, Alena V. (2006), *How Russia Really Works: The Informal Practices That Shaped Post-Soviet Politics and Business* (Cornell University Press: Ithaca, NY)

Lei, Leon, 'Go and Mathematics', unpublished research paper, 2013 (http://agfgo.org/downloads/Go%20and%20Mathematics.pdf)

Libicki, Martin C., 'Cyberspace is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society*, Issue 2 (2012), pp. 321-336

Liles, Samuel, Marcus Rogers, J. Eric Dietz and Dean Larson, 'Applying Traditional Military Principles to Cyber Warfare', in C. Czosseck, R. Ottis and K. Ziolkowski, eds., *2012 4th International Conference on Cyber Conflict* (NATO CCD COE: Tallinn), pp. 169-180

Limnéll, Jarno, 'The cyber arms race is accelerating – what are the consequences?', *Journal of Cyber Policy*, Vol. 1, Issue 1 (2016), pp. 50-60

Lindsay, Jo, 'Getting the Numbers: The Unacknowledged Work in Recruiting for Survey Research', *Field Methods*, Vol. 17, No. 1 (February 2005), pp. 119-128

Lindstädt, Hagen and Jürgen Müller, 'Making game theory work for managers', *McKinsey Quarterly* (January 2010), pp. 1-9

Lineberry, Stephen, 'The Human Element: The Weakest Link in Information Security', *Journal of Accountancy*, Vol. 204, Issue 5 (November 2007), pp. 44-46, 49

Litovkin, Nikolai, 'What is the updated Russian cyber-security doctrine about?', *Russia Beyond the Headlines*, 7 December 2016 (https://www.rbth.com/defence/2016/12/07/what-is-the-updated-russian-cyber-security-doctrine-about_654407)

Lockhart, Keely and Myles Burke, '#OpISIS: Why Anonymous has declared an online war against Isil', *The Telegraph*, 11 December 2015 (https://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-Why-Anonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html)

Lockheed Martin Cyber Kill Chain (http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html)

Logan, David C., 'Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry', *Journal of Experimental Botany*, Vol. 60, Issue 3 (March 2009), pp. 712-714

Lombardi, Ivan, 'Not-so-serious games for language learning. Now with 99,9% more humour on top', *Procedia Computer Science 15* (2012), pp. 148-158

Longley-Brown, Graham, 'High-engagement wargames', presentation given at Connections UK conference, 5 September 2015 (http://www.professionalwargaming.co.uk/2016Engagement.pdf)

Luft, Nick, 'Against the Nature of Gentleness (ATNOG), Onside Review', *Military Muddling*, Vol. 13, Issue 3 (February 2002), pp. 4-6

Lynn, John A. (2003), Battle – A History of Combat and Culture, 2nd ed. (Westview Press: Oxford)

Maelstrom game rules, version .10 (2016) (available at Maelstrom GitHub repository: https://github.com/maelstromthegame/defcon24)

Mahoney, Terence, 'Facilitation of War Games: Roles and Responsibilities at the Naval War College', United States Naval War College

Manderson, Lenore, Mark Davis, Chip Colwell and Tanja Ahlin, 'On Secrecy, Disclosure, the Public, and the Private in Anthropology: An Introduction to Supplement 12', *Current Anthropology*, Vol. 56, Supp. 12 (December 2015), pp. S183-S190

Mandiant, 'APT1 – Exposing One of China's Cyber Espionage Units', 2013 (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

Mao, Chunhua, 'Associative Meaning in Social and Cultural Context', proceedings of 2nd International Conference on Science and Social Research (ICSSR), July 2013, pp. 614-617

Marshall, A. W., 'A Program to Improve Analytic Methods Related to Strategic Forces', *Policy Sciences*, Vol. 15, No. 1 (November 1982), pp. 47-50

Marshall, Frank (dir.), *The Man Vs. The Machine* (http://www.espn.com/video/clip?id=11694550)

Martin, Guy, Paul Martin, Chris Hankin, Ara Darzi and James Kinross, 'Cybersecurity and healthcare: how safe are we?', *BMJ*, 358:j3179, July 2017

Matrosov, Aleksandr, Eugene Rodionov, David Harley and Juraj Malcho, ' Stuxnet Under the Microscope', revision 1.1, ESET (2010) (https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf)

McCormack, Derek P., 'Engineering affective atmospheres on the moving geographies of the 1897 Andrée expedition', *Cultural Geographies*, Vol. 15 (2008), pp. 413-430

Mead, Margaret (2001), *Sex and Temperament In Three Primitive Societies*, first published 1935 (Perennial: New York)

Mills, Sara, 'Gender and Performance Anxiety at Academic Conferences', in Judith Baxter, ed. (2006), *Speaking Out: The Female Voice in Public Context* (Palgrave Macmillan: London), pp. 61-80

Miranda, Joseph, 'Cybernauts', *Competitive Edge*, Issue 11 (1996), pp. 9-25

Miranda, Joseph, 'Wargaming the Cyber Frontier', in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge, MA), pp. 673-680

Mitnick, Kevin D. and William L. Simon (2002), *The Art of Deception: Controlling the Human Element of Security* (Wiley Publishing: Indianapolis)

Modderkolk, Huib, ‘Dutch agencies provide crucial intel about Russia’s interference in US-elections’, *de Volksrant*, 25 January 2018 (https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/)

Morrill, Calvin, David B. Muller, Mary Klein Buller, and Linda L. Larkey, ‘Toward an Organizational Perspective on Identifying and Managing Formal Gatekeepers’, *Qualitative Sociology*, Vol. 22, No. 1 (1999), pp. 51-72

‘Multinational Experiment 7 Cyber Domain Outcome 3 – Cyber Situational Awareness Limited Objective Experiment Report’, Version 1.0, 28 February 2013

Mumford, Andrew, 'Proxy Warfare and the Future of Conflict', *The RUSI Journal, Vol. 158, No. 2* (April/May 2013), pp. 40-46

National Cyber Security Centre (https://www.ncsc.gov.uk/about-us)

National Cyber Security Centre, ‘Cyber security: fixing the present so we can worry about the future’, address by Ciaran Martin, 15 November 2017 (https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future)

National Cyber Security Centre, ‘Password Guidance: Simplifying Your Approach’, updated 8 August 2016 (https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach)

National Cyber Security Centre, ‘Russian military “almost certainly” responsible for destructive 2017 cyber attack’, 15 February 2018 (https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack)

‘National Cyber Security Strategy 2016-2021’, HM Government, November 2016
‘The Digital Arms Race’, *The Economist*, 30 March 2013

NATO Cooperative Cyber Defence Centre of Excellence, ‘Baltic Cyber Shield Cyber Defence Exercise 2010 – After Action Report', 2010

NATO Cooperative Cyber Defence Centre of Excellence, ‘Cyber Security Strategy Documents’ (https://ccdcoe.org/cyber-security-strategy-documents.html)

Newcombe, Colin, ‘Wargames in the Classroom’, *Teaching History*, Vol. 1, No. 4 (November 1970), pp. 300-302

Newman, Edward and Benjamin Zala, ‘Rising powers and order contestation: disaggregating the normative from the representational’, *Third World Quarterly*, Vol. 35, Issue 5 (2018), pp. 871-888

NHS, ‘Colour vision deficiency (colour blindness)’ (http://www.nhs.uk/conditions/Colour-vision-deficiency/Pages/Introduction.aspx)

Nicholson, S. (2010), *Everyone Plays at the Library: Creating Great Gaming Experiences for All Ages* (Information Today: Medford, NJ)

O'Connor, Gabe and Avie Schneider, 'How Russian Twitter Bots Pumped Out Fake News During The 2016 Election', *NPR*, 3 April 2017 (http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election)

Office for National Statistics, 'Overview of the UK Population: July 2017' (https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/july2017)

Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in the Recent US Elections', ICA 2017-01D, 6 January 2017

Orme, Major General Craig, 'Professional Military Education and Simulation', speech presented at the 'SIMTECT 2012: Asia-Pacific Simulation & Training Conference and Exhibition', 19 June 2012 (http://www.defence.gov.au/ADC/Publications/Commanders/2013/02_Orme%20article%20_edited%20version.pdf)

Ormerod, David, 'AlphaGo defeats Lee Sedol 4-1 in Google DeepMind Challenge Match', *Go Game Guru* (https://gogameguru.com/alphago-defeats-lee-sedol-4-1/)

O'Shaughnessy, Brig Gen Terrence J., Lt Col Baron V. Greenhouse, Lt Col Kurt M. Schendzielos, 'Effects Felt Around the World: The Growing Complexities of the Interaction Between Geographic and Functional Combatant Commanders', *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 7, No. 1 (November 2010), pp. 30-33

OWASP *Cornucopia* (https://www.owasp.org/index.php/OWASP_Cornucopia)

OWASP *Hacking* (https://www.owasp.org/index.php/OWASP_Hacking-the_Pentest_Tutor_Game)

OWASP Proactive Controls (https://www.owasp.org/index.php/OWASP_Proactive_Controls)

OWASP *Snakes and Ladders* (https://www.owasp.org/index.php/OWASP_Snakes_and_Ladders)

OWASP *STING* (https://www.owasp.org/index.php/OWASP_STING_Game_Project)

OWASP Top Ten Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

PA Consulting (https://www.paconsulting.com/industries/aerospace-defence-security/)

Packer, Jan, 'Learning for Fun: The Unique Contribution of Educational Leisure Experiences, *Curator*, Vol. 49, Issue 3 (July 2006), pp. 329-344

Paganini, Pierluigi, 'NATO officially recognizes cyberspace as a warfare domain', *Security Affairs*, 18 June 2016

Palmer, Catherine, 'Everyday risks and professional dilemmas: fieldwork with alcohol-based (sporting) subcultures', *Qualitative Research*, Vol. 10, Issue 4 (2010), pp. 421-440

Park, Madison and Dana Ford, 'North Korea to U.S.: Show evidence we hacked Sony', *CNN*, 14 January 2015

Parliamentary Office of Science and Technology, 'Security of UK Food Supply', POST Note Number 556, June 2017

Past Perspectives, 'War in Binni Game Rules', (2016) (http://www.professionalwargaming.co.uk/WIBRules.pdf)

Perla, Peter P. (1990), *The Art of Wargaming: A Guide for Professionals and Hobbyists* (Naval Institute Press: Annapolis, Maryland)

Perla, Peter P. and ED McGrady, 'Why Wargaming Works', *Naval College Review*, Summer 2011, Vol. 64, No. 3, pp. 111-130

Perla, Peter P., 'Operations Research, Systems Analysis, and Wargaming: Riding the Cycle of Research', in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge), pp. 159-182

Perla, Peter P., Michael C. Markowitz, Christopher Weuve, Karin Duggan and Leesa Woodard, 'Wargame-Creation Skills and the Wargame Construction Kit', Centre for Naval Analysis (October 2002)

Pfleeger, Shari Lawrence, M. Angela Sasse and Adrian Furnham, 'From Weakest Link to Security Hero: Transforming Staff Security Behavior', *Homeland Security & Emergency Management*, Vol. 11, No. 4 (2014), pp. 489-510

Phillips, Whitney (2015), *This Is Why We Can't Have Nice Things – Mapping the Relationship between Online Trolling and Mainstream Culture* (MIT Press: Cambridge, MA)

Pieke, Frank, 'Serendipity: reflections on fieldwork in China', in Paul Dresch, Wendy James and David Parkin, eds. (2000), *Anthropologists in a Wider World: Essays on Field Research* (Berghahn: New York), pp. 129-150

Pink, Sarah (2007), *Doing Visual Ethnography: Images, Media and Representation in Research*, 2nd ed. (SAGE: London)

Pouliot, Vincent (2010), *International Security in Practice: The Politics of NATO-Russia Diplomacy* (Cambridge University Press: Cambridge)

Prensky, Marc, 'The motivation of gameplay: The real twenty-first century learning revolution', *On the Horizon*, Vol. 10, No. 1 (2002), pp. 5-11

Privacy card pack and instructions, 2012 (https://vome.org.uk/files/2012/05/PRIVACY-game-card-pack-and-instructions-lo-res.pdf)

Punch, Samantha, 'Hidden struggles of fieldwork: Exploring the role and use of field diaries', *Emotion, Space and Society*, Vol. 5 (2012), pp. 86-93

Purvis, Lt Col Rob and Col Scott A. Forsythe, 'Cyber Wargame Examines Policy and Strategic Issues', *Collins Center Update*, Vol. 15, Iss. 1 & 2 (March 2013), p. 6

Rea, Dan, Kelly Price Millican, and Sandy White Watson, 'The Serious Benefits of Fun in the Classroom', *Middle School Journal*, Vol. 31, Issue 4 (2000), pp. 23-28

Reed, Jason, Yiru Zhong, Lynn Terwoerds and Joyce Brocaglia, 'The 2017 Global Information Security Workforce Study: Women in Cybersecurity', Frost & Sullivan White Paper

Reeves, Carla L., 'A difficult negotiation: fieldwork relations with gatekeepers', *Qualitative Research*, Vol. 10, Issue 3 (2010), pp. 315-331

Reinbold, Fabian, 'Germany Prepares for Possible Russian Election Meddling', *Spiegel Online*, 7 September 2017 (http://www.spiegel.de/international/germany/how-germany-is-preparing-for-russian-election-meddling-a-1166461.html)

Rid, Thomas and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, Vol. 38, Nos. 1-2 (2015), pp. 4-37

Rid, Thomas, 'How Russia Pulled Off the Biggest Election Hack in U.S. History', *Esquire*, 20 October 2016 (http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/)

Rid, Thomas, Twitter post, 14 March 2018 (https://twitter.com/ridt/status/973988732801036302)

Ridden, Paul, 'Ideum and 3M Touch Systems launch new Platform 46 multi-touch tables', *New Atlas*, 6 June 2013 (https://newatlas.com/ideum-3m-platform-multitouch-tables/27823/)

Rieb, Andreas and Ulrike Lechner, 'Operation Digital Chameleon – Towards an Open Cybersecurity Method', Proceedings of the 12th International Symposium on Open Collaboration (OpenSym '16), Article 7, 2016

Rivoal, Isabelle and Noel B. Salazar, 'Contemporary ethnographic practice and the value of serendipity', *Social Anthropology*, Vol. 21, Issue 2 (2013), pp. 178-185

Rosenzweig, Paul, 'International Law and Private Actor Active Defence Measures', *Stanford Journal of International Law*, Vol. 50, No. 1 (2014), pp. 103-118

Ross, David O., 'Investigating the Fundamentals of the Third Generation Wargame: Wargaming, a Course for Future Development', In House Final Technical Report, Air Force Research Laboratory Information Directorate, March 2008

Roth, Andrew, 'Vladimir Putin secures record win in Russian presidential elections', *The Guardian*, 19 March 2018 (https://www.theguardian.com/world/2018/mar/19/vladimir-putin-secures-record-win-in-russian-presidential-election)

Rubel, Robert C., 'The Epistemology of War Gaming', *Naval War College Review*, Vol. 59, No. 2 (Spring 2006), pp. 108-128

Rundstrom Williams, Tracy, 'Exploring the Impact of Study Abroad on Students' Intercultural Communication Skills: Adaptability and Sensitivity', *Journal of Studies in International Education*, Vol. 9, No. 4 (Winter 2005), pp. 356-371

Sabin, Philip, 'Playing at War: The Modern Hobby of Wargaming', in T. J. Cornell and T. B. Allen, eds. (2002), *War and Games* (Boydell Press: Woodbridge), pp. 193-221

Sabin, Philip (2012), *Simulating War – Studying Conflict through Simulation Games* (Continuum: London)

Sabin, Philip, 'Wargaming in higher education: Contributions and challenges', *Arts & Humanities in Higher Education*, Vol. 14, No. 4 (2015), pp. 329-348

Sabin, Philip, 'Wargames as an Academic Instrument', in Pat Harrigan and Matthew G. Kirschenbaum, eds. (2016), *Zones of Control: Perspectives on Wargaming* (MIT Press: Cambridge, MA), pp. 421-438

Salen, Katie and Eric Zimmerman (2004), *Rules of Play – Game Design Fundamentals* (MIT Press: Cambridge, MA)

Salisbury, John and Tom Cole, 'Grounded Theory in Games Research: Making the Case and Exploring the Options', *DiGRA/FDG '16 - Proceedings of the First International Joint Conference of DiGRA and FDG*, Vol. 13, No. 1 (August 2016)

Sanger, David E. (2012a), 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times*, 1 June 2012 (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)

Sanger, David E. (2012b), *Confront and Conceal – Obama's Secret Wars and Surprising Use of American Power* (Crown: New York)

Sanjek, Roger, 'A Vocabulary for Fieldnotes', in Roger Sanjek, ed. (1990), *Fieldnotes: The Makings of Anthropology* (Cornell University Press: Ithaca), pp. 92-121

Santayana, George (1906), *The Life of Reason or the Phases of Human Progress* (New York: Charles Scribner's Sons)

SC Staff, 'WannaCry in the NHS: who takes responsibility?', *SC Magazine*, 15 May 2017 (https://www.scmagazineuk.com/wannacry-in-the-nhs-who-takes-responsibility/article/661492/)

Schaper, Eva, 'Fiction and the Suspense of Disbelief', *The British Journal of Aesthetics*, Vol. 18, Issue 1 (1978), pp. 31-44

Schmitt, Michael and Liis Vihul (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press: Cambridge)

Schneider, Jacquelyn, 'What War Games Tell Us About the Use of Cyber Weapons in a Crisis', *Council on Foreign Relations*, 21 June 2018 (https://www.cfr.org/blog/what-war-games-tell-us-about-use-cyber-weapons-crisis)

Schneider, Jacquelyn, Benjamin Schechter and Rachael Shaffer, 'Navy – Private Sector Critical Infrastructure War Game 2017 Game Report' (2017) (http://www.nwcfoundation.org/Files/Admin/Corp%20Logos/Navy-Private%20Sector%20Critical%20Infrastructure%20War%20Game%20Report%20%281%29%20%282%29.pdf)

Schwartz, Martin A., 'The importance of stupidity in scientific research', *Journal of Cell Science*, 121: 1771 (2008)

Schwartz, Roger (2002), *The Skilled Facilitator: A Comprehensive Resource for Consultants, Facilitators, Managers, Trainers, and Coaches*, 2nd ed. (Josey-Bass: New York)

Scott, John C., 'Review of *The Discovery of Grounded Theory: Strategies for Qualitative Research* by Barney G. Glaser and Anselm L. Strauss', *American Sociological Review*, Vol. 36., No. 2 (April 1971), pp. 335-336

Scott, Ridley (1982), *Bladerunner*

Scruby, Jack, *All About War Games* (publication details unknown)

Secure Workspaces (https://www.teachprivacy.com/?healthcarelibrary=secure-workspaces-game – note: requires login access)

SecureNinjaTV, 'DEF CON 24 > MAELSTROM- A HACKER BOARD GAME', YouTube, 2 November 2016 (https://www.youtube.com/watch?v=sBJW3x-4u3g)

Setear, John K., 'Simulating the Fog of War', RAND, February 1989

Shor, Peter W., 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms in a Quantum Computer', *SIAM Review*, Vol. 41, Issue 2 (1997), pp. 303-332

Shtasel, Derri L., Raquel E. Gur, P. David Mozley, 'Volunteers for Biomedical Research: Recruitment and Screening of Normal Controls', *Archives of General Psychiatry*, Vol. 48, No. 11 (November 1991), pp. 1022-1025

Simpson, William L., Jr., 'A Compendium of Wargaming Terms' (2017) (https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Wargaming%20Department/A%20Compendium%20of%20Wargaming%20Terms%2020%20Sept%202017.pdf?sr=b&si=DNNFileManagerPolicy&sig=BEh3XmMzUbqnHm2SIms6QAWn5YWCMWBWnU8Ira1Oud8%3D)

Sluka, Jeffrey A., 'Reflections on Managing Danger in Fieldwork: Dangerous Anthropology in Belfast', in Antonius C. G. M. Robben and Jeffrey A. Sluka, eds. (2012), *Ethnographic Fieldwork: An Anthropological Reader*, 2nd ed. (Wiley-Blackwell: Chichester), pp. 283-296

Smelkovs, Konrads, 'Bank cyber attacks highlight the need to simulate war games', 2015 (http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/Bank-cyber-attacks-highlight-the-need-to-simulate-%E2%80%98war-games%E2%80%99.aspx, note that link is now defunct)

Smith, Solomon K., 'Pounding Dice into Musket Balls: Using Wargames to Teach the American Revolution', *The History Teacher*, Vol. 46, No. 4 (August 2013), pp. 561-576

Snellman, Pekka, Twitter post, 23 January 2017 (https://twitter.com/PekkaSnellman/status/823498345415057408)

Somers, James (2013), 'The Man Who Would Teach Machines to Think', *The Atlantic*, November 2013 (https://www.theatlantic.com/magazine/archive/2013/11/the-man-who-would-teach-machines-to-think/309529/)

Sood, Harpreet, Keith McNeil and Bruce Keogh, 'Chief clinical information officers: clinical leadership for a digital age', *BMJ*, 358:j3295, July 2017

Specht, Robert D., 'War Games', P-1041, RAND Corporation, March 1957

Spot the Risks (https://www.teachprivacy.com/?privlibrary=spot-risks-privacy-security – note: requires login access)

Stacey, Kiran, 'US and UK to wage cyber war games on City of London', *Financial Times*, 16 January 2015 (http://www.ft.com/cms/s/0/87b2783e-9cd2-11e4-adf3-00144feabdc0.html#axzz3jqH31uUj)

Stebbins, Robert A, 'The Role of Humour in Teaching: Strategy and Self-expression', in Peter Woods, ed. (2012), *Teacher Strategies: Explorations in the Sociology of the School* (Routledge: Abingdon), pp. 84-97

Stedman, Alex, 'Leaked Sony Emails Reveal Nasty Exchanges and Insults', *Variety*, 9 December 2014 (http://variety.com/2014/film/news/leaked-sony-emails-reveal-nasty-exchanges-and-insults-1201375511/)

Stemp, Robert, 'MOR at NPS', *Phalanx*, Vol. 24, No. 1 (March 1991), pp. 13-15

Stone Paper Scissors, 'Humanity Will Prevail Game Rules', version 6.02 (January 2018)
(http://theuniverse.org.uk/rules/hwp/hwp%20campaign%20rules%20v6.02.pdf)

Strayer, Robert (1998), *Why did the Soviet Union Collapse? Understanding Historical Change* (M. E. Sharpe: New York)

Stremba, Bob and Christian A. Bisson, 'Teaching Theory, Facts, and Abstract Concepts Effectively', in Bob Stremba and Christian A. Bisson, eds. (2009), *Teaching Adventure Education Theory: Best Practices* (Human Kinetics: Champaign), pp. 11-22

Suddaby, Roy, 'From the Editors: What Grounded Theory is Not', *The Academy of Management Journal*, Vol. 49, No. 4 (August 2006), pp. 633-642

SyHacked (https://syhacked.com/)

Symantec, 'Dragonfly: Cyberespionage Attacks Against Energy Suppliers', 7 July 2014
(http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf)

Tajfel, Henri, 'Cognitive aspects of prejudice', *Journal of Biosocial Science*, Vol. 1, Issue S1 (1969), pp. 173-191

Taylor, James G., 'Solving Lanchester-Type Equations for "Modern Warfare" with Variable Coefficients, *Operations Research*, Vol. 22, No. 4 (July-August 1974), pp. 756.770

Taylor, Jerome, 'Hacktivists take control of internet security firms', *The Independent*, 8 February 2011
(https://www.independent.co.uk/news/media/online/hacktivists-take-control-of-internet-security-firms-2207440.html)

Taylor, Rod, 'Climate change can be kids' play', *Sunday Canberra Times*, 29 October 2017

'The UK Cyber Security Strategy: Protecting and Promoting the UK in a digital world', Cabinet Office, November 2011

Thomas, Gary and David James, 'Reinventing Grounded Theory: Some Questions about Theory, Ground and Discovery', *British Educational Research Journal*, Vol. 32, No. 6 (December 2006), pp. 767-795

Thompson, Michael F. and Cynthia E. Irvine, 'CyberSIEGE Scenario Design and Implementation', 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (2014)

Thomson, Ian, 'Snowden: US and Israel *did* create Stuxnet attack code', *The Register*, 8 July 2013 (https://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/)

Tibbs, Hardin, *The Global Cyber Game: Achieving strategic resilience in the global knowledge society*, Defence Academy of the United Kingdom Cyber Inquiry Report, 2013

Toles-Patkin, Terri, 'Rational Coordination in the Dungeon', *The Journal of Popular Culture*, Vol. 20, Issue 1 (Summer 1986), pp. 1-14

U.S. Copyright Office, 'Games', FL-108, reviewed April 2016 (https://www.copyright.gov/fls/fl108.pdf)

Vamosi, Robert, 'Anonymous hackers take on the Church of Scientology', *CNET*, 25 January 2008 (https://www.cnet.com/news/anonymous-hackers-take-on-the-church-of-scientology/)

Van den Heede, Pieter, Kees Ribbens, Jeroen Jansz, 'Replaying Today's Wars? A Study of the Conceptualization of Post-1989 Conflict in Digital "War" Games', *International Journal of Politics, Culture, and Society* (2017), pp. 1-22

Vlahos, Michael, 'Wargaming, an Enforcer of Strategic Realism: 1919-1942', *Naval College Review*, Vol. 39, No. 2 (1986), pp. 7-22

VOME (http://vome.org.uk/about/)

Wagner, Helmut R., 'Review of *The Discovery of Grounded Theory: Strategies for Qualitative Research* by Barney G. Glaser and Anselm L. Strauss', *Social Forces*, Vol. 46, No. 4 (June 1968), p. 555

Walker, Miriam, Leila Takayama and James A. Landay, 'High-Fidelity or Low-Fidelity, Paper or Computer? Choosing Attributes when Testing Web Prototypes', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, September 2002, vol. 46, no. 5, pp. 661-662

Wallman, Jim, 'It's Only A Game – Game Design Methodology', version 3 (2007) (http://www.jimwallman.org/clwg/its%20only%20a%20game%202.pdf)

Walny, Jagoda, 'Supporting Everyday Thinking Practices in Information Visualization Interfaces', *ITS 2014 - Doctoral Symposium*, 2014, pp. 479-484

Walraet, Matthieu, ‘A Googolplex of Go Games’, unpublished research paper, 2016 (http://matthieuw.github.io/go-games-number/GoGamesNumber.pdf)

Ward, Mark, ‘What’s involved in cyber war games?’, *BBC*, 16 January 2015 (http://www.bbc.co.uk/news/technology-30853501)

Watt, Nicholas, ‘US and UK plan cyber “war games” to test resilience’, *The Guardian*, 16 January 2015 (http://www.theguardian.com/technology/2015/jan/16/cyber-war-games-uk-us-intelligence)

Weisberg, Deena Skolnick, Audrey K. Kittredge, Kathy Hirsh-Pasek, Roberta Michnick Kolinkoff and David Klahr, ‘Making play work for education’, *The Phi Delta Kappan*, Vol. 96, No. 8 (May 2015), pp. 8-13

Wells, Kathleen, ‘The strategy of grounded theory: Possibilities and problems’, *Social Work Research*, Vol. 19, No. 1 (March 1995), pp. 33-37

Weuve, Christopher A., Peter P. Perla, Michael C. Markowitz, Robert Rubel, Stephen Downes-Martin, Michael Martin and Paul V. Vebber, ‘Wargame Pathologies’, CRM D0010866.A1/Final, September 2004

Whittam, Alexander M. and Whitney Chow, ‘An educational board game for learning and teaching burn care: A preliminary evaluation’, *Scars, Burns & Healing*, Vol. 3, Issue 1 (2017), pp. 1-5

Wiederman, Michael W., ‘Volunteer bias in sexuality research using college student participants’, *The Journal of Sex Research*, Vol. 36, Issue 1 (1999), pp. 59-66

Wiggins, Warren, ‘Adjudication in Game Design: An Introduction', United States Naval War College

Wiggins, Warren, ‘War Game Adjudication: Adjudication Styles’, United States Naval War College

Wilcox, Phil, ‘The true impact of a cyber breach on share price’, *Computer Weekly*, March 2017 (https://www.computerweekly.com/opinion/The-true-impact-of-a-cyber-breach-on-share-price)

Wilhelmson, Nina and Thomas Svensson (2013), *Handbook for planning, running and evaluating information technology and cyber security exercises*, Stephanie Young, trans. (Centre for Asymmetric Threats Studies)

Wilkinson, Michael (2004), *The Secrets of Facilitation – The S.M.A.R.T Guide to Getting Results with Groups* (Jossey-Bass: San Francisco)

Work, Robert O., 'Wargaming and Innovation', Memorandum, 9 February 2015

‘Working for JFC’ (https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment)

World Bank Group, 'Distributed Ledger Technology (DLT) and Blockchain', FinTech Note No. 1 (2017)

Zabalbeascoa Terrán, Patrick, 'Developing translation studies to better account for audiovisual texts and other new forms of text production : with special attention to the TV3 version of Yes, Minister', Doctoral thesis, Universitat de Lleida, 1993

Zadelhoff, Marc van, 'Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It', *Harvard Business Review*, 4 May 2017 (https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it)

Zero Days (2016), dir. Alex Gibney

Zittrain, Jonathan L., 'Reflections on Internet Culture', *Journal of Visual Culture*, Vol. 13, Issue 3 (2014), pp. 388-394

Ziv, Avner, 'Humour as a Social Corrective', in Laurence Behrens and Leonard J. Rosen, eds. (1988), *Writing and Reading Across the Curriculum*, 3rd ed. (Scott, Foresman & Co.: Glenview, Il), pp. 356-360