



Sharon Wiltshire

An Investigation of Influences on Deterrence in Cyberspace

Faculty of Engineering and Applied Sciences
PhD Defence and Security

Doctor of Philosophy
Academic Year: 2024-2025

Supervisor: Dr K McNaught
Associate Supervisor: Prof R Massie
May 2025



Faculty of Engineering and Applied Sciences
PhD Defence and Security

Doctor of Philosophy

Academic Year 2024-2025

Sharon Wiltshire

An Investigation of Influences on Deterrence in Cyberspace

Supervisor: Dr K McNaught
Associate Supervisor: Prof R Massie
May 2025

© Cranfield University 2025. All rights reserved. No part of this publication may be reproduced without the written permission of the copyright owner.

Academic integrity declaration

I declare that:

- the thesis submitted has been written by me alone.
- the thesis submitted has not been previously submitted to this university or any other.
- that all content, including primary and/or secondary data, is true to the best of my knowledge.
- that all quotations and references have been duly acknowledged according to the requirements of academic research.

I understand that to knowingly submit work in violation of the above statement will be considered by examiners as academic misconduct.

Abstract

Deterrence, including deterrence in cyberspace, is typically seen in terms of a cost-benefit calculus. This fails to take account of the wider context of the situation, the cultural factors influencing the parties and the differing perceptions they have. While the existing literature has acknowledged the importance of perception and culture, it contains no demonstration of how to address them. Further, deterrence is viewed as a single event without a past or a future, which does not reflect the reality of ongoing or developing relationships and situations.

This research takes a radical approach in seeking to address these issues, and how they can be taken into account in planning deterrence activities in cyberspace. It uses a critical realist ontology and employs mixed methods research to identify the factors relevant to deterrence through which the deterrer can influence the perceptions of the deterree and thus improve the likelihood of success of their deterrence activity. The primary research and its findings, particularly those from qualitative interviews with relevant experts, address the importance of the perceptions of the deterree and relevant cultural factors, together with an articulation of the wider context and the changing nature of the relationship between the parties in deterrence.

Conclusions from the research emphasise the importance of empathy for the deterree, seeing the situation from their viewpoint. Empathy can, however, present a challenge, and the research recognises this by developing an initial framework to help those planning deterrence activities to take relevant factors into account. The framework does not directly set out the way forward but poses questions, the answers to which will inform discussion and decisions about courses of action.

The research thus makes a valuable contribution to knowledge by taking a wider approach to deterrence in cyberspace than previous academic work.

Keywords: credibility, culture, empathy, escalation, framework, perception

Acknowledgements

I would like to thank all those who have supported and encouraged me through this research, including family, friends and colleagues. I have particularly benefitted from the sound advice and suggestions of Prof Ruth Massie and Dr Ken McNaught, my supervisors at Cranfield University. My greatest thanks go to those who contributed to the research, especially those who gave up their time and offered insights into their experience during the interviews: without them this research would not have been possible.

The work described in this thesis together with the conclusions are entirely my own, and should not be taken as implying any views or policies relating to the Ministry of Defence.

Table of Contents

Academic integrity declaration.....	i
Abstract	ii
Acknowledgements	iv
List of Figures.....	x
List of Tables	xii
List of Abbreviations	xiii
1 Introduction.....	1
1.1 Context	1
1.2 Research gap and novelty of the research	2
1.3 Aim and objective.....	4
1.4 Overview of research design and methodology	6
1.5 Terminology	7
1.5.1 Deterrence in cyberspace	7
1.5.2 Deterrer and deterree	8
1.5.3 Deterrence declaration	10
1.6 Contribution	10
1.7 Thesis layout.....	11
2 Review of Literature	14
2.1 Chapter overview.....	14
2.2 Search process.....	15
2.3 What is Cyberspace?.....	15
2.3.1 Cyberspace and other operational domains.....	18
2.4 What is Deterrence?	20
2.4.1 Deterrence in history	22
2.4.2 Deterrence by punishment versus deterrence by denial	24
2.4.3 Communication and perception.....	25
2.4.4 Credibility	28
2.5 Deterrence in cyberspace	29
2.5.1 Deterrence by punishment and deterrence by denial	32
2.5.2 Describing deterrence in cyberspace	34
2.6 Offence-Defence Balance	36
2.7 Security Dilemma.....	38
2.8 Cognitive Aspects	40
2.9 Cultural differences	44
2.9.1 Models for practical insights	44
2.9.2 Strategic culture	47
2.10 Existing Theoretical Models and Frameworks	49
2.10.1 Snyder (1961): nuclear deterrence.....	49
2.10.2 Straub (2019): combining likelihood, impact and deterrent value ...	50
2.10.3 Sharp (2017): credibility and persuasiveness.....	51

2.10.4 Halas (2019): Boolean logic	52
2.10.5 Lindsay (2015): cost and uncertainty.....	54
2.10.6 Healey and Jenkins (2019): “rough-and-ready”	55
2.10.7 Belfer Center (Voo et al., 2022): National Cyber Power Index	55
2.10.8 Edwards et al. (2017): attribution - the “Blame Game”	57
2.10.9 Cui et al. (2017): attacker in a “three player” game	59
2.10.10 Valeriano and Maness (2015): taxonomy for incidents and disputes.....	59
2.10.11 Agrafiotis et al. (2018): taxonomy of cyber harms	59
2.10.12 McDermott (2019): emotion and response	61
2.10.13 Powell (2002): bargaining theory.....	61
2.10.14 Summary.....	62
2.11 Chapter Summary.....	63
3 Conceptual Framework	65
3.1 Chapter overview.....	65
3.2 Introduction	65
3.3 Conceptual Framework stage 1: initial	66
3.4 Goodman’s (2010) elements of deterrence.....	67
3.5 Conceptual framework stage 2: progression.....	70
3.6 Potential factors for research	70
3.7 Factors to be considered	72
3.8 Conceptual Framework stage 3: outline for research.....	76
3.9 Interplay: the parties and their relationship	77
3.10 Chapter Summary.....	80
4 Research Methodology	81
4.1 Chapter overview.....	81
4.2 Introduction	82
4.3 Ontology	82
4.4 Epistemology	86
4.5 Cultural lens.....	87
4.6 Research strategy.....	89
4.7 Methodology	90
4.8 Methods	92
4.8.1 Quantitative methods	92
4.8.2 Qualitative methods.....	94
4.9 Sample selection.....	95
4.10 Plan for data collection.....	98
4.10.1 Delphi Questionnaire.....	99
4.10.2 Interviews	99
4.10.3 Group workshop.....	100
4.11 Data collection	100
4.12 Participant identifiers.....	101

4.13 Ethical considerations and data handling.....	103
4.13.1 Ethical approval.....	103
4.13.2 Data storage.....	104
4.14 Chapter summary	104
5 Questionnaire: Data Collection, Review and Results	105
5.1 Chapter overview.....	105
5.2 Approach to data collection.....	105
5.2.1 Delphi method	106
5.2.2 Sample	107
5.2.3 Questionnaire	107
5.3 Data collection and management	109
5.3.1 Responses	109
5.4 Results.....	111
5.4.1 Scenario	111
5.4.2 Additional factors.....	112
5.4.3 Factors seen as most relevant	114
5.5 Next steps.....	116
5.6 Chapter summary	117
6 Group Workshop: Data Collection, Review and Results	118
6.1 Chapter overview.....	118
6.2 Approach to data collection.....	118
6.3 Data collection	119
6.3.1 Scenario	119
6.3.2 Individual reflection.....	121
6.3.3 Group discussion	122
6.4 Reflection.....	125
6.5 Chapter summary	125
7 Interviews: Data Collection, Review and Results	127
7.1 Chapter overview.....	127
7.2 Approach to data collection.....	127
7.3 Codification and review.....	130
7.4 Presenting the interview data.....	134
7.5 Defining deterrence in cyberspace.....	134
7.6 Escalation	136
7.7 Credibility	140
7.8 Attribution.....	142
7.9 Perception of external states	144
7.10 Effect on the other state.....	146
7.11 Culture	150
7.12 Impact.....	154
7.13 Understanding of the context	155
7.14 Other remarks	158

7.15 Chapter summary	159
8 Discussion of Findings	160
8.1 Chapter overview	160
8.2 Defining deterrence in cyberspace.....	161
8.3 Escalation	162
8.4 Credibility	165
8.5 Attribution.....	167
8.6 Perception of external states	169
8.7 Effect on the other state	170
8.8 Culture	171
8.9 General discussion	173
8.10 Review of the approach	178
8.11 Conceptual Framework revisited.....	179
8.12 Chapter summary	181
9 Developing a Framework.....	183
9.1 Chapter overview	183
9.2 Introduction	183
9.3 Purpose of framework.....	185
9.4 Structure of the framework.....	186
9.4.1 Escalation.....	187
9.4.2 Credibility	187
9.4.3 Attribution	188
9.4.4 External Perception	189
9.4.5 Other party's services and economy	190
9.4.6 Cultural factors	190
9.5 Format of the framework.....	191
9.5.1 Escalation.....	192
9.5.2 Credibility	192
9.5.3 Attribution	192
9.5.4 External perception	192
9.5.5 Other party's services and economy	193
9.5.6 Cultural factors	193
9.6 Review of the framework	193
9.6.1 Escalation.....	193
9.6.2 Other feedback.....	194
9.6.3 Summary.....	196
9.7 Chapter summary	197
10 Conclusions and Future Work	198
10.1 Chapter overview	198
10.2 Review of objective and Research Questions.....	198
10.3 Conclusions drawn.....	200
10.3.1 The role of perception	200

10.3.2 Factors relevant to deterrence in cyberspace	201
10.3.3 Models.....	203
10.3.4 Cultural issues.....	204
10.3.5 Framework	205
10.3.6 Summary of conclusions	205
10.4 Critical reflection and limitations of the work	206
10.4.1 Research question	206
10.4.2 UK bias.....	207
10.4.3 Theoretical nature of the research	208
10.4.4 Empathy	208
10.4.5 Critical realism.....	209
10.5 Contribution to knowledge and theory.....	210
10.6 Recommendations for policy and practice	211
10.7 Future work.....	212
10.8 Final thoughts	214
References	216
Copyright Permissions	230
Appendix A Questionnaire	231
Appendix B Interview Script	236
Appendix C Workshop Materials.....	242
Appendix D Participant Background Representation using Binary and Hexadecimal encoding.....	248
Appendix E Questionnaire Responses and Comments	251
Appendix F Two States used in Scenario from their Own Viewpoints	261
Appendix G Workshop Outputs	263
Appendix H Initial Proposed Framework.....	266

List of Figures

Figure 1-1: The actors change places as the situation progresses, with each stage as perceived by the 'victim' at that stage	9
Figure 2-1: Layers of cyberspace and their relationship with the three effect dimensions (from Great Britain. Ministry of Defence, 2022, p7)	17
Figure 2-2: Visualising the Offence-Defence balance as a scale with weights which may affect the balance	38
Figure 2-3: The Inglehart-Welzel World Cultural Map - World Values Survey 7 (2022). Source: WVS Wave 7 (2017-2022)	46
Figure 2-4: Meyer's culture map with examples (adapted from Meyer, 2014) ..	47
Figure 2-5: Straub's cross-domain (medium) deterrence (Straub, 2019, p5) ...	51
Figure 2-6: Charts for the National Cyber Power Index (taken from Voo et al. 2022). (a) Radar diagram showing combined capability and intent scores for the United Kingdom. (b) Capability scores for the Norms objective.	57
Figure 2-7: Graphic representation of the "Blame Game" (simplified from Edwards et al., 2017, p2827).....	58
Figure 2-8: Examples of taxonomy of organisational cyber harms (Agrafiotis et al., 2018).....	60
Figure 3-1: Initial conceptual framework.....	66
Figure 3-2: Interpretation of relationships between Goodman's (2010) 8 elements of deterrence	68
Figure 3-3: Each party attributes its own view to the other	69
Figure 3-4: Interpretation of relationships and determination in Goodman's (2010) 8 elements of deterrence	69
Figure 3-5: Conceptual framework reflecting development of Goodman's framework for deterrer and deterree	70
Figure 3-6: Factors affecting deterree's cost benefit calculus which deterrer can influence	77
Figure 3-7: (a) The parties change places as a situation progresses; (b) each party sees itself as the victim and the other as the aggressor	79
Figure 3-8: One-way relationship from the viewpoint of the victim/deterrer	80
Figure 4-1: Critical realist stratified ontology	83
Figure 4-2: Critical realist stratified ontology illustrating different perceptions when the sun is obscured	84

Figure 4-3: Critical realist stratified ontology illustrating polarised views of the security dilemma.....	86
Figure 4-4: Sequential research design with additional concurrent element (adapted from Saunders et al., 2019, p182)	98
Figure 5-1: Questionnaire respondent expertise (multiple responses permitted)	110
Figure 5-2: Questionnaire output: selected factors.....	116
Figure 7-1: Expertise of interviewees (multiple responses allowed)	129
Figure 7-2: Number of areas of expertise claimed by interviewees	130
Figure 7-3: Initial coding scheme.....	131
Figure 7-4: Amended coding scheme after first interview.....	132
Figure 7-5: Final coding scheme	133
Figure 7-6: Screenshot showing part of final coding spreadsheet.....	134
Figure 8-1: Interpretation of relationships in Goodman's (2010) 8 elements of deterrence	174
Figure 8-2: Factors affecting the deterree's cost-benefit calculus which the deterrer should consider	180
Figure 8-3: Factors for deterrer consideration to inform their viewpoint in line with Goodman's 8 elements of deterrence.....	181

List of Tables

Table 2-1: The logic of general deterrence seen from the perspective of Boolean logic (from Halas, 2019, p434)..... 53

Table 2-2: McDermott's taxonomy of conditions, emotions and responses (from McDermott, 2019, p321) 61

Table 3-1: Factors considered for research..... 72

Table 3-2: World views of parties in deterrence situation, including researcher78

Table 4-1: Hexadecimal values to indicate background(s) of participants 102

Table 8-1: Potential impact of factors on deterree from point of view of deterrer 176

Table D-1: Representation of a single hexadecimal digit using four binary digits 249

Table D-2: Meaning assigned to individual bits forming two hexadecimal digits 249

Table D-3: Examples of descriptor coding..... 250

List of Abbreviations

BDA	Battle Damage Assessment
CNI	Critical National Infrastructure
COA	Course Of Action
CR	Critical Realism
DIME	Diplomatic, Intelligence, Military and Economic
DNC	Democratic National Committee (in US)
DPRK	Democratic People's Republic of Korea
MAD	Mutually Assured Destruction
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NCF	National Cyber Force
NCSC	National Cyber Security Centre
NPJ	Necessity, proportionality and justification
OC	Offensive Cyber
OCO	Offensive Cyber Operations
OPM	Office of Personnel Management (in US)
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
UK	United Kingdom
US	United States (of America)
WVS	World Values Survey

1 Introduction

1.1 Context

Deterrence seeks to prevent an action through fear of the consequences (Schelling, 1966, p71; Great Britain. HM Government, 2015, p23). While for much of the second half of the twentieth century it became largely synonymous with the deterrence of nuclear weapons, deterrence can apply in any context where one party seeks to prevent another from taking some action the first party does not want. It involves two actors, the deterrer and deterree (defined below), who each bring their own viewpoints in interpreting the actions of the other and determining their own actions.

Cyberspace, as the newest domain of military operations, brings new challenges to traditional military approaches (Great Britain. Ministry of Defence, 2022, p4-6). Unlike the other domains of maritime, land, air and space, offensive activity may not be so easily attributable: cyber weapons are not physical artefacts that are clearly visible, and malicious activity may not be readily attributable to the perpetrator. While low-end relatively cheap data exfiltration and malicious activity can be conducted through 'off-the-shelf' tools easily accessible to criminals and others, more sophisticated approaches may be available to the most capable threat actors which include zero-day exploits¹. These are focused on vulnerabilities not openly identified, and which, once exploited, can be patched or otherwise defended against, and so are likely to be single use. Cyber defences are also not as prominent as in other domains, consisting of features in the internal architecture of computer systems such as intrusion detection, anti-malware and monitoring tools.

Similarly, where an offensive capability or an impenetrable defence are obvious in the physical world, a potential aggressor can view these and make an informed

¹ Zero-day exploits are "Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit." (NCSC, quoted in Great Britain. Ministry of Defence, 2022, p72).

decision (their cost-benefit calculation) about whether to mount an attack. In cyberspace, however, these deterrent artefacts, the offensive capability or solid defence, are not obvious, so the potential aggressor's decision is harder. The potential victim, meanwhile, may be keen to deter them, but needs to find a way to clearly demonstrate this in a way that will be understood by the aggressor.

The motivation for this research was to understand how the challenges presented by cyberspace would allow deterrence to be articulated by the deterrer and correctly understood by the deterree. Unlike the other operational domains, it can be hard to distinguish in cyberspace between gathering intelligence and preparatory actions to cause damage to data or systems (Buchanan, 2016, p27). This increases the likelihood of misunderstanding or misperception, where a non-aggressive deterrent action can be seen as aggressive by another party. As will be outlined in the literature review, deterrence relies on communication and its perception, so a key concern is how this can be successfully influenced by the deterrer to give the desired effect.

This research is focused on nation states and in the context of a military state-on-state exchange, from a Western, principally United Kingdom (UK) perspective. As noted in the Review of Literature, the UK uses a definition of cyberspace which is closely aligned to that of other Western states, but one that is very different to that used by some non-Western states, such as Russia and China. Focusing on the UK perspective allows the researcher to draw conclusions appropriate to that environment. Whether these would apply beyond the UK, to other Western or non-Western states, would require further research following a similar approach to that described here, and this is recognised in the Conclusion as a potential area for future work.

1.2 Research gap and novelty of the research

The Review of Literature indicated that the main areas of focus of existing research and literature were:

- Comparing cyber with nuclear deterrence. This was found to be not helpful as cyber and nuclear weapons are very different in nature and effect.

- Describing the cost-benefit calculation for deterrence in cyberspace. The focus has been on the value of the interest (the desired outcome), the costs associated with the action and the penalty measures, which together determine the deterree's cost-benefit calculation. This is so even where an attempt has been made to quantify the effectiveness of cyber deterrence (Lindsay, 2015). No wider context, perception or other cultural factors have been included in descriptions of deterrence.
- Attribution in terms of the difficulty of attributing cyber activity, and processes that would help. While these are relevant in terms of whether attribution would occur, there is little interest in whether attribution might be desirable.

While the perception of each party is a key issue in deterrence, as are cultural differences between the deterrer and deterree, these are not well addressed in the literature. The research gap is, therefore:

To identify the factors which are relevant to the interplay between the deterrer and deterree, including societal and political factors. Deterrence is a cognitive process where credibility and communication are vital, but how can the deterrer identify the factors which may contribute to the deterree's perception and help the deterrer's message to be received and understood as intended?

To address this gap, a different approach must be taken, which takes account of the wider context of the situation, rather than seeing it as a single response to a threat, a "one-shot" game as Lindsay (2015, p59) explicitly described it, where neither past nor future are acknowledged. In reality, however, deterrence is influenced by previous events and will in turn influence future events: it forms part of a story with a past and a future.

A second major departure from existing academic work is the inclusion of cultural factors and the perceptions of the deterree. Culture is widely recognised in the literature as important for deterrence, but it is completely absent from the models

reviewed, and even authors who stress its importance fail to suggest how it can be included in the decision making process leading to deterrence.

This research is, therefore, radical in that it acknowledges both the background which has led to the deterrence situation, and how the deterrer wishes the next part of the story to unfold: should this deterrence activity escalate or calm the situation? Not only that, but it deliberately addresses the importance of taking into account perception and cultural factors relating to the deterree, and seeks to make these part of the deterrer's deterrence posture.

1.3 Aim and objective

As noted above, deterrence involves a deterrer and a deterree, and it must be viewed in the context of a relationship between those parties. The literature indicates that misperception, where the motives and actions of one party are misunderstood by the other, is common in deterrence, and that deterrers may wrongly ascribe their own viewpoint to the deterree. If perception is to be taken into account then using a simple calculation of cost versus benefit will not work, and as Tetlock (2005, p123) notes, "Few of us spontaneously factor other views into our assessments – even points of view that, on second thought, we acknowledge have a nonnegligible likelihood of being right." Further, deterrence does not happen in a vacuum: it is influenced by what has gone before and will in turn influence what follows, and there will be other influences on the deterree. So it is important to consider how perception, the wider context of the relationship between the parties, and the challenges associated with cyberspace can be identified and highlighted in deterrence planning.

This research aims to address the deterrer's perspective to explore their understanding of the wider context and how the deterree will receive their deterrence message, to give deterrence the best chance of success. It does this by considering factors that may be relevant to the deterree and the relationship between the parties, so that the deterrer can try to address these in their planning. It seeks, therefore, to answer the Research Question:

How can the wider context of the deterrer and deterree be addressed when planning deterrence in cyberspace?

This research question is broken down into the following sub-questions:

- RQ1: What is meant by deterrence in cyberspace?
- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

RQ1 seeks clarity about the term deterrence in cyberspace: does it refer to deterrence of cyber activity, using cyber activity to deter non-cyber activity, or both of these? This is an area that the literature is not always clear on, so it is important to be clear on the meaning before proceeding to answer the further sub-questions.

RQ2 addresses the main factors which might be relevant to both parties in a deterrence situation. While the deterrer should be able to articulate their own viewpoint they may not understand that of the deterree, and there are many instances of deterrers, and potential adversaries more generally, seeing the other party in their own image and believing that they are rational actors like themselves. In reality they are likely to be rational actors, but in terms of their own version of rationality which may not match that of the deterrer, and the two parties may well not share the same interests and values. The deterrer must be alive to this likelihood – it has occurred too frequently to be merely a possibility, as shown by the examples given by Payne (2011, p398) – and consider the factors which might be important to the deterree, and then act accordingly. While there will be factors which the deterrer cannot control or influence, those over which the deterrer can exert some level of influence will be those relevant to the interplay between the parties.

Having determined the key relevant factors, RQ3 explores how these can be incorporated into deterrence planning to make deterrence activity more effective. This takes a shortlist of the most relevant factors and reviews each in turn,

culminating in the development of a framework to help those planning deterrence activity in cyberspace to understand not only their own situation but also that of the deterree. The framework is intended to inform and encourage discussion of wider issues to try to see the deterree's viewpoint. There is no simple formula for success, but the framework should at least stimulate thought.

The objective of the research is, therefore, to determine the set of factors most relevant to the interplay of the two parties, and to demonstrate how these factors can be brought into the deterrer's planning process to enable them to better target their deterrence activity with the specific deterree and situation in mind. That should result in the deterrence activity being tuned to have the greatest influence on the deterree, and therefore the best chance of success.

1.4 Overview of research design and methodology

This research adopts the critical realism ontology (Bhaskar, 2008) which views reality as stratified into empirical, actual and real layers. Critical realism is well suited to the subject area because it recognises that different actors will experience different realities and that actors' intentional actions allow them to identify causes and their role as causal agents (Bhaskar, 2008, p117). These causes may be perceptions of different empirical observations of actual events, and thus critical realism aligns well with the different perceptions of the deterrer and deterree. In line with the critical realist ontology, a retroductive research strategy was used, beginning from the actions intended to deter in cyberspace and identifying candidate factors as the structures and mechanisms to be tested and refined.

The research itself used mixed methods with different stages of research in a sequential explanatory design with an initial quantitative questionnaire followed by qualitative semi-structured interviews. The opportunity also arose for a group workshop which provided further qualitative data in a different, but supporting, style to the questionnaire and interview data.

One important point to note is that although perception is central to the research, the researcher is not a psychologist, but has approached perception from a cyber

defence background and perspective. Therefore, the research did not seek to explore psychological factors as such, and instead reflected the researcher's background by focusing on the role of perception in terms of its impact on deterrence in cyberspace. This approach also has the benefit of mirroring the likely backgrounds of the deterrer and deterree in real deterrence situations.

1.5 Terminology

Two specific issues regarding the terminology used in this thesis are important to understand to ensure clarity and consistency of meaning. These are the labels used to describe the parties and the use of the term deterrence in cyberspace rather than cyber deterrence. Additionally, the term deterrence declaration benefits from clarification of its meaning.

1.5.1 Deterrence in cyberspace

The terms 'deterrence' and 'cyberspace' are discussed in the Review of Literature chapter alongside an exploration of their nature. The UK Ministry of Defence (MOD) recognises that deterrence and other influence activity, can use the full range of instruments of national power (Great Britain. HM Government, 2021, p100), namely Diplomatic, Intelligence, Military and Economic (DIME). Within the military sphere this could include activity in any operational domains and will not be restricted to the domain(s) used by the aggressor. Thus it is possible that a cyber attack could prompt response action in a kinetic domain, although the response would need to be proportionate.

The term 'cyber deterrence' is commonly used in the literature, but it is imprecise. It is not clear whether it refers to deterrence of cyber activity (using whatever means), using cyber activity to deter non-cyber activity, or the 'cyber-on-cyber' approach of deterring cyber activity using cyber activity. Most authors use the term without explaining what they mean, as noted in the Review of Literature chapter, although they implicitly adopt an implicit cyber-on-cyber meaning, and even some who explicitly offer a wider definition tend to revert to cyber-on-cyber when discussing potential examples.

To avoid this imprecision of meaning, this thesis uses the term ‘deterrence in cyberspace’ which makes clear that the deterrent activity, at least, is within cyberspace, it still allows for both deterrence *of* cyber activity and deterrence *using* cyber activity, but excludes cyber activity being deterred by non-cyber means.

1.5.2 Deterrer and deterree

Deterrence takes place when a potential aggressor is threatening a potential victim, and the victim seeks to deter the aggressor. The terms ‘aggressor’ or ‘attacker’ and ‘victim’ or ‘defender’ are often used to describe the two parties, but they present several issues:

- The ‘aggressor’ may not have any hostile intent. The situation may be an example of the ‘security dilemma’, discussed in the Review of Literature chapter.
- Expanding on the above point, what matters is not so much the aggressor’s intent as the potential victim’s perception, and whether they consider the threat to be credible. If they do not perceive that the threat is credible then they will determine that they do not need to deter it, whether or not the threat is real.
- Both parties are likely to see themselves as the victim, as they will each see the other’s actions as aggression, as discussed in the literature review (as noted by Lebow and Stein, 1989, p221; Morgan, 2003, p3).
- Third parties looking on will share this confusion between the roles, seeing the perspective according to their more general political support for, or hostility to, the states, and therefore effectively taking sides, even if they do not become directly involved.
- The ongoing nature of the situation means that the aggressor/victim relationship will rotate between the parties as the situation progresses, in much the same way as two people bargaining in a market, where one makes an offer, the other considers, and then they change places. This constant change of roles is discussed in the Conceptual Framework chapter, and is illustrated in Figure 1-1 below.

- The agency to deter sits with the victim, not with the aggressor, in that the victim must decide whether and how they wish to attempt to deter before the aggressor can respond. 'Victim' is a passive word and thus gives the wrong impression of the role of the deterring party.

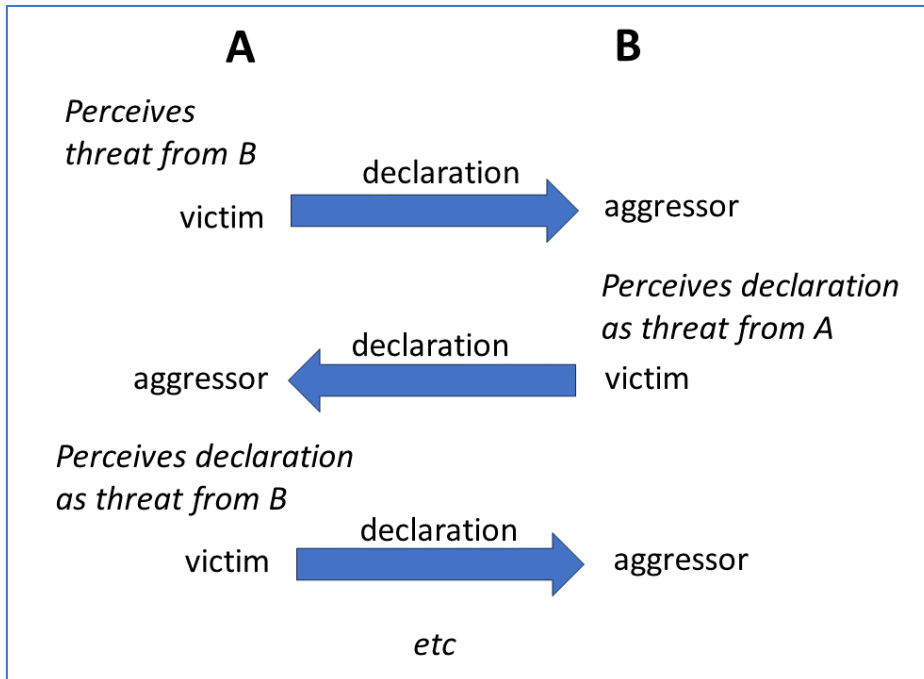


Figure 1-1: The actors change places as the situation progresses, with each stage as perceived by the 'victim' at that stage

In this thesis, therefore, the parties are more precisely referred to as the 'deterrier' and 'deterree', where the deterrier is seeking to deter the deterree from some action. While 'deterred' might be considered a less cumbersome alternative to 'deterree', it includes the tacit assumption that the deterrence has been successful, which may well not be the case. Indeed, the deterree may not even be aware that the deterrier is seeking to deter them. Therefore the terms 'deterrier' and 'deterree' are used within this document because they are accurate and avoid any judgmental inference about the rights and wrongs of the situation. That said, where other authors being cited have used other terms, their terminology has been followed.

1.5.3 Deterrence declaration

The thesis builds on the eight-element model of deterrence proposed by Goodman (2010, p105-6) cited in the Review of Literature. Goodman's model begins with a deterrent declaration made by the deterrer, which includes denial or penalty measures. While the term 'deterrence declaration' suggests an explicit verbal statement of some description, this is not necessarily the case.

An explicit verbal declaration would take the form "if you do *x*, we will do *y*", and could apply against a traditional kinetic threat such as another state's troops massed near the border as "if you invade, we will strike back." In the kinetic operational domains of maritime, land, air and space an explicit statement of this type might be appropriate in some cases. In cyberspace there is no visible signal such as troops massing, and potential evidence might come from intelligence sources or from observation of network activity. A potential aggressor may not want to show their hand openly, as this would undermine the success of their possible offensive activity, and the deterrer likewise might not wish to make their discovery explicit. An implicit approach to deterrence through some action taken might therefore be more appropriate, whether through strengthening defences or demonstrating in some way that the deterrer is capable of striking back.

The term 'deterrent declaration' is therefore used throughout the thesis to describe both explicit statements and implicit messaging through actions.

1.6 Contribution

The radical approach of including wider context and perception within the research is its key contribution to the study of deterrence in cyberspace. It not only explores the factors relevant to deterrence but also introduces culture and how it impacts upon the relationship between the deterrer and deterree, with the deterree's perception of the situation being crucial to successful deterrence. Existing literature has recognised the importance of culture but has failed to demonstrate how to include it and no models have tried to.

It further recognises the changing nature of the parties as a situation progresses, with deterrent activity potentially being viewed by the deterree as aggression,

leading to them seeking to deter and thus becoming the deterrer. This reinforces the importance of the deterree's perception, over which the deterrer can have only partial influence through their messaging and wider activity. To give deterrence the best chance of success, the deterrer needs to show empathy with the deterree to understand the deterree's perspective and respond accordingly. Since this may be difficult in practice, the research contributes a proposed framework to inform decision makers in their planning.

1.7 Thesis layout

Following this introduction, Chapter 2, the Review of Literature, addresses RQ1 by exploring the definition of cyberspace and the nature of deterrence, including issues of perception, before bringing these together to look at the challenges of deterrence in cyberspace. The focus then turns to RQ2, considering the factors relevant to deterrence in cyberspace including the offence-defence balance and the security dilemma. It notes the importance of perception and cultural background, then critically reviews a number of potentially relevant models but finds that none of them address culture.

The Review of Literature leads naturally to the development of the Conceptual Framework in Chapter 3 to address Goodman's (2010) elements of deterrence and other factors identified during the literature review. Each is assessed in terms of whether the deterrer can influence the deterree's view of the factor, leading to a version of the conceptual framework to be used as the basis of the research. The chapter ends with a brief discussion about the relationship of the roles of deterrer and deterree, and how these change places as a situation develops.

Having determined the conceptual framework, Chapter 4 sets out the Research Methodology, recognising how critical realism is an appropriate ontology for this subject, and the cultural lens through which the research has been carried out as well as the potential cultural bias in the research data which will further influence the results of the research. The research strategy, retroduction, is briefly outlined together with its application through a mixed methods methodology using a sequential explanatory design. This leads to an initial discussion of the methods and sampling approach used and the overall plan for data collection, including

the pseudonymous coding of participants, and ethical and data handling considerations.

The detail of Data Collection, Review and Results for each of the three primary research activities is set out in Chapters 5, 6 and 7, covering respectively the Questionnaire, the Group Workshop and the Interviews. All three primary research activities supported RQ2, and the Group Workshop and interviews also supported RQ3. Each chapter outlines the data collection and analysis approach followed by a summary of the results. The questionnaire identified not only the five factors worthy of being taken forward in the interviews, but also suitable interview candidates. The workshop was an independent activity which took place after the questionnaire and just before the interviews, hence its place as the middle chapter of the three chronologically, which was used to give a different, but complementary, approach to exploring factors considered in deterrence planning.

Chapter 8 brings the previous three chapters and the Review of Literature together in the Discussion of Findings in order to answer all three RQs. It reviews the definition of deterrence in cyberspace and the findings about the factors identified as particularly relevant by the research. The importance of empathy is noted, seeing the situation from the deterree's perspective for giving deterrence the best chance of success. The chapter ends by reflecting upon the approach to the research and by developing the conceptual framework from Chapter 2 to reflect the findings.

With the research and analysis now complete, Chapter 9, Developing a Framework, addresses the final part of RQ3 by describing the development of a framework to help those planning deterrence in cyberspace. The framework itself is included with an initial review of its approach.

The thesis ends with Chapter 10, Conclusions and Future Work, by reflecting on how the research has answered the research question. It notes a number of conclusions that can be drawn, as well as critically reflecting on the UK bias and the critical realist ontology. While it acknowledges the limitations of the research, it recognises the value of its contribution by taking a fuller approach to deterrence

in cyberspace than previous academic work, and it fulfils the intent recorded above to take a radical approach including wider context and perception. The chapter concludes with recommendations for future work to build on and further develop this novel approach.

2 Review of Literature

2.1 Chapter overview

This chapter supports the first two research questions:

- RQ1: What is meant by deterrence in cyberspace?
- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?

The chapter starts by describing the approach taken to identifying relevant literature and the reason for the focus on perception. The literature review itself follows, firstly addressing RQ1: “What is meant by deterrence in cyberspace?” This begins with a review of the definitions of cyberspace showing the alignment of the UK MOD view with that of other Western nations and how it differs from those of Russia and China, followed by a discussion of the differences between cyberspace and the conventional domains. Deterrence is then introduced, with its component parts and a brief history to give context to the emphasis of some literature on nuclear deterrence. Types of deterrence are considered together with the challenge presented by communication and perception, particularly the difficulty of not seeing the other party as an image of oneself, all of which will influence the credibility of the deterrence to the deterree.

Bringing the concepts of cyberspace and deterrence together, the challenges of deterrence in cyberspace are described, particularly those relating to credibility, and how deterrence by denial is especially relevant in cyber defence. The approaches of different authors in addressing cyber deterrence are noted as these are relevant to military planning and response, although they are not taken further here as they do not impact directly on perception.

The remainder of the chapter turns to answering RQ2: “What are the main factors relevant to the interplay between the deterrer and deterree?” This begins with an outline of offence-defence theory and the security dilemma, both of which are highly relevant to deterrence in cyberspace. As the discussion so far has shown that the perceptions of the parties are key, cognitive issues are considered, such as bias in interpreting information, how individuals construct a course of action

and the role of emotion. One reason for misunderstanding may be cultural differences, and different approaches to explaining national culture are explored.

Finally, a selection of models which may contribute to understanding deterrence in cyberspace are critically reviewed. These are varied in their intent and approach, but none attempt to consider cultural issues.

2.2 Search process

The search process used to identify relevant literature began by using the search terms “cyber deterrence” and “deterrence” together with reviewing the content of a number of relevant academic journals. This process was repeated at regular intervals to ensure any new literature was identified. References within literature were followed up where appropriate, and in many cases identified further areas of exploration. These included government and military strategy and doctrine from different states, the offence-defence balance, the security dilemma, cyber defence models, perception and cognition, each of which has been subject to a similar approach.

The initial focus of the literature review was the effectiveness of deterrence in cyberspace, but while it quickly became apparent that perception was a key issue it was found that this area was not well addressed in the literature. The role of perception therefore became the primary focus of the research. However, the researcher is not a psychologist, but approached the subject from a cyber defence background and perspective. The research reflected this and did not seek to explore psychology as such but only how perception may affect deterrence in cyberspace.

2.3 What is Cyberspace?

The United Kingdom has declared cyberspace to be an environment of military operations, thus putting it on a par with maritime, land, air and space. Although common parlance suggests that cyberspace is mainly about technology, focusing on “the notional environment in which communication over computer networks occurs” (Oxford English Dictionary, 2015, p2194), academic definitions make clear its breadth. Thus, Libicki (2009, p12) highlights the incorporation of physical,

syntactic and semantic layers, while Barnard-Wills and Ashenden (2012, p2) note its dual nature as both a physical and a social construction. Gray (2013, p20) observes that cyber power is not about the computers or networks themselves but about what they do and what impact they have, and Voo et al. (2022) take a similar view in assessing cyber power against a range of objectives based on the capability and intent of a nation state. The UK government has moved from a purely technical definition in the 2016 National Cyber Security Strategy (Great Britain. HM Government, 2016, p75) to recognising, in the successor 2022 National Cyber Strategy (Great Britain. HM Government, 2021, p18-19), that while cyberspace can be defined in technical terms, people experience it through virtual, logical and physical layers.

While the UK MOD previously included physical, virtual and cognitive elements as domains (Great Britain. Ministry of Defence, 2016, p1), it has more recently adopted a stance complementary to that of the 2022 National Cyber Security Strategy, starting with a technical definition:

“The global environment consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data” (Great Britain. Ministry of Defence, 2022, p1)

but then going on to note that:

“Cyberspace can be thought of as comprising six interdependent layers: social; people; persona; information; network and geographic”

and it incorporates the physical, virtual and cognitive elements as “effect dimensions” (Great Britain. Ministry of Defence, 2022, p7) as shown in Figure 2-1.

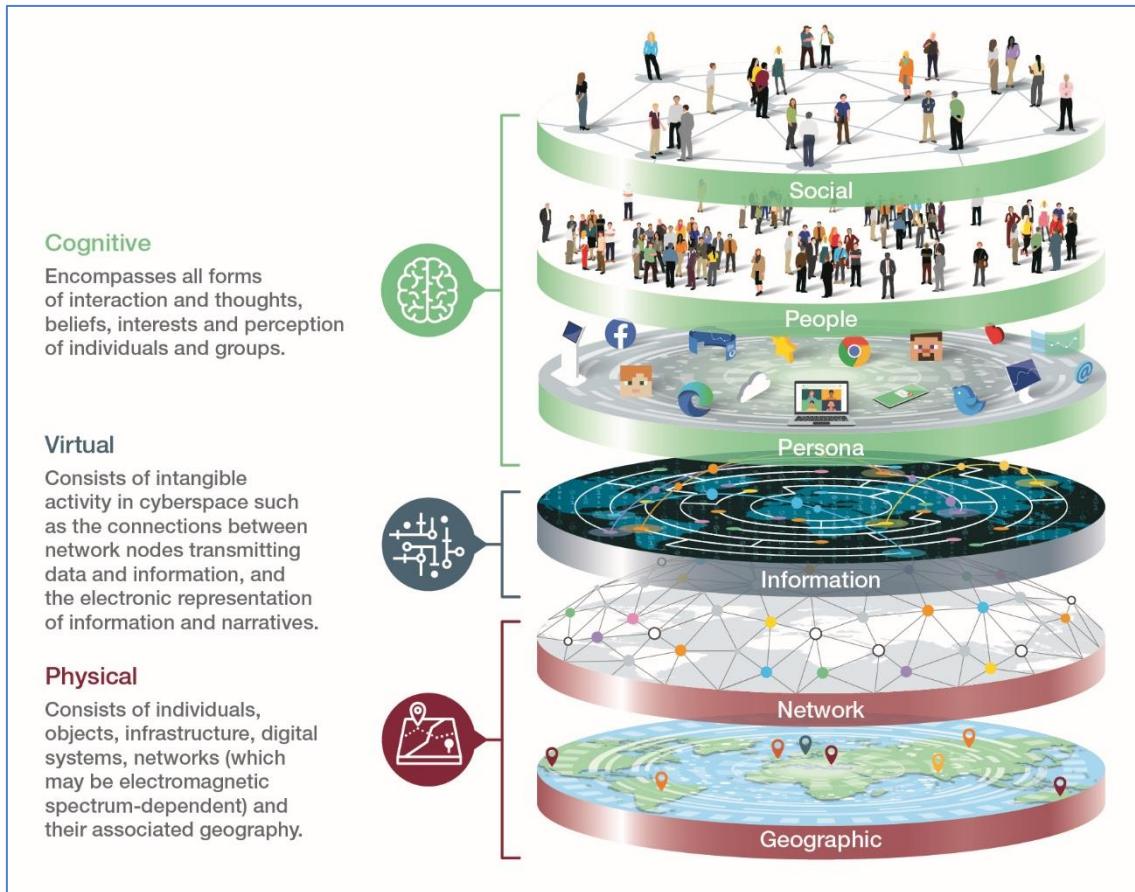


Figure 2-1: Layers of cyberspace and their relationship with the three effect dimensions (from Great Britain. Ministry of Defence, 2022, p7)

Contains public sector information licensed under the Open Government Licence v3.0.

In this the MOD aligns closely with the academic definitions in highlighting the wider scope of cyberspace. According to this approach, cyberspace is the totality of the activities which take place within it, including the societal engagement by humans. The MOD explanation is not only the broadest in terms of inclusion of cognitive aspects, aligning with the cognitive aspects of deterrence in influencing behaviour, but is also specifically and intentionally designed to recognise cyberspace as a military operational environment, and thus particularly relevant to discussion of deterrence.

The MOD is consistent with other Western nations in recognising the physical, virtual and cognitive aspects of cyberspace. Although the names of these elements vary from one country to another they have similar meanings. In the United States, for example, they are the physical, logical and cyber-persona

layers (United States. Joint Chiefs of Staff, 2018, pl-3), while in France they are physical, logical and semantic/social (France. Ministère des Armées, 2019). Given this breadth, and its consistency with both academic and other Western state viewpoints, it is the MOD definition that is therefore taken as the starting point for this discussion of deterrence in cyberspace.

In contrast, other cultures have different views of cyberspace. Russia, for example, does not use the terms 'cyber' or 'cyberspace', instead preferring the term 'information space' where psychological warfare and deception sit alongside computer network operations and the deployment of malware (Tibbs, 2013, p59; Giles and Hagestad, 2013). The formal Russian definition of information space refers to information influencing the individual and community (Russian Federation. Ministry of Defence, 2011); this aligns with the difference in approach to information security in Russia, which focuses on the influence of content on the social-humanitarian environment and the stresses of this influence on stability and state policy (Giles, 2012, p64). This contrasts with the Western view which acknowledges the threat of malicious code rather than malicious content (Giles, 2012, p65). China takes a similar approach to Russia, viewing information space as a place to communicate, bringing together communication networks, databases and information (Giles and Hagestad, 2013), which needs to be protected from destabilising the social order (Raud, 2016, p7). While all states, both Western and others, recognise the contested nature of cyberspace or information space, their different viewpoints on the nature of that contest and the threats it presents over-complicate the consideration of deterrence from more than one angle. As this paper has adopted a Western description (that of the UK MOD) it is thus sensible to retain the Western and UK focus, although the limitations imposed by this are critically reflected upon in Chapter 10, Conclusions and Future Work.

2.3.1 Cyberspace and other operational domains

While cyberspace is not a geographic space in the traditional sense, Betz and Stevens (2011, p37) note that it has many of the attributes of physical space. For them, it possesses reality in the same way as the physical world, with the

boundaries often blurred, although they recognise the interplay of the technology with the wider economic, political and cultural environment (Betz and Stevens, 2011, p37, p85).

In a similar vein, Denning (2015) draws parallels between cyberspace and the traditional (conventional) domains of maritime, land, air and space. She disagrees with others, such as Libicki (2012, p324), that cyber is unique in being man made, arguing that the other domains rely on the man-made vehicles and tools used within them, while cyberspace relies on naturally occurring electromagnetic waves. She also questions the view that cyberspace is more easily changed than the other domains, noting that it is restricted by standards and resources, and citing the internet protocol change from IP4 to IP6 which “has been taking years” (Denning, 2015, p10). In contrast, she observes that man-made roads and bridges can be created to change the land domain. However, it could be argued that this view is oversimplified, in that it misses the point that cyber standards and resources are in a person’s gift to change; and while roads and bridges are man-made, they are temporal constructions created within the land domain rather than permanent features of the domain itself. Further, actions such as re-routing connectivity as in Georgia in 2008 (Tikk, Kaska and Vihul, 2010, p67-71) can be carried out instantly and with no immediately observable indications, whereas building a road or moving troops takes time and can probably be observed by an adversary while in progress.

In contrast to Denning, Libicki (2012) argues that viewing cyberspace as an operational domain is “unhelpful”, particularly when considering the defence of networked systems. He recognises the malleability of cyberspace, but points out that operations are conducted against systems rather than against cyberspace itself; however he does not seem to acknowledge that this surely applies equally to any of the other operational domains. He supports his assertion by noting that domain superiority is meaningless in cyberspace, because it is impossible to control the whole of cyberspace, in contrast to the other domains. Cyberspace cannot be bounded to an area of conflict in the same way as the physical domains, where domain superiority can be achieved over the relevant geographic

area. While he sees the ability to succeed in an offensive cyber operation as a function of target system weakness, the fact that this applies also to offensive operations in other domains somewhat undermines his argument. For example, a warship's ability to sink another warship will depend on the second warship's weakness against the targeted weapon.

As previously noted, the UK MOD description of cyber used in this paper recognises that it spans the physical, virtual and cognitive domains. Since deterrence is about influencing behaviour, it too is clearly associated with the cognitive domain. Cyberspace, however, presents an additional cognitive challenge for the victim of cyber incursion, namely that of determining intent, an issue recognised by many (Geers, 2010, p298; Lindsay, 2015, p55; Mazanec and Thayer, 2015, p15). The same tools and approaches can be used for both hostile activities and for data exfiltration (espionage), which means that the presence of another actor does not immediately make clear whether they intend to cause damage or solely to conduct espionage. Goodman (2010, p123) and Lindsay (2015, p55) suggest that this is an issue unique to the cyber domain. However, there are parallels, particularly with land, where an enemy presence within the camp could be similarly ambiguous. With respect to cyberspace, both Goodman (2010) and Lindsay (2015) highlight that the inability to distinguish between the collection of defensive intelligence (essentially espionage, exfiltrating data but without intent to damage the target system) and offensive reconnaissance or network subversion (exploring the target system to identify weaknesses leading to, or actually causing, harm to the network or the data it holds) is a serious problem. Indeed, as Libicki (2009, p16) observes, the first step is always to compromise a system, and those best able to instigate reconnaissance tend also to be those best able to conduct offensive cyber activities. This aligns with the Russian view of information space, as noted above, which still exploits cyberspace's ability for remote attack and difficulty of attribution.

2.4 What is Deterrence?

Deterrence seeks to prevent an action through fear of the consequences (Schelling, 1966, p71; Great Britain. HM Government, 2015, p23). Before taking

any action, an actor will weigh up its cost, including the likely cost to them of punitive or retaliatory actions by the target (including the likelihood of such retaliatory actions), against the benefit they anticipate from their action. Therefore, as Morgan (2003, p3) and Singer and Friedman (2014, p145) note, deterrence works by affecting the adversary's cost-benefit calculations, so to be successful it must have a cognitive effect on them (Mazanec and Thayer, 2015, p8). In other words, the deterree must be persuaded that to go ahead will result in some form of unacceptable costs to them which will more than offset the potential benefit.

Goodman (2010, p105-6) suggests that deterrence comprises eight elements: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear and cost-benefit calculation. To explain these elements more fully, the deterring state makes a deterrent declaration, including denial and/or penalty measures, in order to protect an interest. This deterrent declaration may be either an explicit verbal statement or implicit messaging through actions. The declaration must be credible to the deterree state, who must also feel reassurance that their compliance will prevent such measures being implemented, while at the same time they must fear the impact of action and weigh up all these factors in their cost-benefit calculations. If the deterrent declaration is not credible, in that the deterrer does not seem to have either the capability or the will to implement it, then the adversary will not be deterred. Credibility is considered in more detail below, together with denial and penalty (punitive) measures. Goodman (2010, p109) goes on to describe reassurance as the "velvet glove" of deterrence in that its absence encourages conflict: while he is speaking specifically of the cyber domain this is surely more widely applicable to other domains, as the adversary will not be deterred if they anticipate they will suffer costs even if they do not attack. Reassurance is thus an essential element of deterrence, alongside denial and penalty measures, and the other elements of Goodman's approach. While Goodman's description is comprehensive, it does not take into account either the deterree's perceptions associated with the deterrent declaration or the wider interplay between the parties.

Deterrence is closely related to coercion and dissuasion. Coercion, also referred to as compellence, seeks to persuade an adversary to adopt a particular course of action, and can be seen as a positive action in that the coerced party takes some action. Even where the required action is that the adversary withdraws or ceases their action, this is considered to be a positive act in the sense that they must *do* something (Gray, 2003, p13). Deterrence, on the other hand, seeks to persuade them *not* to act, and thus is a negative action. Dissuasion is a more generalised approach to an adversary's strategy. Rather than focusing on persuading them not to engage in specific acts of aggression, dissuasion seeks to persuade them not to compete at all. As Bunn (2007, p2) notes, the adversary is dissuaded from acquiring or developing the means of aggression in the first place.

The role of the military in playing an important, though not unique, role in deterring threats to a state's security is confirmed by the view of the House of Commons Defence Committee that deterrence is the military's "primary peacetime role", while recognising that diplomatic and economic levers are also valuable. Indeed, they note that deterrence is most effective when all three of these levers are used in concert (Great Britain. House of Commons Defence Committee, 2014, w1). Deterrence, then, discourages an adversary from acting by influencing their cost-benefit calculus through credible declarations, including the full range of levers.

The key point here is that deterrence is about influence and persuasion: it affects the adversary not through imposing direct costs on them but by making them fear that costs will be imposed and adjusting their cost-benefit calculus accordingly before they take action. Thus, as noted above, it needs to have a cognitive effect. If costs have already been imposed then deterrence has either failed or not been tried, and coercion, rather than deterrence, is taking place (Gray, 2003, p13). While a coercion situation would still offer opportunities for cognitive effect, it is not the primary focus of this research.

2.4.1 Deterrence in history

Deterrence is not a new concept, although it came to prominence during the Cold War in the context of nuclear weapons. Heuser (2010, p315-6) finds examples of

deterrence posturing in Thucydides' contemporary account of the Peloponnesian War in the fifth century BCE, as well as in British maritime strategy in the eighteenth and nineteenth centuries, before it reached prominence in the 1930s with respect to air power. Freedman (2004, p7) goes back even further than Thucydides, (albeit not in a military context) noting God's instruction to Adam to deter him from eating from the Tree of Knowledge by threatening his death. Maxwell (1968, p1) sees deterrence as irrelevant to classical military strategists, although it was recognised, because the earlier nature of warfare "did not stress its importance". This is perhaps because the increased destructive power of weapons has made deterrence of adversaries more attractive. This view is reinforced by Brodie (1959, p271) who, similarly writing in the context of the Cold War, notes that while deterrence is "nothing new" it gained "a special emphasis" and "a distinctive connotation" with the advent of nuclear weapons. This Cold War association has had a lasting effect, as shown by the number of US and British authors who have sought to describe deterrence in cyberspace by comparing it with nuclear deterrence (including Elliott, 2011; Nye, 2011; Mazanec and Thayer, 2015), and as articulated by Singer and Friedman (2014, p145). Within the UK, this is further enforced by the common use of the term 'the deterrent' to mean the UK's nuclear weapons capability (Great Britain. HM Government, 2010, p37). Indeed, in evidence presented to the House of Commons Defence Committee on deterrence in the twenty-first century, all but one of twelve contributors focused principally on nuclear deterrence, with the last focusing on strategic communications. "The deterrence of cyber attack" was the subject of only one short paragraph in the 49-page document, included by the Ministry of Defence in their evidence (Great Britain. House of Commons Defence Committee, 2014).

Yet deterrence, as previously identified, is a cognitive process which relies on persuasion, and is not about a specific weapon, be it nuclear or cyber. In the bipolar nuclear context it may have seemed that deterrence was reduced to a question of who had the largest arsenal in terms of strike capability, but in reality even then it was recognised that nuclear weapons affected the potential patterns of future war, creating fear about passing over the threshold into nuclear war (Schelling, 1966, p111).

2.4.2 Deterrence by punishment versus deterrence by denial

As discussed above, general usage of the term 'deterrence' focuses on the threat of punishment to prevent an action. This concept is applicable also in criminal law and child discipline (Schelling, 1960, p11; Freedman, 2004, p60). In the military context, the potential adversary is threatened with unacceptable costs through retaliation after they have taken a threatened action. An alternative approach, deterrence by denial, seeks to dissuade a potential attacker by persuading them that they will be denied the benefit they seek – “the concept of an impenetrable defense to discourage or frustrate attacks” (Elliott, 2011, p36). Davis (2015, p333) prefers the term “dissuasion by denial”, which he defines as “dissuading an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action.” While Davis' use of the term dissuasion suggests alignment with the generalised approach to strategy referred to above and by Bunn (2007, p2), it seems to address the specific nature of deterrence, since he refers to dissuading an action. His definition does explicitly call up two factors important for deterrence: the capability is *credible*, and the adversary sees it. Thus it recognises that the other party's perception matters.

While references to unacceptable consequences may seem to suggest punishment, some authors include both types of deterrence under this heading. An example is Mazanec and Thayer (2015, p30) who describe “keeping an opponent from doing something that you do not want him to do by making a threat of unacceptable consequences”, and then indeed follow this quotation with a discussion of both deterrence by punishment and deterrence by denial. It is important, then, not to discount deterrence by denial even where it is not explicitly mentioned.

Overall, there is a clear relationship between deterrence and defence, although different authors view the nature of the relationship differently. For example, in the context of nuclear weapons, Morgan (2003, p14) recognises an overlap between deterrence and defence because a vigorous defence against attack could be seen as a form of deterrence by denial. Returning to deterrence more generally, Gray (2003, p1) finds evidence of deterrence being seen as

“yesterday’s concept” but argues that deterrence continues to be an essential component of strategy. Payne (2010, p423) suggests “banishing” the term deterrence because of its Cold War association, but prefers “to work toward a healthier understanding of the term.” He proposes a deterrence framework (p424-5), but although this focuses on describing factors which will affect the deterree’s decision making and strategy, it does not of itself solve the understanding problem: how does one determine what is rational and reasonable for them? Lewis (2022, p17) agrees that deterrence is a concept from the Cold War that needs to be reassessed, as do escalation and miscalculation, as they are “hypothetical constructs” in cyberspace. However, the extensive literature on deterrence, including cyber deterrence, over the last two decades would seem to confirm Gray’s (2003) view of its continuing relevance, as does current UK military doctrine, which refers to “the return to prominence of deterrence in national and international thinking” (Great Britain. Ministry of Defence, 2019, piii).

Regardless of whether penalty measures are through punishment or denial, deterrence may be ‘general’, where an actor maintains a broad deterrence posture with capability and declaratory statements, or ‘immediate’ (also called ‘specific’ or ‘tailored’ deterrence), where signalling is to a specific opponent at a time of crisis (Morgan, 2003, p9, p80-4; Jensen, 2012, p782-3). Deterrence theory generally focuses on immediate deterrence, with links to specific capabilities and potential punishment (Morgan, 2003, p81). This was certainly the case during the Cold War where the United States and the Soviet Union saw in each other a clear and specific nuclear threat. General deterrence may be more applicable to deterrence by denial (Nye, 2011, p34).

Returning to Goodman’s (2010, p105-6) eight elements of deterrence, noted above, this discussion on types of deterrence has addressed the denial and penalty measures to protect the interest, the element of fear and the cost-benefit calculation; the following paragraphs address the remaining elements.

2.4.3 Communication and perception

Both types of deterrence, deterrence by punishment and deterrence by denial, require the communication and credibility of the threat to be effective.

Communication must be clear and, crucially, received and understood by the potential adversary, but this is not trivial (noted by MOD in Great Britain. House of Commons Defence Committee, 2014, w2; Nye, 2017, p53). During the Cold War, both the United States and the Soviet Union were keen to demonstrate to each other that they would not strike first. Jervis (2017, p68) cites John Foster Dulles' belief that Khrushchev, the Soviet President, did not need convincing that the US was not an aggressor. It is, however, clear with hindsight that neither side believed the other (Heuser, 2010, p361) and this was also the case for their intelligence operations (Buchanan, 2016, p28). It seems that this situation is not uncommon (Jervis, 2017, p68; Yorke, 2023, p1083).

One of the related difficulties for deterrence is the perception of the adversary as a rational actor: unfortunately it is difficult to see rationality other than in terms of what appears rational to oneself. Payne (2011, p393) notes that the US approach to deterrence in the Cold War assumed that Soviet leaders were "rational and ultimately reasonable by Western cultural standards". Yet other actors do not always conform to expectations in this way. Indeed, they may act in ways that they consider to be perfectly rational in terms of cultural, political and economic context, or even in line with their particular religion or ideology, but which seem irrational to an outsider (Bar, 2011, p428; Payne, 2011, p399).

This difficulty of understanding what may seem rational to another actor is well understood. Maxwell (1968, p3) noted more than fifty years ago that 'rational' means consistent with the actor's values, "whatever those may be", implying that not everyone may agree with those values. In the same year, but recalling the Cuban missile crisis of 1962, Robert Kennedy observed:

"the importance of placing ourselves in the other country's shoes. During the crisis President Kennedy spent more time trying to determine the effect of a particular course of action on Khrushchev or the Russians ... What guided [him] was an effort not to disgrace Khrushchev, not to humiliate the Soviet Union"

(Kennedy, 1968, p121-122)

Twenty years later Lebow and Stein (1989, p208) recognised that different rational actors will make different calculations. Yet Payne (2011, p398) cites

several examples of mistaken belief in rationality in addition to the US-Soviet example cited above, while Scheber (2011, p454) highlights the importance of cognition and psychology to decision making, and expresses surprise that these have not been considered more actively by those seeking to deter. It is evident that the fact that the problem of rationality is understood does not reduce the difficulty, or guarantee that those seeking to deter will not fall into the same trap, often through “faulty evaluation of available information” (Lebow and Stein, 1989, p217).

One particular source of misperception is the challenger-defender relationship. Theorists, scholars and actors in a deterrence situation not only perceive a distinction between the challenger and defender but also assume that this is clear to both parties. In reality, the situation is not black and white; both sides tend to see themselves as the defender (Lebow and Stein, 1989, p221; Morgan, 2003, p3). This emphasises the need for clear terminology about the parties, leading to use of the more precise terms ‘deterrer’ and ‘deterree’ as noted in the Introduction chapter. If each party sees itself as the defender or victim, then they may seek to deter the other through their own course of action.

The issue is not, however, simply misperception. Communication is a two-way process in which one party attempts to influence the other, but success is not guaranteed: the first party signals and the recipient chooses to receive and respond, or not. As Dorff and Cerami (2000, p111) note, “an actor *chooses* to be deterred” (original emphasis); this point is further stressed by Gray (2003, p13) and Wilner (2017, p310). This aspect of choice may also link to wider rational factors, as noted above, or other broader considerations identified by the recipient. The message may not drive behaviour in the way intended. After the Second World War, Albert Speer, who had been in charge of German industrialisation, noted that while American attacks on industrial targets had been successful in damaging German industrial capability, the British approach of area attacks had not succeeded in “breaking the will of the civilian population” (Quester, 1986, p154), and a similar point was made by an anti-Nazi activist who was determined to repair and find some vestige of home, whatever the

destruction (Grayling, 2006, p86-7). Although not about deterrence, British bombing was intended to send a message to the Germans, but the message did not have the desired effect, and so was clearly not received as intended.

Communication, then, requires clear messaging which is received, understood and acted upon by the recipient in the way the originator intended. To communicate successfully the originator must recognise the context and viewpoint of the recipient in order to influence them. At the same time, the threats of unacceptable costs being communicated must themselves be credible in terms of the deterrer's capability and willingness. With conventional or nuclear weapons this is relatively straightforward at a crude level: one can display one's forces, as at the May Day parades in the Soviet Union, or by massing troops near a border.

2.4.4 Credibility

Credibility is often seen more generally in terms of 'track record': a lack of response to aggressor action will prevent deterrence (Hennessey, 2017). As Bunn (2007, p6) notes, a message to one will be heard by all, in terms of response, thus enhancing or undermining credibility generally. At the same time, uncertainty over response and the potential for escalation may, in Schelling's (1966, p97) view, be beneficial, and offer plausibility when a seemingly simple decision to go to war would appear unreasonable and unlikely.

Thus, credibility is a complex matter, involving both capability and willingness. While words and actions can enhance it, if these are not followed through, or if the capability is deemed inadequate by the other party, deterrence may be reduced. Effective communication can help to create credibility, and so communication and credibility are necessary for both deterrence by punishment and deterrence by denial.

The context of deterrence, in particular whom and what one wishes to deter, also affects the approach. As the MOD stresses, "*Whom* do you wish to deter – from doing *what* – and under which *conditions*?" (Great Britain. Ministry of Defence, 2019, original emphasis). These questions must be answered, although the audience may not be a single specific actor.

2.5 Deterrence in cyberspace

Having considered deterrence and cyber as separate entities, it is appropriate to consider how they can be brought together to develop an understanding of deterrence in cyberspace (or 'cyber deterrence' as it is often termed) and its potential value.

As noted above, deterrence is commonly associated with nuclear weapons, but seeking to describe deterrence in cyberspace through the terms of nuclear deterrence enforces a narrow view which ignores not only the differences between cyber and nuclear weapons and the context of the Cold War, but also the cognitive environment of deterrence. Bayles (2001, p55) considers cyber weapons to be, in themselves, morally neutral, although he recognises that the variety of their effects leaves them without parallel amongst conventional weapons or non-nuclear weapons of mass destruction. These effects include causing serious damage in some circumstances, particularly when combined with physical activities, for example, the 2007 Israeli bombing of a nuclear facility in Syria under Operation Orchard, where cyber methods were used to temporarily disable Syrian air defences (Rid, 2012, p16-17), or the prevention of external communications during the 2008 conflict between Russia and Georgia over South Ossetia (Tikk, Kaska and Vihul, 2010, p67-71). Stuxnet, which was aimed at the particular Siemens control system used on Iranian centrifuges with the intention of surreptitiously damaging them by making them speed up and slow down without the operators seeing any indication, would qualify not only as causing physical damage, if it were indeed successful in damaging the targeted centrifuges (Rid, 2012, p19) but potentially also as an unlawful coercive intervention by one state against another (François, 2020, p241). Therefore, deterrence should be considered more generally than this emphasis on nuclear weapons suggests; this is particularly so with respect to cyberspace, where the threat from cyber weapons is not existential. Further, the potential activities of the deterrer and deterree need not mirror each other: activities in physical space and cyberspace impact upon each other, and the full spectrum of capabilities may be called upon to deter adversaries, integrated across the military domains and other instruments of national power (Great Britain. HM Government, 2021, pp100,106).

These capability levers may be used in different ways, with communication and credibility vital in ensuring effective deterrence.

For the conventional domains, Denning (2015) notes that deterrence is not considered across the entirety of the domain. For example, there is no concept of 'land deterrence' or 'air deterrence'. Instead, she argues, deterrence is focused on particular weapons (e.g. nuclear) or activities (e.g. the actions of Somali pirates). This thesis seeks to establish what is meant by deterrence in cyberspace (RQ1), and Denning's argument might seem to contradict, even negate, that question. However, the question remains valid since it addresses how deterrence can be considered *within* the cyber domain, thus focusing on the activities that take place there (in military terms the effect to be achieved), rather than seeking to deter all activities within the domain. It is questionable whether having a well-defended system is very different from having a well-defended fortress, or whether demonstrating that that one can take control of an adversary system is very different from demonstrating one's ability to inflict physical damage. Indeed, Lewis (2022, p14) asserts that "the risks of an [*sic*] cyberattack on critical infrastructure or command and control are not that different from an attack using conventional weapons." He does, though, note that cyberspace can present "new and more difficult challenge" when used to produce political effects, including through information operations and persistent challenge, and that strategies need to reflect this (Lewis, 2022, p14-15).

It is, however, much harder to display a cyber weapon than a conventional one (as in the Soviet May Day parades), although the creation of US Cyber Command in 2010 might be seen as broadly analogous, at least in signalling that the US were serious about cyberspace. Statements of intent or, better, success in Offensive Cyber Operations (OCO) may also be intended to have a deterrent effect. An example is the statement in the 2016 UK National Cyber Security Strategy about response using "appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing" (Great Britain. HM Government, 2016, p51); this complemented the admission by the then Secretary of State for Defence that the UK had successfully used OCO against Daesh, which was

further reinforced by the Director of GCHQ (Fallon, 2016; Fleming, 2018). More recently, the publication of a document about the National Cyber Force (NCF) notes that:

“The NCF carries out cyber operations on a daily basis to protect against threats to the UK, further the UK’s foreign and national security policy, support military operations, and prevent serious crime ... against both state and non-state threats”

(Great Britain. National Cyber Force, 2023, p11)

Returning to the US creation of Cyber Command, it could even be argued that the US reputation for OCO was enhanced by speculation that they were responsible for Stuxnet (Rid, 2012, p19). Demonstration of credibility, therefore, is less tangible but still feasible in cyberspace.

Credibility, however, requires more than just having capability. Hennessey (2017) notes that the lack of a clear and unambiguous US response to Russian and Chinese activities in cyberspace can be seen as preventing effective deterrence. For her, both the Russian exfiltration and leak of information from the Democratic National Committee (DNC) in 2016 and the Chinese exfiltration of 20 million personnel records from the Office of Personnel Management (OPM) demonstrate a lack of US appetite to deal with the threat. Espionage itself is “generally accepted as a legitimate (if hostile) act by sovereign states” (Lewis, 2022, p15) and “not per se a violation of international law” (Kosseff, 2024, p229). This acceptance of espionage leads Wilner (2017, p315) to suggest that the treatment of the DNC and OPM espionage events highlights a different approach to deterrence according to the level of public release. While Russia was condemned for the DNC leaks, the Chinese OPM exfiltration was recognised by the director of National Intelligence as ‘good espionage’ (Hennessey, 2017; Wilner, 2017). However, a potential adversary presumably does not collect information without reason, even if based on future use. Both examples demonstrate a reticence to respond which is apparent to these and other potential adversaries, and this lack of response fails to send the right message to influence successfully. As

Hennessey (2017, p46) observes, failure to respond “is itself a choice with consequences”.

Thus, credibility is a complex matter, involving both capability and willingness. While words and actions can enhance it, if these are not followed through, or if the capability is deemed inadequate by the other party, deterrence may be reduced. Within cyberspace this can be a particular challenge, as capability is hard to demonstrate without giving away competitive advantage: revealing a cyber weapon allows other parties to defend against it.

While the challenge of misperception is similar in cyberspace to that discussed above, particularly in terms of the rationality of actors, there is an additional aspect to it. The perceived anonymity of cyberspace means that attribution may not be clear (Libicki, 2009, p41) and so it may cause an actor to be confident that they can make their attack appear to emanate from a third party (Jensen, 2012, p783-4).

2.5.1 Deterrence by punishment and deterrence by denial

It is particularly the case in cyberspace that deterrence by denial is more applicable to general deterrence (maintaining a broad deterrence posture rather than focusing on a specific threat). This is because of the difficulty of displaying capability and the importance, noted above, of good defences in denial (Geers, 2010, p301; Jensen, 2012, p782).

Freedman (2004, p39) considers deterrence by denial a more reliable approach than deterrence by punishment, since it removes the option for the target to decide the level of punishment it is willing to bear in terms of its own cost-benefit calculation to achieve its aim. His view does not, however, take account of the increased cost a motivated adversary might be willing to bear to breach a well-secured system if the value to them was high. Libicki (2009, p7) similarly sees deterrence by denial, which he equates with defence, as superior because defence plays a greater role in cyberspace and is always present: this assumes that defence is non-discretionary and that the threat of punishment may be added as an extra component. Following the lead of Libicki (2009, pxiv), who asserted

that organisations “are vulnerable to cyberattack only to the extent they want to be”, Valeriano and Maness (2015, p47) consider that the victim is often culpable in the success of an attack because of their own vulnerability. In other words, if they do not take their own defence seriously then they share the blame for any successful attack against them. While this is a tenuous argument (and not unique to cyber) it does call into question a state’s ability to deter if it is not perceived as serious about defending itself.

Similarly, Iasiello (2013) sees deterrence by denial as a traditional defensive approach, and more likely to succeed in cyberspace than deterrence by punishment, because of the need to maintain effective defences. In the context of deterring cyber with cyber, he also recognises that offensive capability for retaliation still depends on robust and well-funded defence. In contrast, Borghard and Lonergan (2023, p541-542) distinguish between deterrence and defence, noting that defence is about ensuring that the enemy cannot succeed, while deterrence seeks to convince them that offensive action would be too costly to pursue. Gartzke and Lindsay (2015, pp317, 338-9) also believe that deterrence and defence are distinct, but at the same time they see a place for deception in both. Deception can support defence through the use of honeypots or other attempts to confuse, but Gartzke and Lindsay assert that even if defensive deception is not wholly successful it will induce fear and lack of confidence on the part of an attacker. While this may be true for an unsophisticated attacker, it may not have the same level of impact on the powerful and capable actors on which Gartzke and Lindsay focus, although fear of the consequences is related to deterrence by punishment.

It is evident from this discussion that deterrence, then, is relevant to cyberspace, with a place for both deterrence by punishment and deterrence by denial. It is, however, particularly aligned with the latter because of the emphasis on cyber defence, which may in itself deter potential aggressors.

Work by Nye (2017) suggests that deterrence by punishment and deterrence by denial are not the only approaches in cyberspace. He proposes two further categories: deterrence by entanglement and deterrence by norms of behaviour.

Entanglement refers to the interdependencies (such as use of the Internet or common software) which could cause an attack to harm oneself as well as one's adversary (Nye, 2017, p58). Deterrence by norms refers to the development of norms and taboos, analogous to the general international consensus against the use of chemical weapons, which deter through potential damage to reputation (Nye, 2017, p60). Nye acknowledges that it is open to debate whether entanglement and norms are considered as mechanisms of deterrence. However, both concepts appear closer to self-deterrence as they are costs to the attacker, and are not within the gift of the potential victim. Associated with norms of behaviour is public attribution, linking actors' hostile activities with their identities to allow 'naming and shaming', and thus damaging their credibility or reputation: indeed a question on deterrence at a cyber security conference turned almost immediately into a debate about attribution (Five Eyes, 2019), and the UK Government sees attribution as a means of raising "the cost of state-sponsored hostile activity in cyberspace" (Great Britain. HM Government, 2021, p25). By contrast, Ryan (2017) considers these three, entanglement, norms of behaviour and attribution (which he calls deterrence by association), as having "conceptual congruence" in that they share conceptual attributes and are thus related as all forms of deterrence by punishment. None of these proposed additional forms of deterrence challenge the distinct forms of deterrence by punishment and deterrence by denial, in both general and immediate forms.

2.5.2 Describing deterrence in cyberspace

As noted in the Introduction chapter, 'cyber deterrence' is the term most commonly found in the literature, and different authors discuss it in different ways but their meaning is not always clear. The term itself is unhelpful: while Wilner (2017, p309) acknowledges a lack of clear understanding of cyber deterrence and identifies a number of challenges with it, both in theory and in practice, he does not explicitly seek to resolve the issue. He refers to safeguarding data as an example of what he calls digital deterrence, but does not define this latter term, and the example that he gives can be recognised as good cyber security (or

information assurance) rather than deterrence in its wider form, as discussed above (Wilner, 2017, p311).

Burton (2018, p24-5) describes cyber deterrence as necessary to deter offensive acts such as the hacking of the US DNC in 2015-16. However, he does not specifically define the term cyber deterrence in relation to this assertion, other than noting that it “should be a comprehensive strategy that considers the full spectrum of cyber threats” and extends beyond what are traditionally considered national and military security to include “legal, social, normative, and technological approaches” (Burton, 2018, p4, p28).

This lack of clarity is not uncommon. Very few authors make clear precisely how they define cyber deterrence, the most notable exception being Libicki (2009, pp8, 27), who makes a clear statement that cyber deterrence means deterrence in kind and is outside the scope of a physical war. Most seem to adopt, as suggested by Borghard and Loneragan (2023, p535), the same implicit meaning that it means cyber-on-cyber (Iasiello, 2013; Limnéll, 2013; Denning, 2015; Lindsay, 2015; Lonsdale, 2018). In contrast, Nye (2017) criticises theorists for focusing on in-kind activities when a broad range should be considered, but despite this he himself largely addresses only cyber-on-cyber. His stated stance is, however, echoed by Burton (2018) who recognises wider legal, social and normative levers in addition to technological approaches. Fischerkeller (2017) discusses the inclusion of OCO in a conventional deterrence strategy, but while this suggests cyber may be used as a response to non-cyber activities this is somewhat undermined by his use of exclusively cyber-on-cyber examples.

Therefore, while most authors implicitly (and in Libicki’s case explicitly) focus solely on cyber deterrence against cyber aggression, and do not consider wider diplomatic or economic responses, there are wider views even if they are not well articulated in examples. Wider considerations relating to the full range of levers including conventional, cyber and other DIME measures are relevant to military planning and potential response. They are not, however, directly related to the role of perception in deterrence in cyberspace and will not be specifically explored further in this research.

The discussion so far has sought to answer RQ1: “What is meant by deterrence in cyberspace?” This will be reviewed following the research in the Discussion of Findings in Chapter 8. The focus turns now to RQ2 What are the main factors relevant to the interplay between the deterrer and deterree? To answer this, some relevant theories are now considered.

2.6 Offence-Defence Balance

Offence-defence theory offers a useful way to understand deterrence in cyberspace. The theory was matured by Jervis (1978), who argues that nation states adopt either defensive or offensive strategies to maintain their security, with variations in the balance between the relative postures adopted by states which then affect their relationships (Jervis, 1978, pp181, 188; Lynn-Jones, 1995, p670-1). Conflict is more likely when offence has the advantage, while peace and cooperation are more likely to result from a defensive advantage (Lynn-Jones, 1995, p665, 670). The offence-defence balance, which is a continuum (see Figure 2-2), is largely determined by the technology available to states (Lynn-Jones, 1995, p666-7). This is demonstrated by the unique technological features of cyberspace which allow remote and unexpected attack, combined with potential difficulty in attribution, reinforcing the importance of technological differentiation between cyberspace and the other domains of military operation (Libicki, 2009, p5, 41; Nye, 2011, p21). In terms of land warfare, Lynn-Jones (1995) notes that some authors have followed Clausewitz (2007, p160) in arguing that “the defensive is intrinsically stronger than the offensive.” Clausewitz cites generals going back to Quintus Fabius Cunctator² (Clausewitz, 2007, p167) to support his reasoning that the defender has a better understanding of their terrain, and is also able to wait until the attacker is exhausted before engaging: in cyberspace the former still applies (although in terms of network topology and connectivity rather than physical terrain) but not the latter as the adversary will not be exhausted, cold or hungry, although they might be frustrated by the

² Quintus Fabius Cunctator was given the name Cunctator (‘the delayer’) because of his tactic during the Second Punic War (218-202 BCE) of harassing Hannibal’s force while avoiding an engagement with them (Harvey, 1937, p173).

apparent impenetrability of a system. In contrast to Clausewitz, Heuser (2010, p146-7) points out that in the late nineteenth and early twentieth centuries offence was seen as superior to defence.

Scholars and commentators take mixed views of whether defence or offence dominates with regard to cyberspace. Some consider that defence has the advantage (Solomon, 2011, p23; Lonsdale, 2018, p419; Campbell and Donahoo, 2024, p130). More commonly, though, the offensive is held to be dominant (Libicki, 2009, p32,35; Geers, 2011, p11,99-100; Liff, 2012, p415-7; Kello, 2013, p32-3; Singer and Friedman, 2014, p154; Lindsay, 2015, p53; Kania, 2016, p69). This view of offence dominance is generally attributed to two factors: first, the unique qualities of cyberspace, in terms of remote attack and difficulty of attribution as described above; and second, the belief that the onus is on the defender to always succeed in defending against attacks, whereas the attacker only needs to find one route of entry in order to be successful. Furthermore, cyberspace is often perceived as offering a less costly approach to warfare (Kugler, 2011, p317; Singer and Friedman, 2014, p154). Whether this is true is debatable: for low-end, simple activities it may be, but the effort required for a sophisticated offensive activity (Rattray, 2001, p195), such as Stuxnet, is likely to be accessible only to a small number of well-equipped nation states. The 2019 budget for US Cyber Command, for example, was \$610M (Williams, 2019) – well beyond the resources available to smaller states. In comparison, the UK MOD spent £165M on its cyber programme in 2017-8 (Great Britain. Ministry of Defence, 2018, p27). Figure 2-2 shows a graphical representation of the general view described above.

Campbell and Donahoo (2024, p128) consider the US strategy of defending forward through persistent engagement (described by Nakasone, 2019) to be offensive, even though it has a defensive purpose. However, they see the balance as shifting towards the defensive in cyberspace, because of the resources being invested in cyber security and because cyber defence does not cease at the point of penetration of a network but continues once the initial entry is gained (Campbell and Donahoo, 2024, pp130, 132).

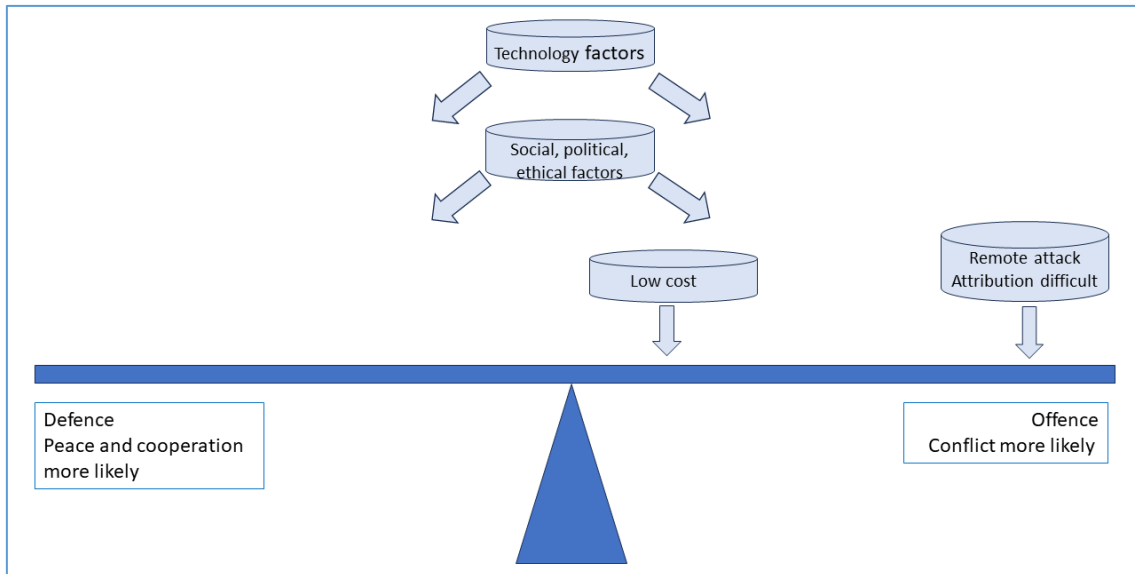


Figure 2-2: Visualising the Offence-Defence balance as a scale with weights which may affect the balance

The offence-defence theory, therefore, seems especially pertinent to cyber deterrence. While it may not address all the relevant factors which must be considered (Lynn-Jones, 1995, p686), it supports a wider review of the technological, social, political and ethical aspects of activities in the cyber domain. It thus offers an approach to understanding how deterrence activities and relationships are perceived by different actors, and the implications these views have for the effectiveness of deterrence.

2.7 Security Dilemma

Misperceptions in the challenger-defender relationship have been noted above. When both sides see themselves as the defender or victim of potential aggression, this can exacerbate the security dilemma, a concept first defined and named by Herz (1950, p157), where one state's desire for security leads it to take measures which others interpret as aggressive:

“the existence of weapons in the hands of one state can provoke at least uncertainty and possibly real fear in others even when those weapons are not intended to be used except for self-protection (following an attack, or

in the event of a threat of an attack)."

(Booth and Wheeler, 2008, p1, original emphasis)

Independently of Herz' work, Butterfield (1951, p21) recognised what he called the "predicament" where one party fears another, but cannot understand that the other might also fear them, or, more simply, the fact that reading the other's thoughts and intent is a mutual problem. Herz (1950, p157) noted that power was desired not as an end in itself but for protection against others in a world where trust was difficult to establish. Jervis (1978, p181) went further, recognising that if one side believes the other knows that their weapons are only for self-preservation, then the first side will conclude that the only possible reason for the other to increase their own weapons is for aggressive purposes. Indeed, even when moves to improve relations are made by one side, the other may not readily respond, as was the case with US President Reagan's suspicion of the motives of Gorbachev, the leader of the Soviet Union, in the latter's overtures to the US to end the Cold War (Booth and Wheeler, 2008, p149-151).

As long ago as 1795, Kant (1983, p108) recognised that the existence of standing armies could result in wars, and a similar reasoning could be seen two thousand years earlier in Thucydides' (1910, p12, para I.23.6) suggested cause of the Peloponnesian War, that "the growth of the power of Athens, and the alarm which this inspired in Lacedaemon, made war inevitable." Here Thucydides has articulated how the security dilemma can set in train a spiral of events leading to conflict. Asking whether arms races cause wars, Sample (2000) concludes that there was a positive association between arms increases and escalation of disputes prior to the nuclear age, but that there was no such association during the nuclear age. The existential threat to life and society posed by nuclear weapons countered the security dilemma, but this is not the case with other weapons, including cyber, which do not present that existential threat.

The security dilemma has since been recognised as a major factor in escalation. This is particularly relevant in the cyber domain, because of the difficulty of distinguishing between intrusions for intelligence purposes (espionage) and

those leading to offensive activity, exacerbated by preparatory action in support of potential future offensive operations (Buchanan, 2016, pp33, 48).

Beckerman (2022) disagrees, suggesting that “the so-called ‘cyber security dilemma’ and related phrases such as the ‘cyber arms race’ are red herrings that distract from other potentially more useful research agendas” (p2). Since one cannot, in her view, have certainty about adversary cyber capabilities, deterrence would focus on research and development towards better monitoring, but would not instigate an arms race (p6). It is hard, however, to agree with this reasoning: as previously noted in this chapter, state spending on cyber capabilities can often be measured, and intelligence gathering would support understanding of capability. While this may not fully address non-state actors operating as proxies under some degree of state approval (whether active encouragement or simply tolerance) it is likely that intelligence gathering would still offer some understanding of capability, or at least of strategic or tactical intent. The Belfer Center’s National Cyber Power Index, however, does not take into account “the close relationship between cybercriminal groups, or proxies, and the state” although it acknowledges it as “a strategic and tactical approach to [the state’s] own cyber power and global policy ambitions” (Voo et al., 2022, p21).

The offence-defence theory is closely aligned to the security dilemma, which is sometimes used as its alternative name: Van Evera (1999, p117) points out that this is wrong because the security dilemma is not the only cause of offence dominance. Alongside offence-defence theory, the pertinence of the security dilemma to cyber activity gives a wider perspective for the relative behaviours of the actors when deterrence is attempted in cyberspace.

2.8 Cognitive Aspects

It is clear from the preceding sections that the perceptions of the parties involved are key to the success of deterrence in cyberspace. How the parties perceive the relative dominance of offence and defence, and misunderstandings through the security dilemma will also affect their interpretation of situations and deterrence messages. As previously noted, this research was not grounded in psychology, although it recognises the relevance of and overlap with psychological theory.

Instead, the research addressed perception in terms of how it might affect deterrence in cyberspace.

The world views of each party need to be understood to avoid the misperceptions described above. This is not straightforward, as it is hard to see from another's viewpoint if that is fundamentally different from one's own, and the predicament of the security dilemma is that one must assume one's own motives may be misinterpreted.

Even with the best intentions, however, motives may be misguided through not considering the other party's viewpoint. Owen and Ludlow (2017, p164-5) criticise the West for the attitudes they held about the end of the Cold War: many saw it as a victory over the Soviet Union, and expected them to fully embrace the Western democratic model, and when the Russian economy subsequently collapsed, they were triumphant about its demise. The end result was "a growing feeling of humiliation and resentment in Russia, and a harkening for a return to the glory days" (Owen and Ludlow, 2017, p165). A similar point was made about the European Union's approach to enlargement following the 2014 Russian incursion into the Crimea:

"While we are clear that NATO is a defensive alliance, for the Russians NATO is seen as a hostile military threat ... threateningly close to the Russian border. EU enlargement, as it has become conflated with NATO enlargement, has also taken on the aspect of a security threat. These views are sincerely and widely held in Russia."

(Great Britain. House of Lords, 2015)

The clear message here is that the other party's views need to be taken into account.

Yorke (2023) goes further, advocating the importance of empathy as "critical" in achieving strategic ends, and arguing that it should be "a constant practice" (p1083). She associates its absence with the security dilemma (p1087), but recognises that empathy "can be a hard and uncomfortable process" and that direct action may be preferred by many to "a cognitive process of exploring

different perspectives” (Yorke, 2023, p1091). When it can be achieved, however, it offers “a willingness to listen and understand ... thus creating opportunities and space for change and transformation” (Yorke, 2023, p1090).

Heuer (1999, p7) asserts that “perception is demonstrably an active rather than a passive process; it constructs rather than records ‘reality.’” Further, early impressions, whether correct or not, tend to persist, as people perceive what they *expect* to perceive and assimilate new information to suit their existing perceptions rather than change them (Heuer, 1999, p8-14). It is difficult to understand another’s viewpoint, particularly where their values and assumptions may be different to one’s own, and “Few of us spontaneously factor other views into our assessments – even points of view that, on second thought, we acknowledge have a nonnegligible likelihood of being right.” (Tetlock, 2005, p123).

This bias towards existing perceptions is widely recognised. Heuer notes that cognitive psychology does not support the ‘mosaic’ theory of intelligence, where small pieces of a jigsaw are put together to reveal the whole picture: rather people form the picture first and then select the pieces to fit (Heuer, 1999, p62). This view is shared by Tetlock (2005, p16), who points out that dissonant views require higher standards of proof than consonant ones, and by Stein (2013, p196), who sees the capacity for rational choice compromised by a general preference for simplicity and an aversion to ambiguity and dissonance. Subconscious mental information processing uses simplified strategies which introduce cognitive bias in terms of evidence evaluation, perception of cause and effect, probability estimation and the effects of hindsight (Heuer, 1999). Although he is writing specifically about intelligence analysis, Heuer’s work has wider applicability, including not only to the parties in deterrence but also to any researcher exploring the subject.

Stein goes further, recalling Kahneman and Tversky’s work on framing, where choice is influenced by the order or language of how options are presented (Stein, 2013, p199). She further notes the effect of group decision making in constructing

a shared view of the problem, and the tendency of those lower in the hierarchy to comply with seniors' views (Stein, 2013, p214).

Dodd (2019, p102) recognises a similar approach in her description of 'choose-ables' as "the imagined deemed possible ways forward" an individual must construct before they can decide upon a course of action. These are subjective and defined by both the context and the individual's understanding of that context. As well as courses of action, choose-ables may be applied to other situations where different options may be possible, such as interpreting scenarios or establishing beliefs. Where individuals are willing to consider the perspectives of others, then they may include compromises in their choose-ables to meet not only their own needs but also those of another party (Dodd, 2019, pp104, 107-8). Dodd further notes the potential value of four coefficients from catastrophe theory:

- Critical 'normal' factors.
- Confusion factors representing uncertainty.
- Belief bias factors.
- Assessment factors used in evaluation. (Dodd, 2019, p111)

The values and relative importance of each of these will vary over time, but they may assist in determining and evaluating options. These factors may help to set predisposition and expectations, although the views of the other authors cited in this section suggest that it is doubtful whether these coefficients will be consciously considered, but that predisposition and expectations will be more important in determining courses of action.

Other authors highlight the importance of emotion. For Stein (2013, p214) rationality and emotion are complementary to each other in forming judgment, while McDermott (2004) advocates the relevance of emotions during and after decisions are made, as well as anticipated emotions and memories of past emotions, and situational and trait factors. In her later work on emotion in cyber conflict she highlights that emotions such as fear and anger are not inevitable responses to situations but that emotions and responses will vary between individuals (McDermott, 2019, p316-7). As well as fear and anger, anxiety and uncertainty about potential consequences can affect decision making. In

McDermott's view, understanding one's own emotions and those of others "may do more to control unwanted escalation than any other single factor" (2019, p323).

Zilincik (2022) shares McDermott's focus on emotions. In exploring the role of technologically inspired awe in the construction of military theories, he recognises the role that nuclear weapons played in the development of deterrence theories, but felt that "For too long, [theorists] ignored the role of cognitive biases and emotions" in favour of seeing humans as "cold cost/benefit maximisers" (2022, pp19, 22). He notes that emotions allow us to "operate in an everchanging environment" (2022, p11). Technology can inspire awe because of its novelty, but that does not necessarily translate to good strategy (2022, p23): this is a particularly salutary lesson in cyberspace.

2.9 Cultural differences

One of the reasons for misunderstanding and different perceptions of actors may be the differences between different cultural groups, whether because of political, ideological, economic, religious or other values. This explains some of the difficulties of attributing one's own "rational" viewpoints on others.

Culture encompasses many different things at different levels, some of which may be easily recognised, such as style of dress and various customs, such as how others are greeted. Less visible but more important are commonly held attitudes and behaviours. Kartchner (2023, p4) suggests that culture not only binds a community, but can also "blind" that community by promoting courses of action which align with its previous approaches and avoid novelty.

This section considers models of expressing culture which can give simple and practical insights, and then considers how the strategic culture of nation states has been addressed.

2.9.1 Models for practical insights

National cultural differences have been recognised for over fifty years, including Hofstede's seminal work with IBM staff in some fifty countries during the 1970s.

Hofstede defines culture as “the collective programming of the mind that distinguishes the members of one group or category of people from others” (Hofstede, 2011, p3) and over time he recognised six dimensions:

- “1. *Power Distance*, related to the different solutions to the basic problem of human inequality;
2. *Uncertainty Avoidance*, related to the level of stress in a society in the face of an unknown future;
3. *Individualism* versus *Collectivism*, related to the integration of individuals into primary groups;
4. *Masculinity* versus *Femininity*, related to the division of emotional roles between women and men;
5. *Long Term* versus *Short Term Orientation*, related to the choice of focus for people's efforts: the future or the present and past.
6. *Indulgence* versus *Restraint*, related to the gratification versus control of basic human desires related to enjoying life.”

(Hofstede, 2011, p8)

Unlike Hofstede's research, which focused on work-related characteristics, the World Values Survey (WVS) addresses general societal issues by sampling individuals in countries across the globe. Analysis of WVS data by Inglehart and Welzel posits two major dimensions of cross-cultural variation: Traditional vs Secular-rational values and Survival vs Self-expression values (WVS, 2022) based on specific indicators addressing views on issues as diverse as religion, respect for authority, political interest, trust in others, happiness and attitudes to homosexuality. Traditional values include religion, the importance of family and defence to authority, while secular-rational values take an opposite view, with greater acceptance of issues challenging tradition such as divorce, abortion and euthanasia. The second dimension contrasts survival values, which give high value to economic and physical security, with self-expression values, where there

is greater tolerance of difference, concern for the environment and participation in political life is expected.

The latest version of the WVS is summarised in the cultural map at Figure 2-3. WVS claim that, while the boundaries and zones assigned are subjective, the positions of countries on the map is objective, determined by the survey data. Studying the detailed data against some of the questions indicates clear differences which align with the dimensions, and which may be used to understand different state's approaches, or for research scenarios to simulate different types of state.

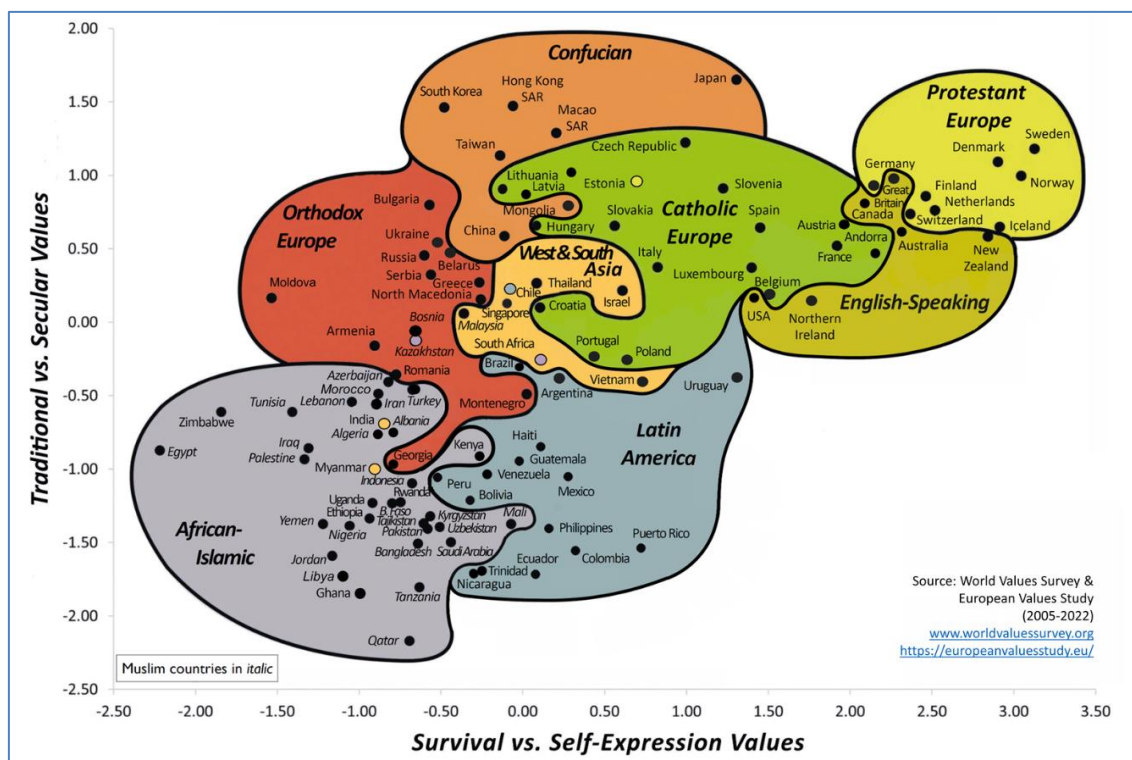


Figure 2-3: The Inglehart-Welzel World Cultural Map - World Values Survey 7 (2022). Source: WVS Wave 7 (2017-2022)

A very practical approach to cultural difference is presented by Meyer (2014), highlighting eight areas where approaches vary along scales, as shown in the culture map at Figure 2-4. Her book is written for business executives to help them communicate and interact more effectively when working with international colleagues. It presents the cultural map in a factual manner, with reference to its origins and derivation limited to her work at the INSEAD business school and a

brief mention of Hofstede's work. This lack of referencing is particularly frustrating in a book which contrasts the applications-based inductive approach of the US and UK with the principles-based deductive approach of others such as France. However, Meyer constantly reiterates that what matters is not absolute position on her mapping but the relative position of one's own culture vis-à-vis those with whom one is working. In the context of deterrence this would obviously translate to those whom one wishes to deter.

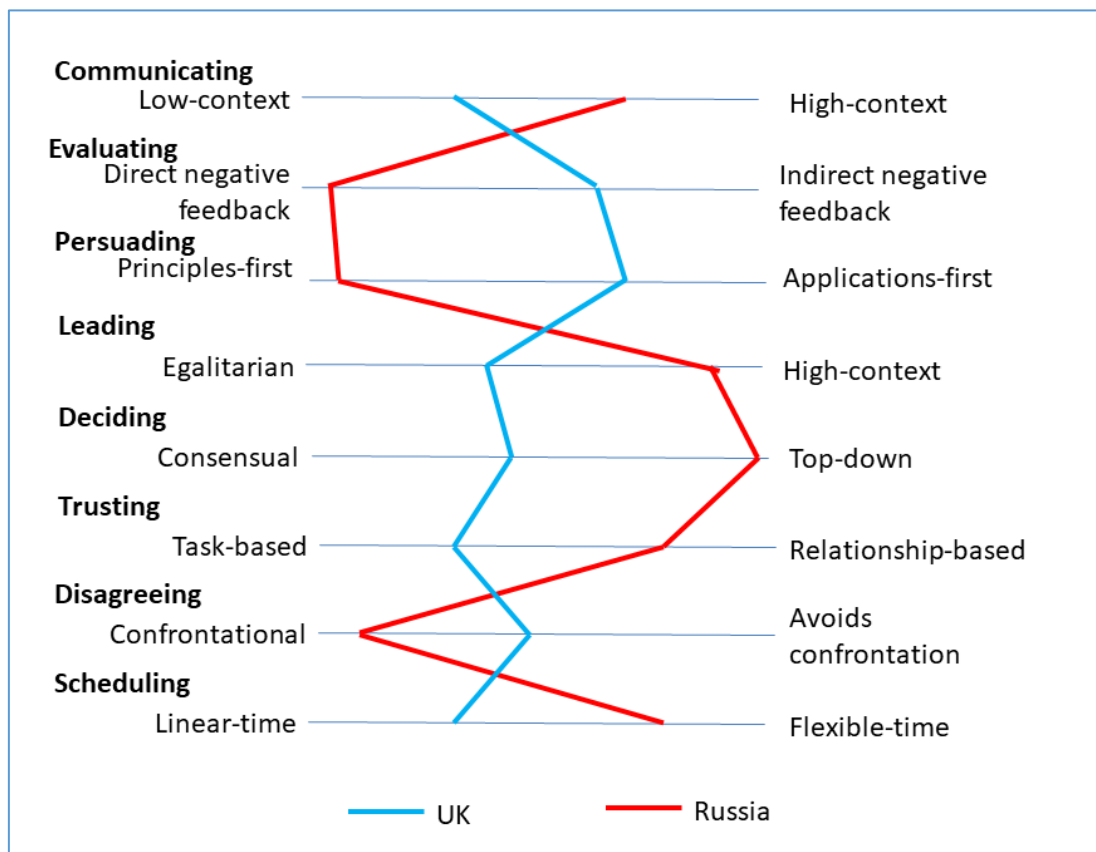


Figure 2-4: Meyer's culture map with examples (adapted from Meyer, 2014)

2.9.2 Strategic culture

At the nation state level, strategic culture was first defined by Snyder during the Cold War:

“Strategic culture can be defined as the sum total of ideas, conditioned emotional responses and patterns of habitual behavior that members of a

national strategic community have acquired through instruction or imitation with each other with regard to nuclear strategy.” (Snyder, 1977, p8)

Snyder applied his use of the term ‘strategic culture’ to political communities, including the military, government officers and political decision makers. Heuser contrasts this with her use of the wider term ‘collective mentality’ to include entire nations as well as elements within them (Heuser, 2023, p26). Strategic culture, however, can be broadened to whole nations as communities.

Kartchner (2023, pp7, 11) notes that, while there is limited consensus on the definition of strategic culture, there is broad agreement about many of the themes within it, particularly:

- It is associated with groups.
- It exists as ideas, values, beliefs and perceptions, which group members hold.
- As a subset of culture, it addresses issues of national security and conflict, including related “values, norms, intentions and objectives”.
- It includes ways of thinking and organising, and patterns of behaviour that resist change.

Gray (2023, p48) adds historical experience to this list, an element also recognised by Heuser (2023, p22) within her “collective mentalities” where historical events may be distorted into national myths to explain the world and to provide a pattern for future behaviour. She notes how a “myth of uniqueness, of difference, or of separateness in some form” is held by several countries including Britain, where this myth underpins the country’s fluctuating relationship with Continental Europe (Heuser, 2023, p22-23). Kari and Pynnöniemi (2023, p79) similarly recognise Russia’s view of itself as a “besieged fortress [with] the mythology of permanent war” as influencing the decisions made by the Russian state.

While this seems to imply a degree of consistency and continuity, Bloomfield (2012, p439) recognises that these are not absolutes, and criticises those who overemphasise consistency in behaviour or suggest that strategic culture has an

unchanging nature. He notes that inconsistency and change can, and does, occur in a nation's strategic culture over time and that strategic culture is an outcome rather than a course of policy behaviour.

Strategic culture can, however, provide "insights into the motivations, intentions and beliefs" of others and thus offset the likelihood of misperception and misunderstanding in diplomacy and strategy (Kartchner, 2023, p7). While it is a major area of study in its own right, it has only been touched on briefly in this Review of Literature.

2.10 Existing Theoretical Models and Frameworks

This section considers a range of models which may contribute to an understanding of deterrence in cyberspace. Models range from formalising specific elements for consideration to proposing a means of calculating the effectiveness of deterrence. The intent of this section is to consider the relevance of the different approaches, their benefits and shortcomings when addressing the role of perception in deterrence. While not all the models are directly concerned with deterrence, they may offer help in considering it, including factors that may be relevant to studying deterrence in cyberspace.

Each model is briefly described, and points of relevance are then drawn out. Where factors are introduced that may be pertinent to deterrence in cyberspace they are considered further in the next chapter, Conceptual Framework.

2.10.1 Snyder (1961): nuclear deterrence

Focusing on deterrence in the context of nuclear and conventional attack against an ally, and recognising the stalemate of the two nuclear superpowers, Snyder (1961) proposed a mathematical approach based on the risk calculus of both the aggressor (A) and the deterrer (D). For the aggressor, the risk calculus is based on four elements: the value of the objective; the anticipated cost of the deterrer's response; the probability of different responses; and the probability of winning the objective for each response. The deterrer's risk calculus has a similar, but complementary, basis: the value of the objective; the anticipated cost of fighting; the probability of successfully retaining the objective; and the probability of future

attacks on other objectives which would follow different responses (Snyder, 1961, p12-13). From these, Snyder develops a comprehensive and mathematical means of calculating the expected value of a decision, based on the probability of the aggressor attacking as viewed by each of the two parties and tabulated for comparison (Snyder, 1961, p17).

Snyder assumes rationality and treats credibility as the likelihood of retaliation; while this is a reasonable correlation of credibility it is based solely on one party's estimate of the likelihood of the other's action. Snyder's basic calculation for the aggressor is:

$$\text{"(likelihood of retaliation * cost of war) plus (likelihood of no retaliation * gain)"} \quad (\text{Snyder, 1961, p18})$$

Despite his mathematical approach and his stated context of a threat to an ally, Snyder is (as one would expect from the time he was writing) rooted firmly in the bipolar nuclear world, considering a combination of relatively straightforward elements (cost and gain) and a subjective assessment of credibility in terms of likelihood. That said, Snyder's work set a standard in terms of clarity and simplicity of approach which paved the way for more recent models addressing deterrence in cyberspace.

2.10.2 Straub (2019): combining likelihood, impact and deterrent value

Mutually Assured Destruction (MAD) was a major driver in nuclear deterrence: each of the two superpowers in the bipolar stalemate knew that if they struck first the other would retaliate in kind, so any nuclear attack would impose unbearable losses on both sides. Straub (2019) attempts to translate MAD to a multipolar information and cyber context, although his approach is not specific to cyber. He proposes a model (Figure 2-5) in which likelihood, impact and deterrent value are combined as a single value and compared. While Straub claims that this allows the consideration of factors such as perception, fear and longer term impact, he does not make clear how these would be included, or indeed how to calculate the single value for each actor. However, he does point out that this is only a

framework to help decision making, and that there is no guarantee that the calculations are correct. Straub's model offers a simple approach for comparing multiple actors by adding additional calculated values (in additional boxes feeding into the decision), although its value is severely constrained by the lack of clarity about the inclusion of wider factors and the calculation of the value.

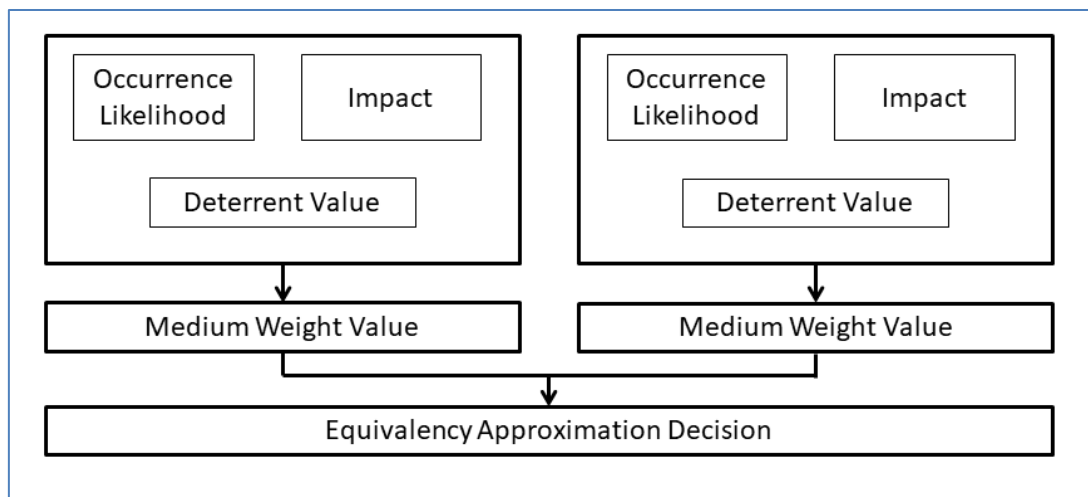


Figure 2-5: Straub's cross-domain (medium) deterrence (Straub, 2019, p5)

2.10.3 Sharp (2017): credibility and persuasiveness

In contrast to these models, Sharp (2017) seeks to show the coercive value of cyber operations through the imposition of costs and destabilisation of the adversary's leadership. He uses a single example, that of the 2014 North Korean operation against Sony (in response to the latter's satirical cinema film 'The Interview') to illustrate his point, noting that this "(1) represents a clear coercion attempt and (2) features sufficient evidence about the target's decision-making. While a state-versus-state case might be preferable, none exist that definitively meet these two requirements" (Sharp, 2017, p901).

Sharp offers six factors to measure the credibility and persuasiveness of a cyber threat:

- reputation for resolve (having the will to act)
- political support
- reversibility

- causing private losses
- demonstrating cyber power advantage
- reputation for proficiency.

He notes that the Sony case met four of these, with the private losses condition not applying because the coercive cyber operation was made public, and the reversibility condition failing because (in his view) going public caused irreversible harm to Sony's reputation (Sharp, 2017, p917-8). The factors do break down credibility and persuasiveness, potentially making them more measurable, but Sharp does not explore how they could be considered other than in 'yes/no' terms, and as only the one example is used wider applicability is not addressed.

Although Sharp focuses on compellence rather than deterrence, in general the challenger-defender relationship is not necessarily clear, with both sides tending to see themselves as the defender or victim (as noted by Lebow and Stein, 1989, p221; Morgan, 2003, p3). Sharp naturally takes the US viewpoint, where North Korea are the aggressor and Sony the defender, but there is also an opposite view, in which Sony's actions were a challenge to the North Korean regime. Sharp does not consider this, and while it could be stretching the point too far to consider Sony wishing to change the status quo by preparing to launch their film (and therefore if Sony were a state whether this could be considered analogous to the Soviet activities leading to the Cuban Missile Crisis), if that were the case and North Korea wished to maintain the status quo, then the cyber operation could be seen as deterrence. Taking this alternative stance, and applying the six factors as if Sony were a nation state, the six factors could be useful as measures relevant to credibility when considering deterrence in cyberspace, although causing private losses may deter the specific aggressor but will not send a wider message to others, and it is clear from Sharp's discussion that he sees these as relevant factors, not absolutes.

2.10.4 Halas (2019): Boolean logic

A very different approach is offered by Halas (2019), using Boolean logic to explore whether lack of aggression demonstrates the adversary's lack of interest

and opportunity rather than effective deterrence in terms of capability, credibility and communication. He expresses concern that scholars have focused on immediate deterrence rather than on the ongoing general deterrence between hostile states (Halas, 2019, p434). The outcomes to a two-term Boolean formula are presented in a truth table, shown in Table 2-1, where only the first row (shaded) indicates that general deterrence is working. The second row shows a successful attack, where the aggressor has the opportunity and motivation but the deterrer fails in at least one of capability, credibility and communication. In the third and fourth rows, where the status quo is preserved, the aggressor lacks opportunity or motivation.

Table 2-1: The logic of general deterrence seen from the perspective of Boolean logic (from Halas, 2019, p434)

<i>A</i>	<i>F = (B ∧ C ∧ D)</i>	<i>E</i>
1	1	1
1	0	0
0	1	1
0	0	1

Note: All the variables, including the challenger's willingness to consider using force to advance his/her own interests if the opportunity arises (*A*), preservation of the status quo (*E*), and the deterrer's sufficient capabilities (*B*), solid credibility (*C*), and strong communication (*D*), can be either true/present (1) or false/absent (0).

Unfortunately, Halas does not give the Boolean formula to determine the preservation of the status quo, although this can be derived from his truth table. The formula is:

$$E = \bar{A} \text{ OR } (A \wedge F)$$

The use of Boolean logic is an interesting approach, and demonstrates the difficulty of understanding whether deterrence is effective: how should the values of *A* and *F* be determined? Halas misses a key point, however, that what is at issue is not so much the would-be deterrer's capability, credibility and

communication, but the adversary's perception of them. Further, since it is hard to determine cognitive effect, how does one know that the adversary is not interested?

2.10.5 Lindsay (2015): cost and uncertainty

While Halas focused on possible lack of aggressor interest, Lindsay (2015) notes that cyber incidents have been mainly against low-value targets and seeks to explain this. He suggests that cyber operations are not appropriate for direct coercive signalling, but that they can support conventional military signalling through cross-domain approaches as well as having their own value in subversion and espionage (Lindsay, 2015, p54-56).

Lindsay proposes a formal model to illustrate the effect of assumptions of cost and uncertainty on deterrence. He simplifies the problem by leaving out consideration of earlier sunk costs (such as defensive measures) and repeated interactions, and focuses on an attacker S_1 incurring a cost c_1 while attempting to realise a benefit v , while a defender S_2 promises retaliation r at cost c_2 . The attack has two potential outcomes:

- S_2 does nothing: S_1 wins v at cost c_1 ; S_2 gets nothing.
- S_2 retaliates: S_1 pays $(c_1 + r)$; S_2 retains v but pays c_2 .

Lindsay captures his calculation in a three-dimensional graph plotting target value, punishment and effectiveness of deterrence, offering not only the simplest case with perfect information available but also introducing ambiguity through probability factors for retaliation and different combinations of attacker and defender costs. While concluding that "Deterrence works, just not everywhere" (Lindsay, 2015, p62), he notes the model's simplicity of approach and urges caution in interpreting it.

Overall Lindsay's model offers a useful approach to analysing the cost/benefit ratio for both sides in a consistent manner, addressing probability of retaliation and different cost combinations. It is, however, necessarily simple in that it focuses on a single event, whereas in reality hostilities are likely to build over many exchanges. It also fails to take account of the wider costs of defending

systems, seeing these as sunk: while this may at one level be reasonable it does not recognise the effort expended to deter a determined actor. Further, it focuses exclusively on the economic calculation of a rational actor, and does not allow for other factors such as political, geopolitical or technical contexts which may affect cost/benefit calculations. Including these would make Lindsay's simple mathematical approach unwieldy.

2.10.6 Healey and Jenkins (2019): “rough-and-ready”

A different simple approach to exploring whether cyber deterrence is working is proposed by Healey and Jenkins (2019), specifically looking at the US policy of ‘persistent presence’, which the then Commander of US Cyber Command described as “To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well” (Nakasone, 2019, p12). This includes “gaining access to systems that adversaries value, to hold them at risk with offensive cyber operations” (Healey and Jenkins, 2019, p124) - although it could be argued that effectively placing capability within adversary territory (their systems) is an aggressive rather than a deterrent act. Healey and Jenkins put forward what they describe as simple “rough-and-ready” metrics to determine the effectiveness of the policy, counting the number of significant cyber incidents, possibly for each major adversary, and exploring the metrics for different types of incidents. While this is focused on whether the specific US policy is working, and the authors recognise the potential shortcomings of attacks being hidden and the difficulty of proving causality, it is an interesting and straightforward approach to their stated question. It does not, however, offer a means of determining the effectiveness of deterrence as it looks retrospectively at incidents.

2.10.7 Belfer Center (Voo et al., 2022): National Cyber Power Index

A more comprehensive view of a state's cyber power is the Belfer Center for Science and International Affairs' National Cyber Power Index (Voo et al., 2022). This rates thirty states against eight objectives, scoring them for capability and intent against each. The objectives are (short titles in brackets):

- Surveilling and monitoring domestic groups (Surveillance)
- Strengthening and enhancing national cyber defences (Defence)
- Controlling and manipulating the information environment (Information control)
- Foreign intelligence collection for national security (Intelligence)
- Growing national cyber and commercial technology competence (Commerce)
- Destroying or disabling an adversary's infrastructure and capabilities (Offence)
- Defining international cyber norms and technical standards (Norms)
- Amassing wealth and/or extracting cryptocurrency (Financial).

This leads to an overall league table for cyber power, supplemented by radar diagrams for each state and charts for each of capability and intent for each objective (see examples at Figure 2-6). Their assessment is wide-ranging and reasonably transparent: they give the algorithm used to combine the scores and 34 out of 52 pages of their report (including 36 pages of annexes but excluding covers and preamble) are charts. What is not so clear, however, are the details of how the scores for each objective were reached, and some cases have been highlighted where assumptions have had to be made in the absence of any evidence (in the case of North Korea for every objective).

Over time details will change, but this is the second iteration of the Index (the first was in 2020) and as well as updating scores an additional objective, Amassing and Protecting Wealth, has been included. Overall, the Index offers a comprehensive and seemingly well-researched view.

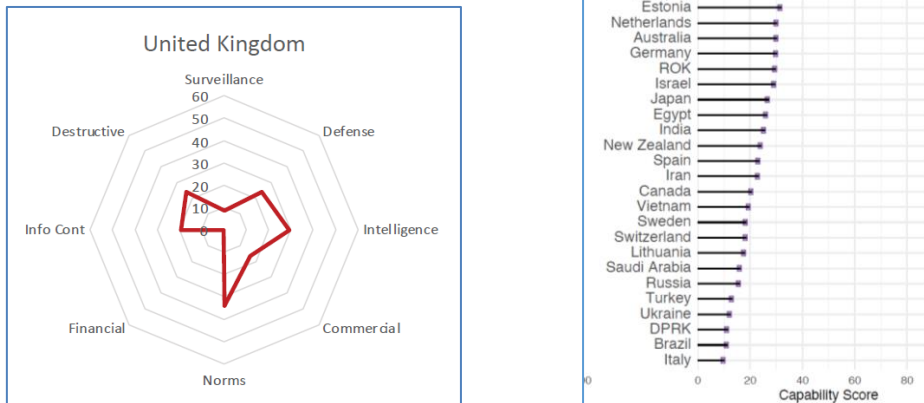


Figure 2-6: Charts for the National Cyber Power Index (taken from Voo et al. 2022).
(a) Radar diagram showing combined capability and intent scores for the United Kingdom. (b) Capability scores for the Norms objective.

2.10.8 Edwards et al. (2017): attribution - the “Blame Game”

Attribution plays an important although complex role in deterrence. Edwards et al. (2017) note that states may overstate their attribution capability as a deterrent. They present a Bayesian game-theoretic model, the “Blame Game”, between an attacker (A), who may be vulnerable (or not) to blame, and a victim (B), who may be knowledgeable (or not) about the attacker’s vulnerability to blame. They include variables to describe the gain G to the attacker, the loss L to the victim, the loss I suffered by a vulnerable attacker when blamed by the victim, and the gain g the victim receives from blaming a vulnerable attacker. The game begins with A choosing whether to attack B: If A attacks, then A receives gain G and B suffers loss L . B then chooses whether to blame A for the attack: if B chooses not to, then B pays for their inaction, either N if B is knowledgeable or n if B is not knowledgeable, where $0 < n < N$; if B does blame A but A is not vulnerable, then B pays additional cost (representing reputational cost or direct retaliation), either C if B is not knowledgeable or c if B is knowledgeable, where $0 < c < C$. The possible outcomes are presented in a graphic representation, shown at Figure 2-7.

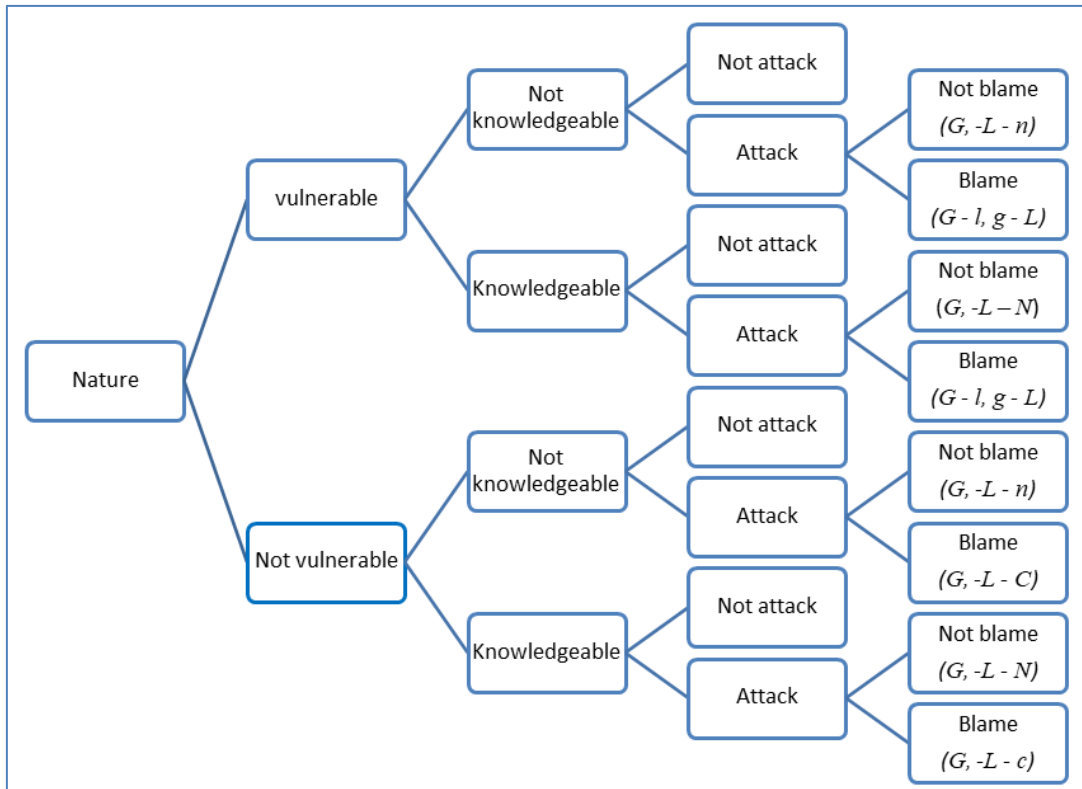


Figure 2-7: Graphic representation of the “Blame Game” (simplified from Edwards et al., 2017, p2827)

The model is straightforward with few variables (even though assigning values to them is not trivial) but it covers a range of situations relating to the attacker and the victim’s knowledge about the attacker’s vulnerability to blame. Thus, it does try to address wider elements relating to rationality, rather than focusing exclusively on the economic cost-benefit calculation. Edwards et al. recognise its value in identifying whether a prospective attacker should attack and whether a victim should blame or tolerate an attack. However, the model focuses on a single event, whereas hostilities are likely to build over many exchanges. It further assumes that any retaliation will be in kind, i.e. in cyberspace, and so does not allow for escalation or the context of a wider conflict. It also fails to take account of the sunk costs relating to development of exploits (for the attacker) and to defence (for the victim), although these would form part of their decision making process. While not focusing specifically on deterrence, it provides a useful insight into the wider factors and reasons for declaring attribution, using a simple mathematical basis and decision tree output, and recognising equilibrium states.

2.10.9 Cui et al. (2017): attacker in a “three player” game

Another approach to examining deterrence of an attacker by a defender (in this case a system administrator or security provider) is offered by Cui et al. (2017) in the context of a network attack by an unspecified non-state actor. Despite their calling this a “three-player behavioural game” (the third player being the system user), their focus is the action of the attacker, who is the only “real” player as the others are simulated. While this imposes control it also prevents the full interaction between the parties to be explored in terms of understanding how the parties expect others to perceive their actions and whether these perceptions are correct. They do note, however, that adversaries “might differ strongly in their risk-taking propensity because of personality, emotion, or other considerations” assessing best- and worst-case outcomes differently, and so the deterrer cannot influence all factors (Cui et al., 2017, pp351, 354).

2.10.10 Valeriano and Maness (2015): taxonomy for incidents and disputes

International cyber conflict is explored by Valeriano and Maness (2015), who recognise that overstating the threat may result in responses which fuel conflict, a stance in line with the security dilemma, and their stated intent is to prevent discourse being dominated by fear. They present a taxonomy for the type and severity of cyber incidents, addressing the interaction and target type of an incident or dispute, together with the initiator’s objectives (e.g. disruption, theft or change in behaviour), and then apply this to publicly known cyber espionage operations and other international cyber conflict.

As a taxonomy for incidents, its intent is to describe an event that has happened and it is therefore not directly relevant to deterrence. It may be useful in considering the type of impact an aggressor, or even oneself, wishes to have.

2.10.11 Agrafiotis et al. (2018): taxonomy of cyber harms

At a non-state level Agrafiotis et al. (2018) propose a taxonomy of cyber harms to allow the creation of effective metrics for the impact of cyber attacks. Their approach is influenced by criminology and focuses on asset and impact rather

than specific threats. Each of the five broad themes of harm (physical/digital, economic, psychological, reputational and social/societal) is decomposed into a number of sub-types as shown in Figure 2-8. The focus is on crime, but the taxonomy is threat-agnostic and would have value in wider contexts such as hostility between states.

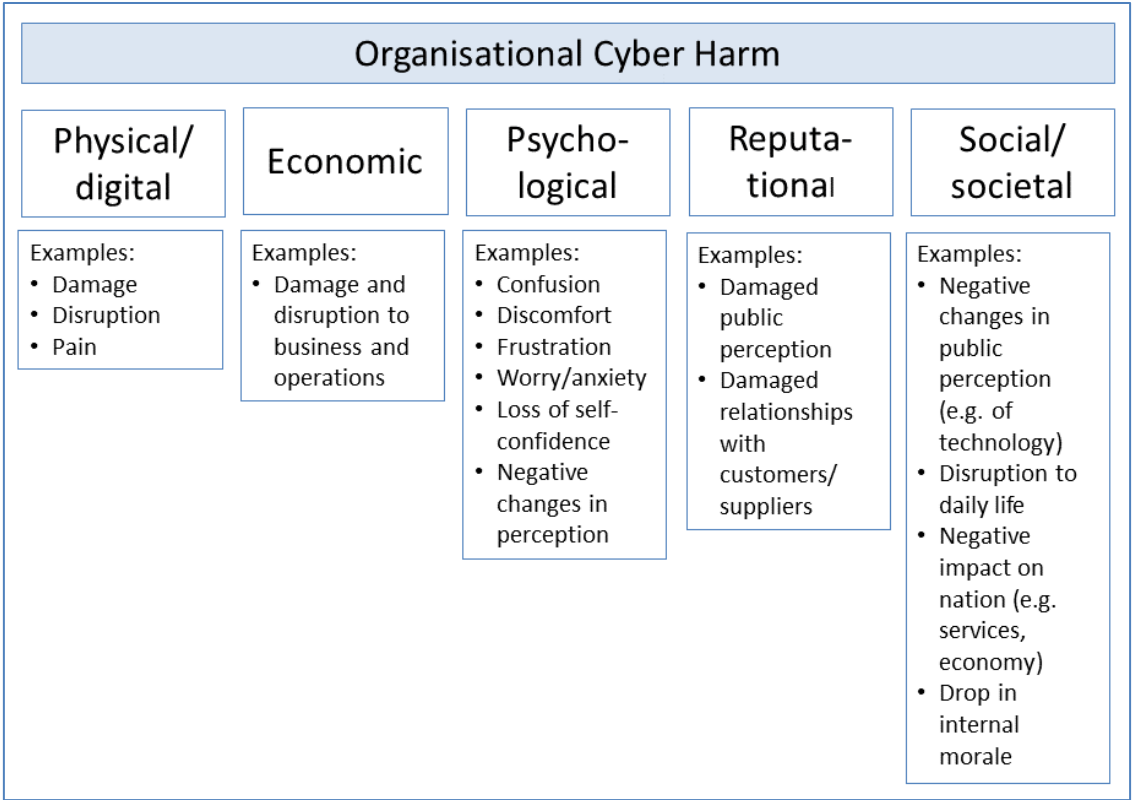


Figure 2-8: Examples of taxonomy of organisational cyber harms (Agrafiotis et al., 2018)

As with the taxonomy proposed by Valeriano and Maness (2015), Agrafiotis et al. (2018) attempt to describe what has happened after the event and so their model is not directly concerned with deterrence. That said, some elements might be useful to consider as relevant to deterrence, particularly from the physical/digital and economic themes. It may, however, be useful both in developing an understanding of not only the results of failed deterrence but also the potential target and objectives which an aggressor may consider.

2.10.12 McDermott (2019): emotion and response

McDermott (2019) offers a very different approach to a taxonomy by addressing emotion, which she sees as a neglected aspect of cyber conflict. Fear, anger and surprise are pertinent emotions in cyber conflict, but emotions do not operate in isolation and the consequences can influence immediate and future choices. Her taxonomy (which she notes is untested) is shown at Table 2-2 and identifies responses to actions and emotions. She points out that individuals do not recognise their own - and certainly not others' - dispositional responses, but that decision makers can be taught to recognise them and to acknowledge the consequences for their own decisions and their impact on others' responses, in order to control unwanted escalation. McDermott is clear that individuals will bring their "unique dispositional composition of background mood traits, emotional awareness, capacity for self-regulation, resilience ... and reactivity" to a situation as well as wider environmental factors (McDermott, 2019, p322). Her views clearly reinforce the importance of cognitive effects on deterrence.

Table 2-2: McDermott's taxonomy of conditions, emotions and responses (from McDermott, 2019, p321)

Nature of threat	Emotion activated	Response
Threat to civilian infrastructure	Fear	Withdrawal; negotiation
Election meddling	Anger	Retaliation
Attack on military forces	Surprise	Escalation if judged intentional
Infiltration/infection of critical domestic cyber systems	Disgust	Elimination/destruction

2.10.13 Powell (2002): bargaining theory

In addition to these models, bargaining theory, cited by Lindsay and Gartzke (2022) amongst others, is clearly relevant to deterrence because of the interaction between the actors. Powell (2002) identifies three protocols for bargaining:

1. Player 1 makes a single ‘take it or leave it’ offer. If player 2 accepts, both receive the agreed payoff, but if they reject then the status quo remains.
2. Player 1 makes offers which player 2 can accept or reject (as for protocol 1), but player 1 can make as many offers as they wish.
3. Offers and counter-offers are made alternately back and forth, with no limit.

In terms of deterrence, where player 1 is the deterrer and player 2 is the deterree (the potential aggressor in player 1’s view), protocol 1 is the simplest to model, but it is unable to take account of the ongoing relationship (whether improving or deteriorating) of the actors or the ongoing context in which they operate. Protocol 2 suggests a degree of desperation on player 1’s part, where player 2 can wait for a more favourable offer before withdrawing from the situation, although this also does not take account of their ongoing relationship and context. Protocol 3, which is the classic situation of haggling in a market where the two sides start far apart but close in until an acceptable agreement is reached or one walks away, is the most realistic in reflecting the actors’ relationship and context. In conventional or nuclear deterrence the ‘offers’ would be the progressive escalation of weaponry which would seek to change the advantage gap (by closing the gap or seeking to outdo the other) while also leading to potential escalation. While that may also apply in cyberspace, the difficulty of declaring capability might prevent protocol 3 being used in negotiation, and the speed and nature of activity in cyberspace (including the potential actions of others) may result in a moving context of concurrent activity rather than the back and forth “ping-pong” of protocol 3.

2.10.14 Summary

The models and taxonomies discussed above are all useful in highlighting specific areas which could be considered when researching deterrence in cyberspace, and some of the concepts noted will be explored in the next chapter in the development of a Conceptual Framework for the research. There is, however, one unifying feature in all of them: none addresses culture. Further,

only McDermott (2019) even acknowledges the viewpoint of the other party, although she does not develop it. If the work on cultural difference and cognitive aspects cited earlier in this chapter is to help those engaged in deterrence to understand the viewpoint of the other party, then any model or taxonomy needs to take this into account.

2.11 Chapter Summary

Deterrence is not an academic exercise but an operational necessity to maintain stability. In order to examine its value, its effectiveness needs to be determined. However, this requires a clear understanding of what is to be deterred and how that deterrence can be achieved. This chapter has explored the literature relevant to deterrence in cyberspace to seek clarity about its meaning and the specific issues which apply within cyberspace.

The basic traditional concepts of deterrence by punishment and deterrence by denial still hold in cyberspace (with deterrence by denial having a clear affinity with cyber defences). Communication and credibility remain vital to successful deterrence, although credibility in particular needs new approaches in this context. Intent presents a further challenge, as the difference between espionage and offensive activity on networks may not be immediately apparent.

While the particular features that differentiate cyberspace from the other operational domains should not be ignored, it is important not to overstate them. Similarly, deterrence in cyberspace should not be seen as unique: it sits alongside not only deterrence activity in the other domains but also diplomatic and economic measures.

Several models have been described which may contribute to an understanding of deterrence in cyberspace, although all of these have limitations, particularly in addressing the importance of perception, and in not attempting to address potential cultural difference.

This chapter has answered RQ1: “What is meant by deterrence in cyberspace?” by modifying the basic definition of deterrence offered by Schelling (1966, p71)

and HM Government (Great Britain. HM Government, 2015, p23) to give the definition:

Deterrence in cyberspace seeks to prevent an action through fear of the consequences, using cyber activities as part of the full range of levers including conventional and DIME measures.

It has also begun to explore RQ2: “What are the main factors relevant to the interplay between the deterrer and deterree?” The development of the conceptual framework in the next chapter will build on this ahead of further consideration in the research.

3 Conceptual Framework

3.1 Chapter overview

This chapter addresses the conceptual framework developed to answer:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

It begins by setting out an initial conceptual framework developed following the literature review. An exploration of the component parts, particularly Goodman's (2010) elements of deterrence, and considering how these elements are under the determination of one or other party, leads to a progression in the conceptual framework. Factors highlighted by other authors in their models are considered, and all the identified factors are reviewed for their inclusion in the research, according to whether the deterrer can influence the deterree's view of them. This leads to a third iteration of the conceptual framework which is used as the outline for the research.

One further issue that needs to be resolved is how to approach a subject that involves two parties, the deterrer and the deterree. The difficulty of research involving two parties is considered and a solution identified.

3.2 Introduction

Leshem and Trafford (2007, p96) highlight the importance of the conceptual framework in "providing a theoretical overview of intended research". It thus helps to give direction to the research through the whole process, from problem definition, establishing theoretical coherence and organising the research process, to framing the conclusions (Berman, 2013, p2). It identifies the key factors and their interrelationships, typically explaining these in graphic form (Robson and McCartan, 2016, p68). In line with these authors' views, the initial conceptual framework at Figure 3-1 was developed following the literature review as a vehicle for visualising and managing the research process.

3.3 Conceptual Framework stage 1: initial

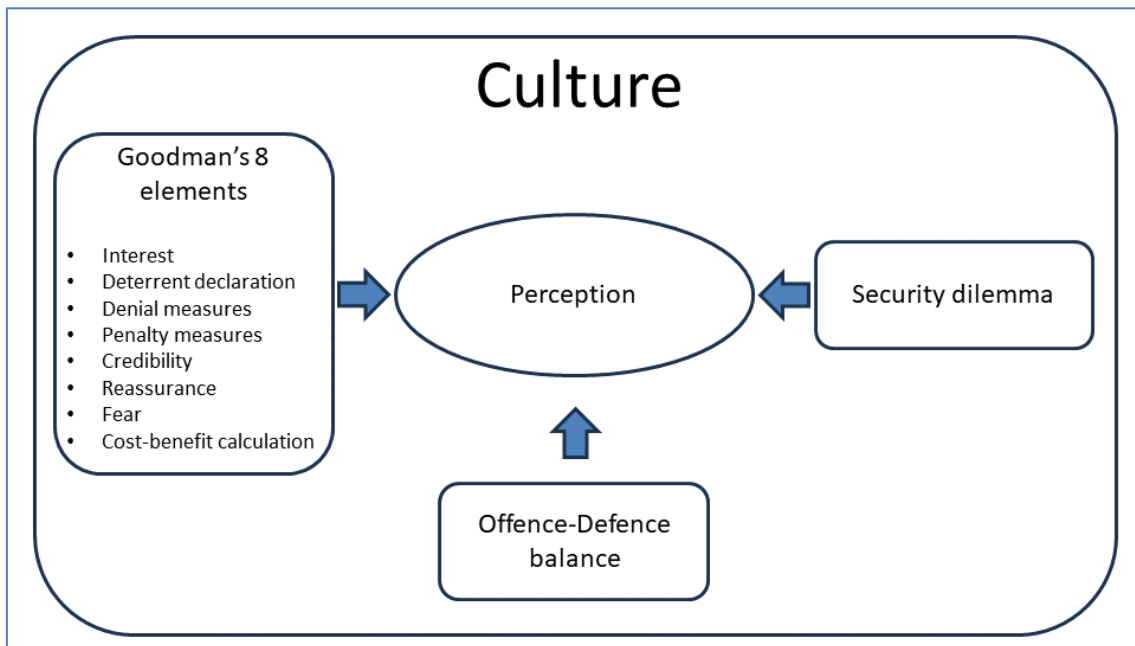


Figure 3-1: Initial conceptual framework

Figure 3-1 shows the key areas highlighted in the literature review as relevant to deterrence in cyberspace, and indeed deterrence more generally. Together these will influence the perception of both parties.

The security dilemma may cause one or both parties to feel under threat from the other if they see evidence of the other increasing their military capability.

The offence-defence balance may cause the parties to adopt either an offensive or defensive strategy towards their security. They may vary in how they determine and set their strategy and could each be anywhere along the offence-defence continuum. As noted in the literature review, conflict is more likely when offence is deemed to have the advantage. For cyber activities attribution is of particular relevance as the perceived difficulty of definitive attribution of an attacker's remote access is seen as favouring an offensive strategy (Libicki, 2009, p5, 41; Nye, 2011, p21).

Goodman's (2010, p105-6) eight elements of deterrence were identified in the literature review as a comprehensive description of deterrence, and so is used here as the start point for considering deterrence. Although it does not address

the deterree's perceptions or the wider context between the parties, it can be described in terms of the different interpretation of the parties. This is discussed in greater detail below.

Culture underpins all of these, hence it is shown as filling the whole. Cultural factors will impact both parties and their interpretation of the threat from the other (the security dilemma), whether their security strategy leans to an offensive or defensive posture, and their interpretation of the elements of deterrence. Cultural factors will thus affect their perception of all aspects of the situation. In any interaction between two states they will have their own version of reality.

The Research Methodology in the next chapter addresses the ontological stance taken in this research, namely critical realism (Bhaskar, 2008) which views reality as stratified into empirical, actual and real. Each party will experience their own view of reality (the empirical layer), which can be considered as essentially their own version of Figure 3-1. Each will take actions based upon their view: these take place within the actual layer but will be experienced by the other party at the empirical level, again in the context of their cultural disposition, and further influence their viewpoint. Confirmation bias will also play a part in this, with each party interpreting the other's actions in the light of their existing perceptions (Heuer, 1999, p8-14; Tetlock, 2005, p123). Culture, as the underpinning driver, corresponds with the real layer, which comprises the causal structures and mechanisms with enduring properties. While it could be argued that culture can change, this is usually slow, and even where a sudden ideological change is forced, such as through a revolution, that will not result in an immediate change of culture.

3.4 Goodman's (2010) elements of deterrence

Returning to the eight elements of deterrence identified by Goodman (2010), the two parties will have different perceptions of each of the elements. The deterrer will make what they consider is a deterrent declaration, but the deterree may interpret this as an aggressive declaration. The interest in a specific situation is likely to be the same, provided that the deterree really has threatened it; however, the value of that interest may vary in the eyes of each. The deterrer will consider

the denial or penalty measures to be proportionate, but the deterree may see them as lower (so worth the risk of them taking the action) or more severe (aggressive). Both parties will have potentially different views of their own, and of the other's, credibility. These different views of credibility, coupled with the different view of the penalty measures, will lead to a different interpretation of the level of fear imposed, and may also impact on the perceived level of reassurance. These factors all come together for each in determining their own version of the cost-benefit calculus. The researcher's interpretation of the relationships between the factors is shown at Figure 3-2.

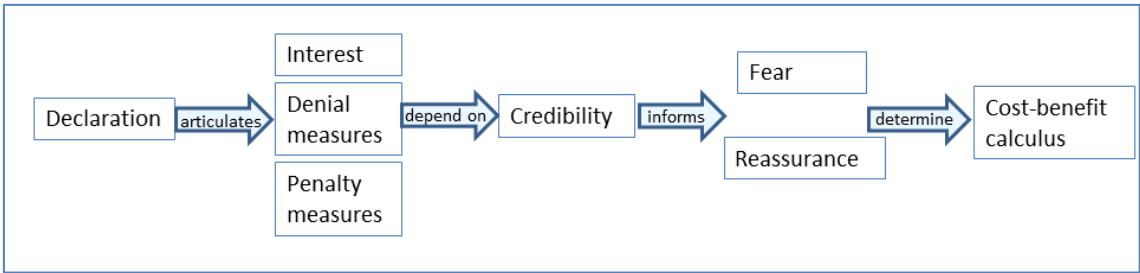


Figure 3-2: Interpretation of relationships between Goodman's (2010) 8 elements of deterrence

Although both parties will have their own perception of each of the elements, the literature review has shown that each party tends to assume the other will take the same view as them, and be 'rational' in that the other will think in the same way they do. This then leads to each party attributing their own view of the eight elements to the other, as shown in Figure 3-3, which uses the analogy of an object which the deterrer sees as a blue square and believes the deterree does also, while the deterree actually sees it as a red circle and believes the deterrer also sees it as a red circle.

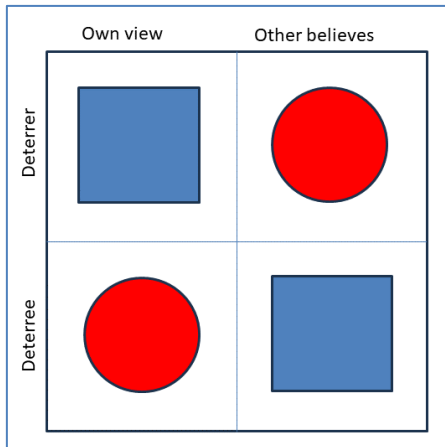


Figure 3-3: Each party attributes its own view to the other

While this might seem to make the conceptual framework excessively complex, it can be simplified in terms of who determines each of the eight elements. The deterrer determines their deterrent declaration which, as Figure 3-2 shows, will articulate the interest and the denial and penalty measures. The effectiveness of the deterrence, however, depends upon the deterree's view of the declaration's credibility which will inform their level of fear and reassurance and in turn determine their cost-benefit calculus. Figure 3-4 shows this overlay of determination.

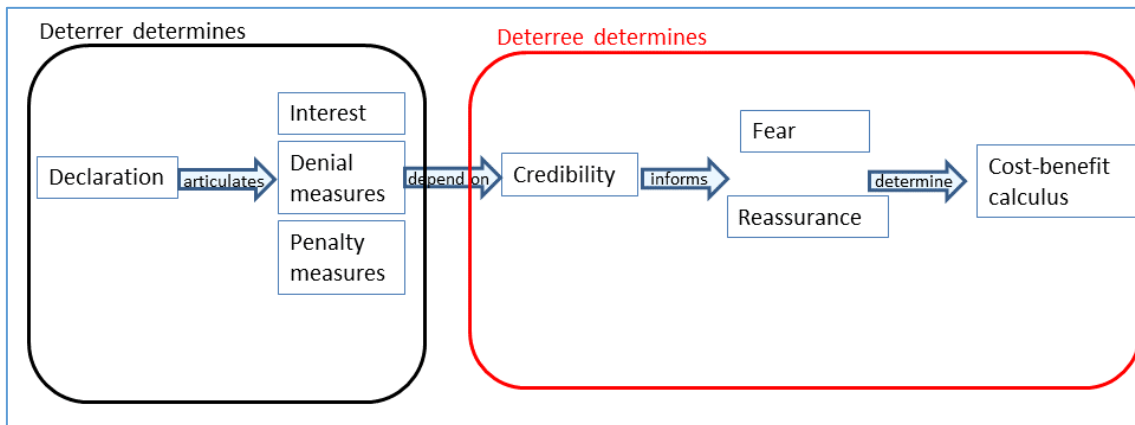


Figure 3-4: Interpretation of relationships and determination in Goodman's (2010) 8 elements of deterrence

3.5 Conceptual framework stage 2: progression

Feeding this development of Goodman's (2010) elements into the conceptual framework leads to two versions of the initial framework, one for each party, as shown in Figure 3-5. Although the deterree is in control of the elements of credibility, fear, reassurance and cost-benefit calculus, the deterrer needs to try to influence these in order to create the best environment for their deterrence to be effective.

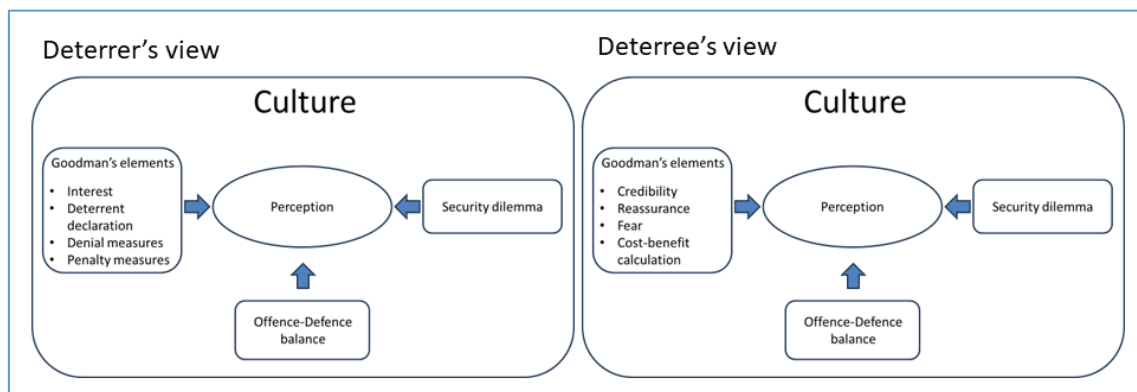


Figure 3-5: Conceptual framework reflecting development of Goodman's framework for deterrer and deterree

3.6 Potential factors for research

The research seeks to answer two questions:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

Looking at the development of the conceptual model at Figure 3-5, the research will need to address the factors that the deterrer can influence, even though they may not have control over the deterree's perception of them. If the deterrer considers how the deterree may perceive a factor, then they can attempt to craft their messaging to try to get the interpretation they intend. This requires some form of measurement, which may be subjective and qualitative but can still attempt to articulate what the perception is considered likely to be. The key in this

measurement is avoiding the temptation to see the deterree as an image of oneself – in other words, to consider the deterree's cultural drivers.

So far, only the elements proposed by Goodman (2010) have been addressed. Other models discussed in the literature review may also offer factors which may contribute to exploring less tangible elements, or may highlight other areas worthy of consideration.

Payne (2011, p349) highlighted a number of factors which might influence potential aggressors, including ideology, geopolitical and domestic affairs (which might distract leaders or encourage them to exploit circumstances to distract their citizens).

Sharp (2017) proposed six factors to measure the credibility and persuasiveness of a cyber threat, which are summarised below:

- reputation for resolve
- political support
- reversibility
- causing private losses
- demonstrating cyber power advantage
- reputation for proficiency.

The overall ratings of the National Cyber Power Index (Voo et al., 2022) offer an independent view of a state's capability and credibility. While the scores against the eight component objectives used to create the overall index may also be useful for deeper insight, they are probably less useful for a high-level view.

The taxonomy of cyber harms proposed by Agrafiotis et al. (2018) addresses different broad themes which focus on the pain inflicted by a cyber attack. Two of the five themes (physical/digital and economic) are comparable with Goodman's interest and denial and penalty measures, while the remaining themes address the less tangible psychological, reputational and social/societal aspects, comparable with Goodman's credibility, fear and reassurance.

States also have important stakeholders, who may be considered in any decision they make, and who will certainly have their own perceptions based on those decisions. These stakeholders may be either internal (such as citizens, businesses, opposition politicians) or external (allies and other states, both neutral and hostile). The perceptions of fear and reassurance may be particularly pertinent with regard to these stakeholders. Fear may align with the concerns of internal stakeholders and with allies, who look to the state to protect them and expect appropriate leadership against threats from other states. Relevant elements from the taxonomy of Agrafiotis et al. (2018), such as damage and disruption from the Physical/digital and Economic categories, or negative changes in perception from the Social/societal category, should therefore be considered in terms of applicability to these stakeholders.

A different perspective may be offered by the taxonomy of responses to actions and emotions proposed by McDermott (2019). Different adversary actions will activate different emotions (fear, anger, surprise or disgust) which then drive different responses (McDermott, 2019, p321). Her taxonomy might give a broader insight into their response rather than the specific concerns which contribute to that response.

3.7 Factors to be considered

Having identified further potential factors from other models, all the candidate factors are evaluated at Table 3-1.

Table 3-1: Factors considered for research

Factor and source	Included	Rationale
Deterrent declaration (Goodman, 2010)	No	This is a statement (verbal or action) to deter. It must be clear and received by the deterree, but that partly depends upon other elements rather the declaration itself.

Factor and source	Included	Rationale
Interest (Goodman, 2010) Also includes: - Physical/Digital (Agrafiotis et al., 2018) - Economic (Agrafiotis et al., 2018)	No	The value of the interest will be assigned by each party for itself. While the deterree may have a very specific view, e.g. for geopolitical reasons, the deterrer is unlikely to have direct influence over this.
Denial measures (Goodman, 2010) Also includes: - Physical/Digital (Agrafiotis et al., 2018) - Economic (Agrafiotis et al., 2018)	No	The measures themselves are completely in the determination of the deterrer, but how they are received will depend upon the credibility of the deterrent declaration.
Penalty measures (Goodman, 2010) Also includes: - Physical/Digital (Agrafiotis et al., 2018) - Economic (Agrafiotis et al., 2018)	No	The measures themselves are completely in the determination of the deterrer, but how they are received will depend upon the credibility of the deterrent declaration.
Credibility (Goodman, 2010) Also includes: - Reputation for resolve (Sharp, 2017) - Political support (Sharp, 2017) - Demonstrating cyber power advantage - Reputation for proficiency - Cyber power (Voo et al., 2022)	Yes	Credibility combines the deterrer's capability size and strength with its political will, in terms of its 'track record'. The deterrer can influence this through their strategies, words and actions.

Factor and source	Included	Rationale
Fear (Goodman, 2010)	No	While the deterrer needs to influence the deterree so that their perceptions about fear match, fear itself it is an abstract that must be articulated as fear <i>of</i> some adversity, such as psychological and social or societal factors, so is addressed there.
Reassurance (Goodman, 2010)	Yes	The deterrer needs to influence the deterree so that their perceptions about reassurance match for deterrence to be effective.
Cost-benefit calculation (Goodman, 2010)	No	This is the result of the deterree's consideration of other factors rather than a factor to be influenced directly, hence it is not included in the list of factors to be considered, but it is recognised as the focus <i>of</i> those factors.
Ideology (Payne, 2011)	No	This is a fundamental element of the deterree's approach to government and internal society which cannot be easily influenced by the deterrer.
Geopolitical affairs (Payne, 2011)	No	May not be possible for deterrer to directly influence the deterree.
Domestic affairs (which might distract leaders or encourage them to exploit circumstances to distract their citizens) (Payne, 2011)	Yes	This covers internal dissatisfaction or unrest within the deterree state from which its government might wish to deflect attention, perhaps by demonstrating the need to pull together in unity against an external threat. This is an area the deterrer needs to consider and try to influence.
Reversibility (Sharp, 2017)	No	Reversibility does not detract from potential seriousness or weakness, and may indicate more power over the recipient (the deterree) than a simple one-way action
Causing private losses (Sharp, 2017)	No	Whether any loss is kept private or made public may be the choice of the deterree rather than the deterrer

Factor and source	Included	Rationale
Psychological: discomfort, frustration, worry/anxiety, loss of self-confidence, negative changes in perception (Agrafiotis et al., 2018)	Yes: worry/anxiety; loss of self-confidence	While these can be influenced by the deterrer, discomfort and frustration will manifest in the worry/anxiety they cause and disruption to daily life (in social/societal factors, including negative changes in perception).
Reputational (Agrafiotis et al., 2018)	Yes: Detterrer's political reputation; how external stakeholders perceive the deterree	This addresses the deterree's view of the deterrer, in terms of its reputation for resolve, which is influenced by the wider view of the deterrer, including their actions outside the specific situation. Reputational also includes the deterree's reputation as viewed by its allies and neutral states, which the deterrer can influence.
Social/societal: negative changes in public perception (e.g. of technology), disruption in daily life activities, negative impact on nation (e.g. services, economy), drop in internal morale (Agrafiotis et al., 2018)	Yes: Each addressed separately	All of these can be influenced by the deterrer. While the quality of the deterree's technology may not easily influenced directly, perceptions of it may be. Demonstrating weakness might reduce the way technology is perceived by the citizens, businesses, allies and the state's leadership.
Emotions (McDermott, 2019)	No	These give a broader insight into the response to the deterrent message rather than contribute to influencing the deterree through it.
Security dilemma	Yes: but only escalation	The deterrer cannot <i>directly</i> influence the deterree's viewpoint, although other factors may indirectly support it. The potential for escalation can, however, be influenced by trying to keep deterrent activities at a level within the deterree's tolerance.

Factor and source	Included	Rationale
Offence-defence balance	Yes: but only attribution	The deterrer cannot <i>directly</i> influence the deterree's strategic intent, although other factors may indirectly support it. Attribution, however, is a factor that influences the offence-defence balance, is highly relevant to cyber activity and can be influenced by the deterrer's approach (although not guaranteed).

The complete list of factors proposed for the research was therefore:

- The deterrer's credibility to the deterree
- Reassurance to the deterree that if they do not act then the deterrer will not take further action
- Potential use by the deterree of any deterrence threat to distract from internal unrest or other political issues
- Worry/anxiety of the deterree's leadership and citizens
- Loss of self-confidence of the deterree
- Deterrer's political reputation as viewed by deterree
- How external stakeholders (their allies or neutral states) perceive the deterree
- Negative changes in perception of technology by the deterree's citizens or businesses
- Disruption to the deterree's daily life activities
- Negative impact on deterree's services or economy
- Drop of deterree's internal morale
- Potential for escalation of the situation
- Deterree's willingness to attribute the deterrer's actions

3.8 Conceptual Framework stage 3: outline for research

The factors for inclusion in the research are shown in the developed conceptual framework at Figure 3-6. In this version the full set of Goodman's (2010) elements are reduced to credibility and reassurance, while the security dilemma and offence-defence balance are replaced by escalation and attribution respectively,

and other factors are added. This reflects the logic about inclusion of factors which can be influenced by the deterrer as set out in Table 3-1. The focus of the factors is the deterree's perception, as before, but the link to their cost-benefit calculus is made explicit as that calculus is what the deterrence seeks to affect through influencing the deterree's perceptions of the different factors. Culture is still the underpinning lens which will affect the deterree's perception of each factor. This version of the conceptual framework was taken forward to the data collection phase of the research.

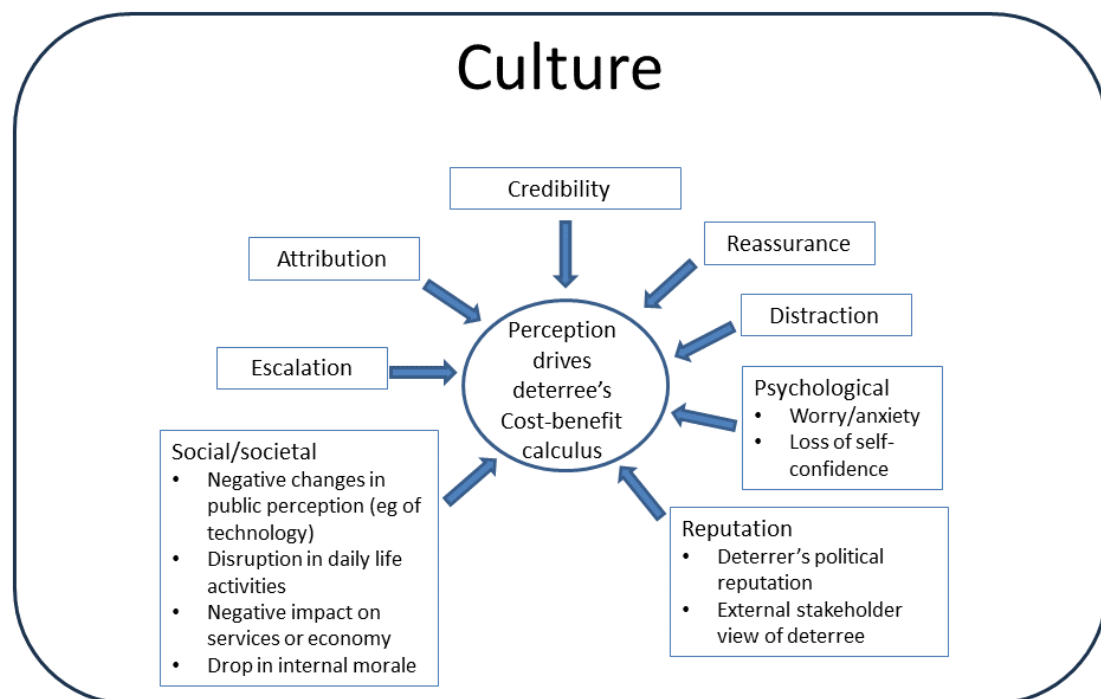


Figure 3-6: Factors affecting deterree's cost benefit calculus which deterrer can influence

3.9 Interplay: the parties and their relationship

One further point needs to be addressed. The term 'interplay' in RQ2 implies interaction between more than one party, and the research needs to be grounded in reality, so that meaningful conclusions can be drawn from it. A way of reflecting this interaction needed to be found.

Initially a simulated scenario with both sides represented was considered, but it would have been unwieldy to administer and, more importantly, would have

required participants to immerse themselves fully in their respective roles while at the same time having a high degree of self-reflection. This could be particularly difficult for those role-playing a context and culture very different to their own. This approach was therefore deemed impractical as it was unlikely to deliver realistic and meaningful insights, and an alternative approach was sought.

As noted in the literature review, although from the outside it may seem clear who is the deterrer and who the deterree, or the potential victim and aggressor respectively, in practice this may not be how the parties see themselves, as suggested by the example world views at Table 3-2. This also includes the viewpoint of the researcher, which generally followed that of the deterrer since it was the deterrer's influence which was being studied. Both sides tend to see themselves as the victim (Lebow and Stein, 1989, p221 and Morgan 2003, p3).

Table 3-2: World views of parties in deterrence situation, including researcher

	Viewer sees party as:	
Viewer	Deterrer	Deterree
Deterrer	Victim	Aggressor Seeker of deterrer's valuable interest
Deterree	Potential aggressor Adverse influence on third parties Possessor of some valuable interest	Victim
Researcher	Victim	Aggressor

This research seeks to identify the factors relevant to the interplay between the parties, and the literature review suggests that considering the situation from the other's perspective is worthwhile. How the deterrer can influence the deterree's perspective will, as shown in the developed conceptual framework at Figure 3-6, include both potential impacts on them as the deterree and their view of the factors relevant to the deterrer. In any situation between deterrer and deterree, the parties will change places as the situation progresses, with each needing to

consider the impact of their course of action on the other party (the deterree), as shown in Figure 3-7(a).

As Lebow and Stein (1989, p221) and Morgan (2003, p3) note, both parties in a deterrence situation tend to see themselves as the defender or victim (so the deterrer) and the other party as the aggressor (so the deterree), as indicated in Figure 3-7(b). The view from each side can therefore be indicated by a simple one-way relationship as shown in Figure 3-8. This indicates to whom the different factors apply, and it is this view, or context, that the deterrer must seek to understand. Thus, the research can usefully be carried out using only the deterrer, not the deterree, and a single-party approach was therefore adopted.

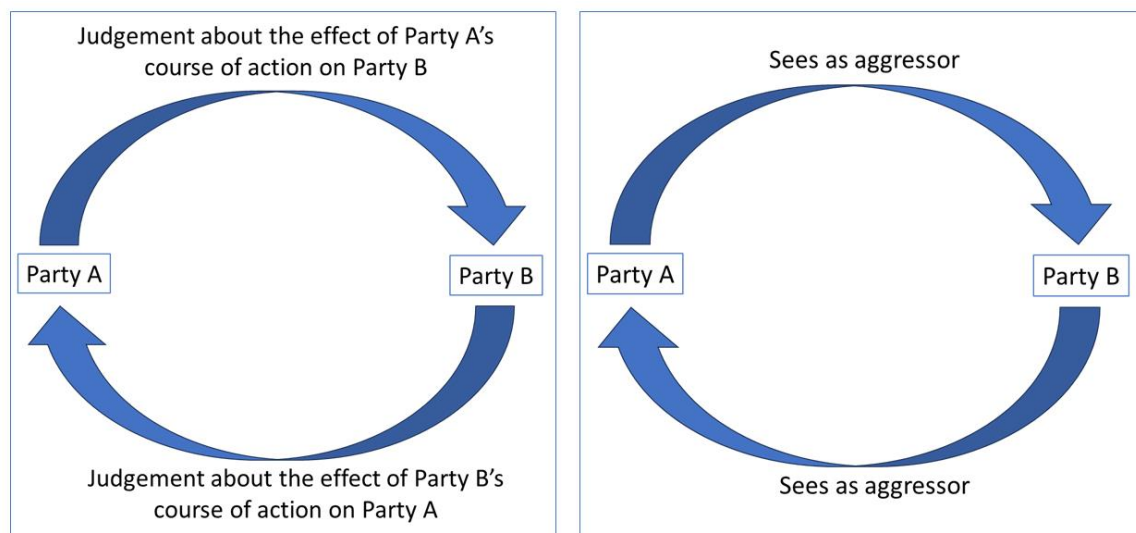


Figure 3-7: (a) The parties change places as a situation progresses; (b) each party sees itself as the victim and the other as the aggressor

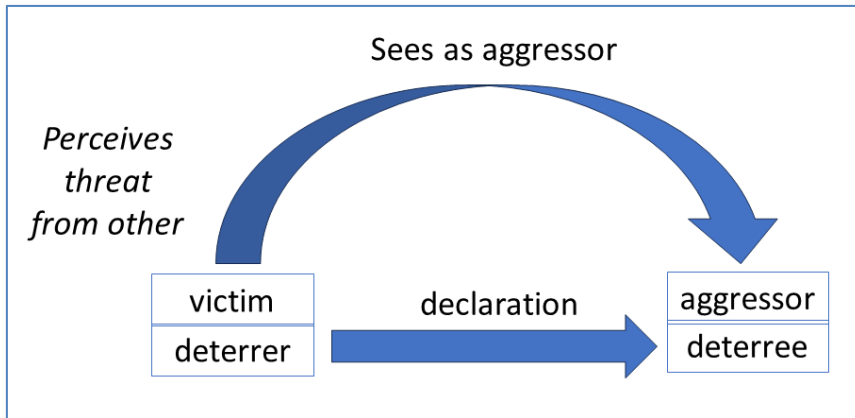


Figure 3-8: One-way relationship from the viewpoint of the victim/deterrer

3.10 Chapter Summary

This chapter has taken the output of the literature review to develop a conceptual framework in order to give direction to the research. It has developed the conceptual framework and explored its component parts, leading ultimately to a version suitable for taking forward the research in line with the methodology discussed in the next chapter.

In doing this, it has refined Goodman's (2010) elements of deterrence and introduced factors from other models relevant to deterrence in cyberspace. Each has been evaluated to determine whether or not it should be part of the research.

Finally, it has considered the intent to address the interplay between the parties, which suggests a need to include both in the research. The difficulty of doing this realistically has been resolved by considering how the two view themselves and each other, and how this changes over time. This has led to a research approach which acknowledges that interplay can be considered from a single perspective.

4 Research Methodology

4.1 Chapter overview

This chapter addresses the research methodology adopted to answer:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

The chapter begins by considering the type of research conducted, and briefly describes the ontology used (critical realism) and its relationship to the epistemology. This introduces the issue of potential bias, and the cultural lens through which the research was approached is discussed. The research strategy (retroduction) and its relationship with the critical realist ontology leads to a description of how this was applied in practice, moving from the literature review through the research elements. A mixed methods methodology comprising of a sequential explanatory design was considered most suitable for the research, and the selection of methods is described and justified, although details about the design elements are given in separate chapters for each element.

Sampling methods are considered and the approaches to sampling for the elements of the sequential explanatory research design are described. The overall plan for data collection is then outlined, including an additional concurrent element added as an opportunity arose, together with a very brief outline of the types of qualitative and quantitative data collected. Again this chapter covers only general points about the relationship between the elements with full details provided in separate chapters for each.

As all data recording, analysis and discussion was pseudonymous, the approach to describing participants by coded identifiers to designate them together with their backgrounds is described, which naturally leads into the final section on ethical considerations and data handling.

4.2 Introduction

For deterrence (including in cyberspace) to be effective, the deterree must have both intended to carry out some action and been dissuaded from it by the deterrer's action. It is, however, difficult to prove causation between the deterrer's action and the deterree's inaction because the deterree may have been influenced by other factors, or may not have intended to act in the first place. Whether deterrence is successful cannot, therefore, be proved scientifically through replicable experimentation. The study of deterrence in cyberspace falls within the sphere of social science, in that it seeks to address aspects of society, behaviour and influence. Further, this research was focused on the behavioural and cognitive elements associated with deterrence in cyberspace, and thus was clearly within the field of social science. It thus aligned with the subjectivist research philosophy, which argues that social reality is created by the perceptions and actions of social actors (Saunders et al., 2019, p135-7), and which accordingly drove the ontology, epistemology and methodology of the research.

Edgar and Manz (2017, p67ff) distinguish four categories of research: observational (suited to broad research questions), theoretical (to explore how a system and its environment behave), experimental (focused on hypotheses and experiments) and applied research (to rigorously quantify a system). They stress that none is "better" than the other categories. Thus it is important to ensure appropriate rigour through systematic and replicable research. The nature of this study lent itself initially to observational research, using exploratory techniques to collect, analyse and interpret observations to search for patterns and arrive at a theory (Edgar and Manz, 2017, p95).

4.3 Ontology

Ontology concerns how we understand what exists and the nature of reality. According to the theory of pragmatism, truth and knowledge can be verified through experience and practice (Howell, 2013, p17). While objectivist approaches seek objective knowledge (which may be appropriate for physical science), this research addressed social science since deterrence depends upon

the actors' perspectives. Experience and practice are therefore confined to the interpretation of meaning to understand how and why things happen.

This is in line with critical realism, as developed by Bhaskar (2008), which views reality as stratified into empirical, actual and real. We experience the 'empirical', but what we experience is only part of the 'actual' events at any time, which result from the 'real' structures and mechanisms (Saunders et al., 2019, p147), as shown in Figure 4-1.

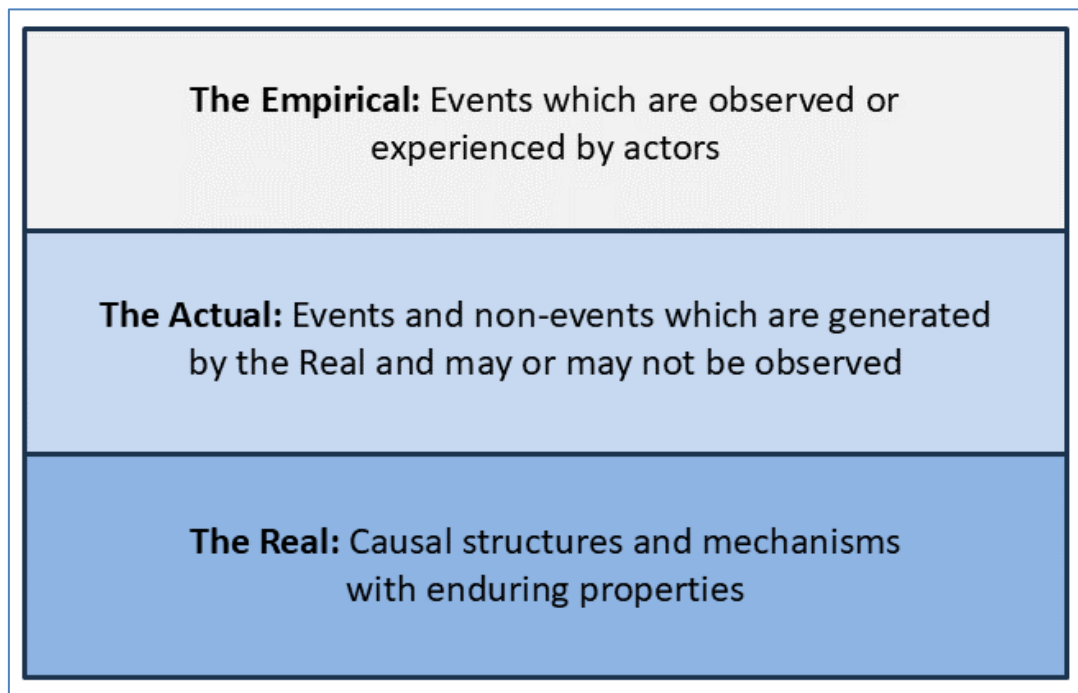


Figure 4-1: Critical realist stratified ontology

Bhaskar stresses that this does not mean that there is any reduction in reality between experiences, events and structures (Bhaskar, 2008, p58). Not only are experiences social products, but so are events, and he therefore sees an “implicit sociology” is necessary for his ontology (Bhaskar, 2008, p57). Further, we act on our environment knowingly and intentionally, and therefore we can identify causes in our environment and recognise where we have acted as a causal agent (Bhaskar, 2008, p117). This view is shared by Fletcher, who notes that “The ability to engage in explanation and causal analysis ... makes CR useful for analyzing social problems and suggesting solutions for social change” (Fletcher, 2017, p182).

The three layers of critical realism allow clear articulation of the viewpoints of different parties. Using the sun as an example, one person (A) might believe that the sun is a blazing mass which lies at the heart of the solar system, whereas another (B) might perceive the view of the sun in the sky as a god who brings warmth and light. On a particular day the sun is obscured. Figure 4-2 shows that A sees this as a solar eclipse and a natural phenomenon, while B sees the same thing but interprets it as meaning that the sun god is angry, and so B immediately prays and offers sacrifices to try to appease the sun god. The following day, the sun appears as normal. A is confirmed in their belief that it was an eclipse. B is relieved that the sun god is no longer angry and is confirmed in the knowledge that their prayers and sacrifices were sufficient to appease the sun god.

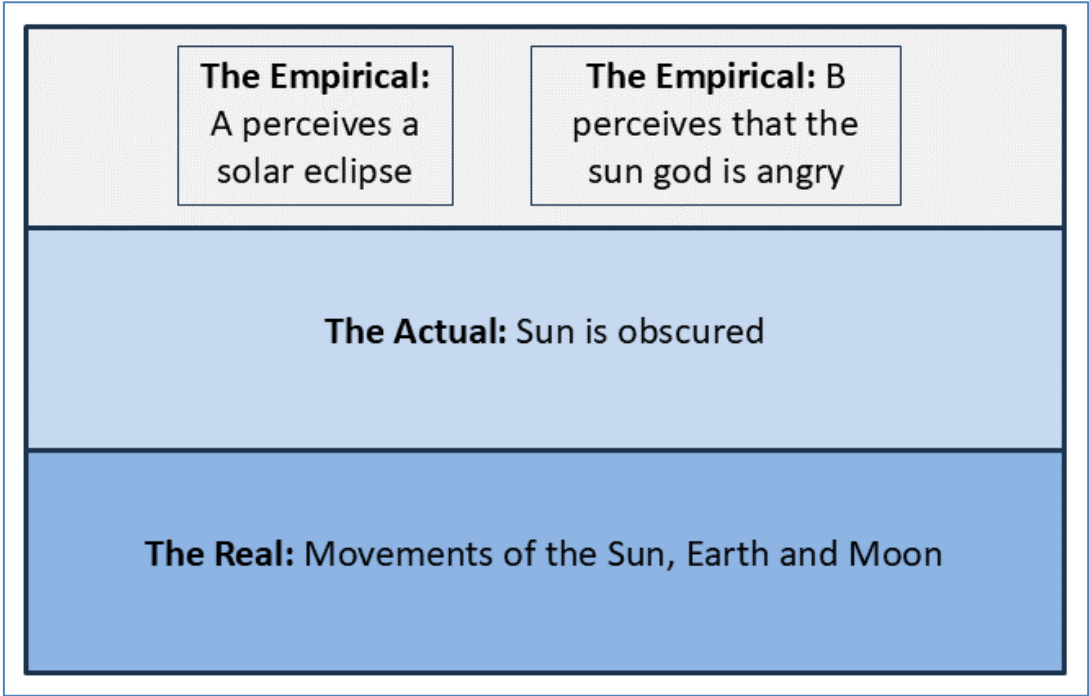


Figure 4-2: Critical realist stratified ontology illustrating different perceptions when the sun is obscured

What is interesting here is that A and B have very different views of the same entity based on their experience and their cultural context. In this example, they cannot both be right about the nature of the sun. Indeed, neither may be completely right, although there may be elements of truth in each. Yet each of them interprets the obscured sun in a way that aligns with their beliefs, and each

finds evidence for that belief when the sun reappears the next day, thus confirming their interpretation level.

Critical realism accepts these different empirical realities and recognises that they do not conflict with the actual (the obscured sun) or the real (the movements of the sun, earth and moon). This reinforces Bhaskar's observation cited above about recognising one's role as a causal agent (Bhaskar, 2008, p117).

In the example of the sun, while the views are polarised, they may be able to coexist without causing serious issues. In other contexts, such as international relations contexts concerning aggression or deterrence, different views can be significant. Figure 4-3 shows the security dilemma (discussed in the literature review) where A is concerned that B poses a threat to their security, so it increases its weaponry in order to defend itself. A now feels safer, but B interprets the increase as posing a threat to its security and feels threatened. As discussed in the Conceptual Framework chapter, the parties change places as B responds by increasing its forces and A feels threatened. These polarised views are reinforced by the tendency for bias towards existing perceptions (Heuer, 1999; Tetlock, 2005). Critical realism is thus particularly appropriate to research such as this where the different viewpoints can have a serious impact on the perceptions of the parties, which in turn influence their actions.

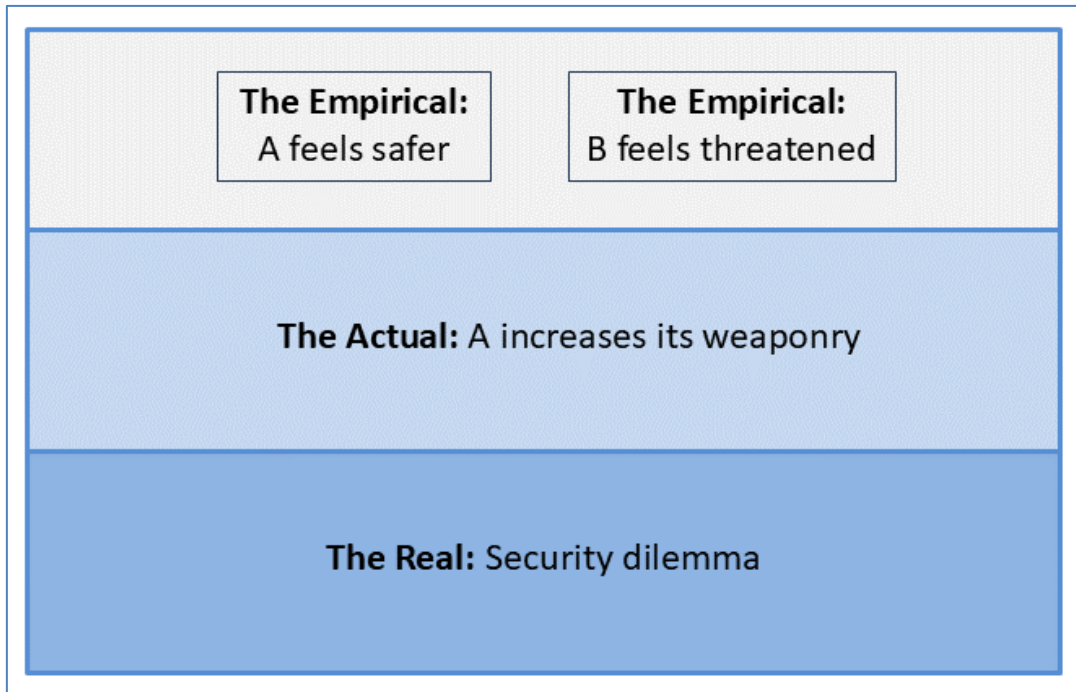


Figure 4-3: Critical realist stratified ontology illustrating polarised views of the security dilemma

4.4 Epistemology

Epistemology addresses the origin, structure, methods and validity of knowledge: in other words, why reality is as it is and how we can know about it. Easterby-Smith et al. (2015, p59-60) note that critical realism is a realist ontology with a relativist thread, and “is located quite close to the middle ground philosophically.” It is concerned with events (observable or otherwise) and the structures and mechanisms which cause them. Knowledge at the empirical level is specific to a situation, and social facts do not have an independent existence but are social constructions agreed on by people (Saunders et al., 2019, p148).

Since critical realism draws upon both positivism and constructivism in its ontology and epistemology, it “functions as a general methodological framework for research but is not associated with any particular set of methods” (Fletcher, 2017, p182). Easterby-Smith et al. (2015, p60) agree, noting that its middle ground position allows “an eclectic approach to research methods”. The researcher must therefore attempt to pursue objectivity while accepting that they

cannot be independent of the cultural influences on them (Saunders et al., 2019, p148).

Hence it is important for the researcher to be clear about how they see the world and to recognise that those with different cultural and historical backgrounds will see different views. This applies to recognising that elements such as actor motivations and deterrence calculus will be affected by viewpoint.

4.5 Cultural lens

This research approaches deterrence in cyberspace through the cultural lens of the Western world, as typified by the United Kingdom, United States and NATO, and specifically uses the UK viewpoint by using the UK MOD definition of cyberspace as well as the research being conducted within the UK environment. As noted in the literature review, the definitions common in the Western world do not always match those of Russia and China, for example, who approach cyberspace differently to the West. While these differences are acknowledged, they are not explored here in detail. This cultural lens impacts on the researcher, those participating in the research and on the subject of the research.

While the UK viewpoint is, as noted in the literature review, aligned to that of other Western states such as the US and France, the differences between these and the viewpoints of non-Western states may reflect either cultural or doctrinal viewpoints. The effect is the same in both cases, and it is reasonable to consider them both as cultural lenses, as doctrine will impose an approach to military activities which will impact on them in a similar way to wider national culture. Similarly, most of the relevant literature has been produced by UK- or US-based authors and published in the UK or US, or by NATO which is heavily influenced by those two states. English-language viewpoints from non-Western states are hard to find, other than through commentaries on it from the Western perspective.

The researcher needs to be aware that this enforces the UK/Western perspective, and to reflect on how this is impacting their research at all stages, from the framing of the research questions and the literature review to the research itself and the conclusions drawn from it. While those participating in the research may

not be aware of cultural bias, and do not need to be, the researcher must recognise its presence and the potential impact on their work. While cultural bias does not of itself detract from the validity of the research provided that it is acknowledged, to fail to acknowledge it would adversely impact on validity if general conclusions were drawn which might be specific to those participants.

As well as the researcher and participants, however, the subject of this research will be affected by cultural bias. Differences in culture and doctrine are not only relevant to academic analysis, but are also important to military and state decision makers, who must take the approach of potential adversaries into account when considering how they may be deterred. The need for communication to be clear and understood was discussed in the literature review, together with the apparent irrationality of actors; this may be linked to cultural or doctrinal difference. However, it may be that actors are not irrational with respect to their own values, but simply that one naturally projects one's own viewpoints on others and fails to see that they may take a different stance or interpret events differently. For example, before World War II, Chamberlain and his military advisers attributed "mirror-image" versions of their own assumptions about strategy and air power to Hitler, and failed to see that he might have views which did not fit with British strategic doctrine (Hughes, 1989, p284). Therefore, it is important to recognise that others will see things differently to oneself.

Lebow and Stein (1990, p353-5) stress the need to try to understand the different perspectives of all parties in relation to deterrence, since each party will have their own view, which will be valid for them. To focus only on viewing an event through the prism or cultural lens of one party necessarily equates to taking a partisan stance on one or other side. While Lebow and Stein (1990) seek to obtain an objective analysis in this way, achieving this in practice will be difficult. Aligned to this failure to understand the potential opponent's cultural lens is a tendency to overestimate the degree of direct influence that one party can have on the other. Jervis (2017, p344-5) notes several examples where influence has been overestimated, including the Germans believing that the reason for the British not bombing German cities early in World War II was that the British were

responding favourably to German restraint, whereas the reality was that the British were short of aircraft – which Jervis considers a striking example “because one expects wartime opponents to attribute the least charitable motives to each other” (Jervis, 2017, p345).

In summary, recognising the researcher’s own cultural bias, as well as that inherent in the data being collected, is vital to ensure as much objectivity as possible while acknowledging the limitations it causes. For the subject of deterrence, in particular, these limitations apply also to the subject matter of the research and the parties involved. As discussed above, critical realism seeks to understand causal structures at the real level through experience at the empirical level, and it accepts the difference between the experience and explanations of different parties at that empirical level. If the researcher understands the limitations imposed by their own cultural bias and that of the participants, and adopts the critical realist non-judgmental stance, they will ensure the validity of the research is maintained.

4.6 Research strategy

The retroductive research strategy is considered by Blaikie (2007), Fletcher (2017) and Saunders et al. (2019) as most appropriate to a critical realist ontology, although Fletcher also suggests a flexible deductive approach is consistent with it (Fletcher, 2017, p182). Retroduction “refers to the process of building hypothetical models of structures and mechanisms that are assumed to produce empirical phenomena” (Blaikie, 2007, p83). It follows a cyclic process of constructing models to represent the structures and mechanisms which explain observable phenomena, and then testing these models by determining further consequences which can be tested empirically. Successful testing will suggest that the structures and mechanisms are accurate. The process is repeated to progressively reveal different aspects of Bhaskar’s three levels of reality (Blaikie, 2007, p83-4).

Since the first stage of the retroductive research strategy is to describe an observable phenomenon, this lends itself to use of an inductive approach to determine the model or theory, which can then be tested through a deductive

approach. Induction begins with an initial theory to facilitate a deeper analysis which will support or deny the initial theory and thus ultimately enable reality to be more accurately explained, which is the intended outcome of retroduction (Fletcher, 2017, pp184, 190).

Applying this retroductive process to this research began with the specific questions to be answered, namely:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

First, the factors referred to in these questions needed to be determined. As Blaikie (2007, p83) notes, the retroductive process begins by discovering the structures and mechanisms which explain observable phenomena, but since these are unlikely to be observable it is necessary to construct a model of them. For this research, the observable phenomenon was the actions (including lack of action) intended to deter in cyberspace and the factors referred to in the research questions were the structures and mechanisms. The literature review explored what factors were relevant to the interplay between the deterrer and deterree (RQ2) and offered candidate factors (empirical generalisations) which could then be combined to create a model or theory to be tested and refined.

The candidate factors identified from the literature review were fed into the research first in the questionnaire where they were tested. The resulting refined model (the set of factors) was in turn fed into the interviews for further testing. Thus the retroductive research strategy was followed. Further specific details about each element of the research are given in the relevant chapters on Data Collection, Review and Results

4.7 Methodology

As noted in the introduction to this chapter, the nature of this study lent itself to observational research, using exploratory techniques to collect, analyse and interpret observations to search for patterns and arrive at a theory (Edgar and

Manz, 2017, p95). This was considered appropriate to understanding the cognitive process associated with deterrence, which seeks to prevent an action through fear of the consequences and thus relies upon the different perceptions of the parties involved. It was therefore important to select the right methodology to acquire knowledge about these perceptions.

Looking at models of deterrence, during the Cold War, nuclear deterrence focused on a simple calculation of strength of arms (Schelling, 1966, p36-7). In the same way, models considering the cyber domain do not seem to have addressed perception. An exception is the “3 player game” (Cui et al., 2017) which was actually one player looking at the historic responses of system administrators and users and deciding whether to attack.

As previously noted, the retroductive research strategy is considered as most appropriate to a critical realist ontology. Its cyclic process and use of inductive and deductive approaches, beginning with an observable phenomenon, allow empirical testing to understand reality, which aligns well with theoretical research grounded in a realistic environment. Critical realism also aligns well with a mixed methods approach to methodology (Saunders et al., 2019, p181).

Mixed methods research uses both quantitative and qualitative data collection and analysis in an integrated manner, and allows different stages of research to be carried out in phases, such as what Saunders et al. (2019, p182) describe as a sequential explanatory design using quantitative methods followed by qualitative methods. Saunders et al. (2019, p185) offer many reasons for using a mixed methods design, of which the most relevant for this research are that one method may be used to define the scope of subsequent research activity using the other, and a sequential approach may allow for the confirmation and elaboration of findings. The sequential explanatory design was adopted for this research to allow quantitative review of the initial list of factors which were then refined into a shortlist to be confirmed and explored through a qualitative approach.

4.8 Methods

Having determined that a sequential explanatory mixed methods approach was appropriate, it was necessary to determine how this would be administered. Quantitative methods include experiments and surveys, while qualitative methods include interviews, focus groups and case studies. Different methods each have advantages and disadvantages, and may also offer different views of phenomena as the situation is interpreted.

Since deterrence may be influenced by many factors, it was important for the research to address the rationale for the importance of factors, which could only be achieved through open questions to elicit the required depth and understanding. While a qualitative approach would have facilitated this, data collection would have been time-consuming and analysis would have been challenging and complex. The sheer number of factors under initial consideration (thirteen) exacerbated these challenges, and risked extensive nugatory work where factors were not found to be relevant. As noted above, a sequential explanatory design was adopted for this research using quantitative review of the initial list of factors to create a shortlist to be qualitatively confirmed and explored. The quantitative element therefore bounded the factors being considered and thus helped to reduce effort on the 'what' in order to give more opportunity to explore the 'why' and 'how' to answer RQ3: "How can these factors be included in deterrence planning for deterrence in cyberspace?"

4.8.1 Quantitative methods

Quantitative methods include experiments and surveys. An experiment was not considered appropriate because, as noted in the introduction to this chapter, the success of deterrence cannot be proved scientifically through replicable experimentation. Robson and McCartan (2016, p249) observe that non-experimental research usually includes a survey of some sort, whether self-administered (internet/postal questionnaire) or by direct interview.

Direct interview by a researcher asking questions and recording responses was not considered appropriate for this study because of the dispersed locations of

the sample and the time that would need to be consumed in working through the questionnaire with each respondent.

A questionnaire made available online to potential respondents is easy to administer and analyse, and lends itself to a larger number of respondents, including those who are geographically dispersed or otherwise difficult to reach. However, while qualitative questions can be included, quantitative ones are more appropriate because of their simplicity and convenience for the respondent. It is hard to know how much engagement or thought concerning the responses has taken place, and the respondent rate must be sufficient to give a representative response. For a subject such as this, where there is no requirement for a statistical representation, what Saunders et al. (2019, p315) refer to as “non-probability sampling” or “non-random sampling” is appropriate, and the required response rate depends upon the research question. This is particularly so in this case as the questionnaire is part of a sequential explanatory mixed methods approach (Saunders et al., 2019, p315-7).

A further development of the questionnaire method is the Delphi questionnaire. The Delphi method (Linstone and Turoff, 1975; Day and Bobeva, 2005) is appropriate where collective subjective judgments from a range of diverse experts are sought, offering an opportunity to explore a subject and seek pertinent information from each contributor (Linstone and Turoff, 1975, p4-5). It uses “an integrated set of surveys, each progressively building upon findings” (Day and Bobeva, 2005, p108) and is based around a series of distinct phases including setting an objective, formulating the problem, testing the solution and circulating results (Sackman, 1974, p3). Delphi is useful “to structure a good communication process in order to obtain a useful result” (Linstone and Turoff, 1975, p5). The iterative approach of feeding respondent results back into subsequent rounds allows consensus on a topic to be sought (although it may not always be achieved), but meaningful results depend upon planning to ensure the quality of the ‘panel’ of respondents (Sackman, 1974, p25). A Delphi study is run over several rounds (often three) to gain consensus, and, like other questionnaire

formats, quantitative questions are most appropriate because of their simplicity and convenience, although qualitative ones may also be included.

For this research, a Delphi questionnaire was considered the most appropriate method for the initial quantitative element of the sequential explanatory design. Use of Delphi would enable a diverse range of experts to reach a consensus of the relevance of the initial long list of factors so that a shortlist could then be taken forward for detailed exploration in the qualitative phase.

4.8.2 Qualitative methods

Qualitative methods include interviews, focus groups and case studies, each of which is considered briefly below.

An interview is “a conversation that has a structure and a purpose” (Kvale and Brinkmann, 2009, p3). It offers an opportunity to probe and is particularly good for open-ended questions providing qualitative data. Semi-structured interviews use an interview schedule to ensure coverage of relevant topics while also allowing free-flow discussions where appropriate, so that the subjects’ expertise and point of view can be explored. They further allow the interviewer to engage directly with the interviewee to acknowledge responses, seek clarification and offer personal assurance regarding confidentiality. Interviews are, however, time-consuming to administer and analyse, and lend themselves to including a smaller number of participants. Interviews with experts in the field offer greatest value to explore a subject in depth but inevitably reduce the size of the population which can be sampled from. Kvale and Brinkmann (2009, p113) observe that 15 +/- 10 interviews is common, and saturation, the point at which further interviews will not yield additional insight, may require no more than twelve (Guest et al., 2006).

A focus group is essentially a group interview addressing a particular topic through discussion and interaction between group members (Saunders et al., 2019, p470). They align with a critical realist approach through the interaction and group dynamics. Focus groups are usually face-to-face interactions to give the group coherence, so would not have been appropriate for the geographically dispersed sample required for the qualitative element of this research. Group

discussion would also have potentially restricted participants' willingness to be candid in their responses.

A case study is an in-depth study into a topic or phenomenon within its real-life context (Saunders et al., 2019, p196). While this might appear to fit with a study into deterrence in cyberspace, it is difficult (as noted in the introduction to this chapter) to recognise whether deterrence is indeed taking place and operating as a causal factor in another party's action. Further, reports of historic events will be subject to the bias of the reporter, however hard they have tried to be objective and factual, and the researcher would thus be exploring the empirical level of reality as seen by the reporter, so at one level removed. For these reasons a case study was not considered to be a useful method for this research.

Regardless of the method used, it is important to avoid bias caused by how the researcher asks questions, and to recognise that the researcher will also bring their own interpretation to the research process and data. The results and analysis will therefore reflect the culture and experience of all participants (including the researcher).

For this research, semi-structured interviews were considered the most appropriate method for the qualitative element of the sequential explanatory design. These interviews would build on the findings of the prior quantitative questionnaire, and allow a high level of engagement between the researcher and the interviewees so as to gain most benefit from their expertise.

4.9 Sample selection

The ideal population for this research would be those targeted by deterrence approaches (i.e. leadership of states who are deterred or not deterred). It was, however, impossible to sample these, as they were unlikely to respond to questioning from a researcher, might not acknowledge whether they had been deterred (or not), and indeed might not realise whether or not they had been deterred. Indeed, the difficulty of obtaining data about decision making, especially that relating to "elite decisionmakers associated with security and foreign policymaking" is acknowledged by Lin-Greenberg et al. (2022, p84).

In order to allow practical but realistic and useful research, it was decided to use a sample with appropriate expertise in at least one category from cyber operations, military doctrine, operational planning, intelligence and cultural factors. These categories allowed a wide range of views and understanding of situations, and the researcher was fortunate in having good professional connections with some leaders combining depth and breadth of expertise across these areas. While they did not represent precisely the actual population described above, there were strong overlaps in terms of leadership and those who influence them through their training and practical expertise, and these categories allowed the expertise of those addressing particular elements to be tapped.

For clarity, expertise in cultural factors was used to refer to those with particular insights into other (non-Western) cultures through exposure to them by study and, in at least one case, through having resided in a non-Western state. This gave an insight into the behaviours and strategic culture of other states, but in a different way to that which would be taken by an anthropologist, who would seek to understand societal structures and customs and their impact more generally. The focus of the cultural expertise within the sample was, however, appropriate for this research.

The types of sample considered for this research were:

- Purposive sampling: the researcher uses their judgment to select participants who may be particularly informative with respect to the research question (Saunders et al., 2019, p321). Since purposive sampling relies on the researcher's judgment, ensuring an appropriate sample is particularly important and may skew the findings of the research.
- Convenience sampling: participants are identified because they are easily available or convenient, and is a form of haphazard sampling, although Saunders et al. (2019, p324) note that samples selected for convenience often meet the criteria for purposive sampling.
- Self-selection sampling: the researcher advertises their research through an appropriate means and invites volunteers to respond (Saunders et al.,

2019, p323). There is a risk that participants may have strong views and not be representative of the whole relevant population.

- Snowball sampling: this is another form of volunteer sampling where initial participants are selected by the researcher and invited to identify further potential participants (Saunders et al., 2019, p323).

Saunders et al. (2019, p316) suggest that where a sample need not represent the population proportionally as no statistical inference is required, but access may be difficult, then snowball sampling may be most appropriate. If, however, access is not difficult and there is a clear focus for selecting the sample, then purposive sampling may be most appropriate.

While a purposive sample is ideal for a bounded subject, such as deterrence in cyberspace, it had been deemed impossible, as noted above, to sample the actual population who are targeted by deterrence approaches. However, the researcher's professional connections would offer a suitably expert sample as a start point. These were not, however, large enough as a sample or comprehensive enough in terms of expertise coverage to meet the full needs of the research, which sought a spread of expertise across the relevant areas of cyber operations, military doctrine, operational planning, intelligence and cultural factors, in order to determine a generalised view.

For the initial quantitative element (Delphi questionnaire) a convenience approach, utilising those to whom the researcher had access, supplemented by suggested contacts from others (in line with the snowball approach), was therefore used, together with a self-selection approach advertising the research to those studying for a Cyber Masters degree with Cranfield University. These students are principally military officers employed in areas relevant to the research who will also have undergone military Staff College training and will have a broad perspective on military issues and a sound foundation on aspects of cyber activity at a practical level. They are seen as future leaders in this field (and indeed some of the other participants were previous graduates of the course). In the event, this was not as fruitful a source of candidates as had been hoped.

The Delphi questionnaire was used both to gather quantitative data and to identify a potential follow-on interview sample. The interview stage was purposive, in that the sample was selected from questionnaire respondents either because they were already known by the researcher to have particularly relevant expertise, or because their specific expertise offered additional value. This latter was the case for some of those with strong cultural factors backgrounds, the majority of whom were not previously known to the researcher.

4.10 Plan for data collection

As noted above, a sequential explanatory design was adopted for this research. The first element of the research design was a quantitative review of the initial list of factors identified following the literature review, in the form of a Delphi method questionnaire. This was used to create a shortlist to be confirmed and explored in the second, qualitative, element conducted through semi-structured interviews.

The quantitative element therefore provided the principal answer to RQ2: “What are the main factors relevant to the interplay between the deterrer and deterree?” The qualitative element was then able to address the rationale behind the choices and move towards answering RQ3: “How can these factors be included in deterrence planning for deterrence in cyberspace?”

As well as these two elements, the opportunity arose for an additional group workshop with a relevant group, so the original plan for a sequential explanatory design was modified to have an additional concurrent phase added, as indicated in Figure 4-4.

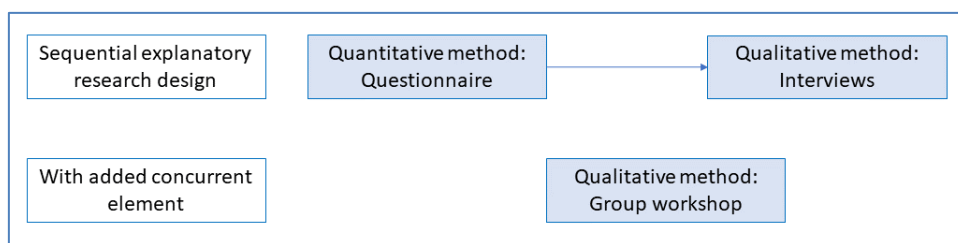


Figure 4-4: Sequential research design with additional concurrent element (adapted from Saunders et al., 2019, p182)

Each of the elements is discussed briefly below and in more detail in the relevant sections on 'Data Collection, Review and Results' in Chapters 5, 6 and 7.

4.10.1 Delphi Questionnaire

The first element of the explanatory design process was the quantitative Delphi model questionnaire, which addressed RQ2: "What are the main factors relevant to the interplay between the deterrer and deterree?" As described above, this approach was considered the most appropriate way to reach consensus among a diverse range of experts. Up to three rounds of Delphi method questionnaires were anticipated to reduce the initial list of factors identified in the literature review to a short list output that could be explored in the interviews. In the event, however, as the responses to the initial questionnaire were reviewed it became obvious that five factors were the most popular, and so the level of consensus made a second round unnecessary. Further detail on the results and the decision to stop after the first questionnaire is given in the Questionnaire: Data Collection, Review and Results chapter, and the initial questionnaire is shown at Appendix A.

4.10.2 Interviews

The second element of the explanatory design process was the set of qualitative semi-structured interviews, which explored the rationale behind each of the shortlisted factors (identified by the Delphi questionnaire) in support of RQ2 and began to address RQ3: "How can these factors be included in deterrence planning for deterrence in cyberspace?" The interview script was developed to take advantage of the open-ended nature of semi-structured interviews. It covered not only why the interviewee had assessed the factor as one of the most relevant (or not), but also follow-on questions such as about the circumstances under which the factor might be desirable, its impact on the state and how it could be taken into account in planning. A final general section addressed culture and offered the World Values Survey (WVS, 2022) as an example of a practical framework to probe views on categorising culture. The interview script is at Appendix B.

4.10.3 Group workshop

During the research I was invited to give a lecture to a small class of Cyber Masters students at Cranfield University, and offered the opportunity to hold a workshop with them, which I accepted. The workshop took place after the initial quantitative Delphi questionnaire had been completed and during the analysis of the results. It was also possible that some members of the group might already have already contributed to the Delphi questionnaire as it had been made available to students on the Cyber Masters course.

Given the military community studying on the course, it was instead decided that a workshop would offer an opportunity to explore their thoughts about planning and cyber operations through a simulation, thus producing additional qualitative data. The workshop began by presenting a scenario where cyberspace had been suggested as a route for deterrence, and the students were asked to work in two groups to make recommendations. After the scenario a group discussion was held to hear their thoughts about relevant factors for planning. The workshop materials are presented at Appendix C.

4.11 Data collection

Across the three research elements, most of the data collected was qualitative, although the Delphi questionnaire gave mainly quantitative output. The quantitative data addressed the relevance of specific data elements, while the qualitative data included additional elements suggested for consideration in the questionnaire, and the rationale for responses collected in interviews. The group workshop produced qualitative data about the options selected in the simulation, together with personal and group reflection on the exercise.

Data was analysed in a manner appropriate to the type and quantity of data. For the questionnaire, the quantitative data was recorded in a spreadsheet and the total figures analysed, both for all respondents and for subsets (such as for those with particular expertise). The additional free-text comments were reviewed and grouped into common themes.

All data from the interviews was reviewed and coded using a thematic analysis approach (Saunders et al., 2019, p651-2). This allowed the analysis to compare and contrast different views, drawing out common and divergent themes. Full details of the coding are given in the chapter on Interviews: Data Collection, Review and Results.

The group workshop produced a very different set of qualitative data, which was reviewed separately. The views of the two groups and individual participants' personal reflections were analysed for common themes and differences, and the subsequent group discussion reviewed for key points.

Fuller details about the storage and analysis of data are given in the relevant sections on Data Collection, Review and Results in Chapters 5, 6 and 7.

4.12 Participant identifiers

All data recording, analysis and discussion was pseudonymous, so that the individual identities of participants were protected. This was important to ensure candid responses which could not be attributed by name and benefitted the research through more open discussions than might have been expected from some quarters. All individual records are therefore identified by numeric identifiers containing encoded descriptors of the individual's background experience.

Limited personal data was collected, consisting of the contact details (email and optional telephone number) of questionnaire respondents with generic descriptions of their background (expertise). These details were stored separately and will be destroyed after the assessment of this thesis. Interviewees were selected from questionnaire respondents, so were already allocated numeric identifiers, apart from two additional interviewees who were allocated numeric identifiers at the time of their interviews.

The numeric identifiers for questionnaire and interview participants consisted of a two-part code where the first part denoted the background of the individual and the second part was a decimal integer value, assigned in order of receipt of first

response from the individual³. The first part (background) was articulated as an 8-bit hexadecimal value formed as shown in Table 4-1. This approach allowed multiple backgrounds to be recorded for an individual by adding the relevant bits together to give a value between 00 and 2F⁴ (although in practice “Other” was never used).

Table 4-1: Hexadecimal values to indicate background(s) of participants

	Bit	Value binary (hexadecimal)	Meaning when set
Hex digit 1	1 (most significant), 2	n/a	Not used
	3	0010 0000 (20)	Other (detail separately recorded)
	4	0001 0000 (10)	Understanding different cultures
Hex digit 2	5	0000 1000 (08)	Intelligence analysis
	6	0000 0100 (04)	Military planning
	7	0000 0010 (02)	Cyber leadership/management, including Cranfield Cyber Masters course
	8 (least significant)	0000 0001 (01)	Cyber technical

As an example, 14-26 indicates an individual with experience of both understanding different cultures and military planning, whose first response was the 26th received. This approach is described in more detail at Appendix D.

A slightly different approach was used for workshop participants, who were only allocated identifier numbers based upon the group they were in for the simulation. Their codes are allocated as G-xy where x is the group number for the simulation and y distinguishes individuals within that group. As an example, G-2g indicates a member of group 2 for the simulation, who is identified as g to distinguish them from other group members.

³ Responses 1-4 were used in trialling the questionnaire before the research was carried out. The first recorded response was therefore allocated a respondent identifier of 05.

⁴ Hexadecimal uses the digits 0-9, then continues with letters A-F to represent decimal 10-15.

4.13 Ethical considerations and data handling

In any research it is important to consider any ethical implications and to avoid causing harm or anxiety to the sample, or anyone else, or to put them in a difficult position. This study sought to minimise any such impact. Since the approach was to seek opinions, there could be no physical impact, and participants were reassured that all responses were valid, and that the researcher had no prior expectations and would not be judgmental regarding responses – indeed the specific focus on perception reinforced the validity of all views.

Potential anxiety or feelings of being in a difficult position could be caused by concerns about either disclosure of sensitive material or from participants feeling under pressure to take part. The former was addressed by stressing that any scenarios had been fabricated and that responses must only be unclassified. For the latter, while it was proposed that students studying the Cyber Masters and other programmes would be invited to take part, the researcher had no formal relationship with them so pressure was minimised. Further, anonymity was reinforced and reassured.

Throughout, the privacy and confidentiality of respondents and individual responses was assured, and their informed consent sought to take part, along with their right to withdraw at any point. If exercised, this would have overridden any prior agreement from them to take part in any part of the research.

4.13.1 Ethical approval

Before the research began a proposal was made to CURES (the Cranfield ethical approval system) and MODREC (the Ministry of Defence ethical approval system), and acceptance was received from both. The original CURES reference number was CURES/12446/2020, and the project title change request was CURES/23849/2024. Consent forms were created and used for each primary research exercise, and are included in the relevant appendices. All participants were over eighteen years of age, but otherwise there were no restrictions in terms of age or sex, and these attributes were not known for the sample.

4.13.2 Data storage

All data was stored in a private area for access only by the researcher on the Ministry of Defence information technology system at the OFFICIAL classification. Personal data was held in a separate file containing the email address and background descriptors, and marked as OFFICIAL-SENSITIVE PERSONAL (in line with the government security classifications policy in force at the time questionnaire responses were received).

Collection of personal data was limited to contact data and generic professional background. This was stored separately to the data to be analysed and will be destroyed once the final grading has been awarded to the thesis. The research data for analysis will be retained in pseudonymous form and is published as appendices in this thesis.

4.14 Chapter summary

This chapter has addressed the research methodology and how it supports answering the research questions using the critical realist ontology and a mixed methods approach combining quantitative and qualitative data collection. It has considered the risk of bias from the researcher and the data collected, and discussed the relationship between the different elements of the research with a basic outline of each, to be developed further in the next three chapters.

The approach taken to sampling for the questionnaire and interviews and to protecting the identities of participants has been explained, and the ethical considerations around participants and the storage of research data have been addressed.

Further detail on much of the content is provided in the next three chapters, which explore the Delphi questionnaire, the simulation workshop and the interviews respectively.

5 Questionnaire: Data Collection, Review and Results

5.1 Chapter overview

This chapter addresses the approach to collecting and reviewing data from the questionnaire. This takes the development of themes to be explored from the Conceptual Framework into the first stage of research in support of answering:

RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?

The chapter begins by outlining the data collection approach used for the questionnaire, leading on from the overall approach to research data and expanding on the brief review of the Delphi method set out in the Research Methodology chapter above. Comments on the selection of the sample justify the approach taken. The questionnaire and its application are then introduced.

Following this, the response rate and respondents are considered and the results are presented. The results address each part of the questionnaire in turn: the scenario, any additional factors offered and the factors seen as most relevant. These were, as the final section indicates, taken forward to the interviews alongside suitable interview candidates identified from the questionnaire sample.

5.2 Approach to data collection

The quantitative Delphi model questionnaire was the first element of the explanatory design process. The objective of this element was twofold: first, to reach consensus about a short list of the most relevant factors from those identified in the literature review and articulated in the conceptual framework as most relevant to the interplay between the deterrer and deterree; and second, to identify both appropriate factors and appropriate interviewees to take forward to the interviews.

As described in the Research Methodology chapter, a Delphi method questionnaire run over up to three rounds was considered the most appropriate way to reach consensus among a diverse range of experts. However, while up to three rounds were anticipated to be needed to reduce the initial list of factors

identified to a short list output to be explored in the interviews, the results of the first round were decisive and so only one round was needed. This flexibility was in line with the research philosophy, and care was taken to ensure that the overall plan for the data collection was not compromised.

5.2.1 Delphi method

Delphi was deemed an appropriate method because its approach lent itself to exploring the subject of deterrence in cyberspace and seeking pertinent information from each contributor, in line with Linstone and Turoff's critique of its usefulness (1975, p5). Day and Bobeva (2005) see the method as valid for both scientific and interpretive research with the researcher as facilitator, and they promote a structured approach to design, implementation and evaluation.

Not all reviewers of Delphi are positive, however. Sackman (1974) is scathing about the lack of rigour and poor approach to process, and notes (p62) that the anonymity of the Delphi process leads to a complete lack of accountability, where the researcher is merely reporting group opinion, while the anonymous panellists are not held to account for any specific opinions. Most of Sackman's criticisms relate to a poor approach to process in identifying experts, questionnaire design, promoting groupthink in workshops as consensus, and the analysis and presentation of results. While the early Delphi studies he addresses may exhibit some or all of these failings, the fault should not be attributed solely to Delphi. Rigour and intellectual scholarship are needed in any approach.

To counter Sackman's criticisms, the selection of experts has already been discussed, and was specifically designed to give value. Further, the questionnaire plan was intended to reduce any risk of bias or groupthink by offering a range of options to respondents and also seeking their additional suggestions. The intent was to take those offered options scoring at least moderately well in the first round and supplement them with any suggestions offered in the second round, and, if necessary, close in further on the most popular options in a third round.

5.2.2 Sample

As noted in the Research Methodology in Chapter 4, a convenience approach was used, utilising those to whom the researcher had access, and supplemented by suggested contacts from others (in line with the snowball approach). Additionally, those studying for a Cyber Masters degree with Cranfield University were invited to take part on a self-selection basis (although in practice only five respondents came from this source). Those invited (including the Cyber Masters students) had suitable expertise and most were leaders with depth and breadth of expertise in relevant areas.

Unlike most Masters degree programmes, the Cranfield University Cyber Masters has a unique targeted population. It is specifically designed for, and only open to, military personnel from the UK and its key partners, and to some defence civilian personnel. All those selected are recognised not only for their academic ability but also their potential as future leaders in cyber-related roles. The students on the course thus have a level of expertise relevant to this research.

Sackman (1974, p33) notes that while convenience sampling is attractive because it is easier, it can lead to participants having similar backgrounds and thus inhibit diversity of thought. This criticism is echoed by Robson and McCartan (2016, p281) who refer to convenience sampling as “probably one of the most widely used and least satisfactory methods of sampling”. In this research, however, the risk was mitigated because the criteria for sample selection had been defined for different groups of expertise relevant to the research.

5.2.3 Questionnaire

The questionnaire, which had been expected to be the initial Delphi questionnaire (see Appendix A), began with a consent statement and acceptance outlining details of the study and seeking the email address and optional phone number of the respondent together with an indication of their area(s) of expertise and their willingness and preferences to be interviewed. Following this, it offered a scenario describing two states (referred to as “your state” and “the other state”) from the point of view of “your state”, where intelligence suggested an impending potential

cyber attack on a critical national infrastructure⁵ (CNI) asset within “your state” by “the other state”, and the leadership of “your state” was considering activity in cyberspace to deter this threat. The respondent was told they were in the role of an adviser to the leadership, advising on and considering the likely effectiveness of the deterrence activity.

Respondents were not asked what type of deterrence activity they would recommend to their leadership. Doing so was considered, but this was decided against as the focus of the research was on the factors which might be relevant and asking about the proposed activity might have distracted respondents from those factors to the proposed activity. In the same way, while the language of “your state” and “the other state” might be considered cumbersome, it was deliberately chosen following the approach taken by Schechter et al. (2021) who used the terms “our state” and “other state”, and had selected those names “to discourage easy analogy or caricature, but emphasizing their alliances” (p519). The scenario was offered as a potential tool to help respondents contextualise their thoughts, and respondents were asked if they found it helpful, and comments on it were invited.

The main part of the questionnaire offered thirteen factors suggested by the literature (as previously established and described in the Conceptual Framework chapter) and respondents were asked to identify the five most relevant factors. Limitations caused by the use of Microsoft Forms (which was used because of its familiarity to the target audience and because it would run on the main MOD information system) meant that the factors could only be marked as relevant, rather than being ranked as 1-5 (which might have been preferable, although the approach used did avoid respondents debating over the relative relevance of their

⁵ CNI is defined as “Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or
b) Significant impact on national security, national defence, or the functioning of the state.”
(Great Britain. National Protective Security Authority, 2024)

five factors). Up to three additional relevant factors were also invited in a free text box, and as ranking had not been possible, the respondent was also asked to give their top two factors, which could include one or more of the additional factors offered. Finally, respondents were invited to offer any further comments.

The questionnaire was trialled with non-expert colleagues to check that it was clear and that responses were delivered in the expected format. This exercise highlighted a couple of very minor problems with wording and with a comment question being mandated in error: these points were resolved before the questionnaire was made live to the intended sample and the trial responses were discarded.

5.3 Data collection and management

Data was collected from questionnaires using Microsoft Forms, and transferred to, and stored as, Microsoft Excel files. Microsoft Forms was selected because of its familiarity to the target audience (which consisted mainly of serving military and MOD civilian personnel) and because it could be accessed easily on MOD systems (unlike some tools).

Microsoft Excel was selected because of the researcher's familiarity with it, which allowed easy sorting and collation of data for analysis, and because Microsoft Forms exports directly to it. It was initially anticipated that there would be no more than 200 separate responses (treating each round of the questionnaire as a separate response), and so the data could be easily managed in this way. In the event, there were fewer responses and only one round.

5.3.1 Responses

The first Delphi questionnaire was duly sent out in line with the planned approach to the target sample. It had been anticipated that the bulk of the responses would come from the students, as the experts might be too busy or unwilling to take part. In the event, while only a few students responded, most of the experts selected from the researcher's contacts not only responded themselves but many also suggested other well-placed contacts, many of whom also responded. When the closing date for the questionnaire arrived (after four weeks) 32 responses had

been received. A summary of the responses including comments is at Appendix E.

As a number this appeared disappointing, and had these responses been principally from students the exercise would have been worthwhile but frustratingly low. However, the majority of responses (81%) were from experts, whose opinions were both valid and valuable, reflecting those who would be offering advice in a real situation. A further 16% were from Cyber Masters students, who have a broad perspective on military issues and a sound foundation on aspects of cyber activity at a practical level. The low response rate was therefore justified by the quality of the responses. Figure 5-1 shows the expertise areas claimed by the respondents, which were considered to be an accurate reflection in view of what was known by the researcher about both the individuals invited and the military training that many of them would have received.

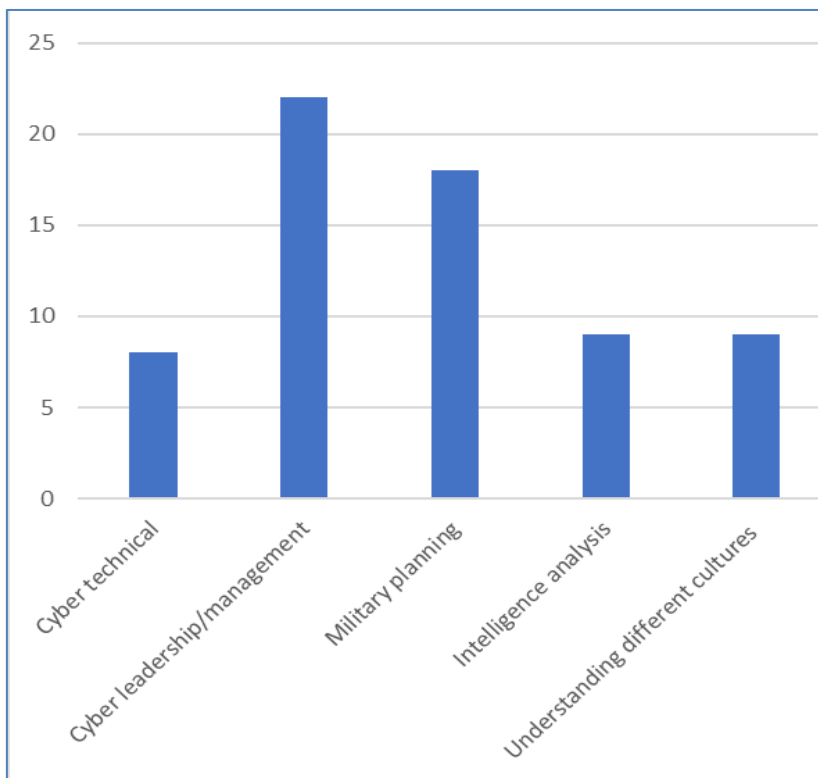


Figure 5-1: Questionnaire respondent expertise (multiple responses permitted)

Note that two respondents did not claim any expertise in any of these categories. One of these is a policy lead in another operational domain related area, and so could offer an informed response from their experience of that, while the other was an additional contact whose background was unknown to the researcher. Their responses were in line with others received, and it would not have made any difference to the final selection of five factors if their responses had been excluded. Their inputs have therefore been included in the final data.

5.4 Results

5.4.1 Scenario

Responses to the initial question about the scenario indicated that a large majority of respondents (25) found the scenario helpful. Some commented that it set out the context (14-26) and the parties' position (0B-29), although there was a clear appetite for more information. 14-26 continued by noting that they would like to know more about the adversary's longer-term history and rationale for the threat. 14-16 thought the scenario was "useful to shape the conceptualisation of how the states are likely to behave" but also wanted wider contextual information, while recognising that this may have been deliberately excluded (as indeed it had been). Also deliberately excluded were other levers of power such as conventional (kinetic) force, diplomatic and economic influences, which were mentioned by several (particularly 0F-07, 0E-22 and 1C-33). The initial version of the scenario, created originally to explore a two-sided scenario working through deterrer actions and the response of the deterree, had originally included scores out of 10 for factors such as conventional military capability, cyber military capability and the level of diplomatic and economic punishment which could be imposed, but these were omitted from the revised approach because the scenario was intended only as a handrail to spark consideration rather than the specific situation to be addressed.

Seven respondents did not find the scenario helpful. Reasons given touched on the vagueness of situation (07-13 and 07-35), the lack of detail about the economic dependencies between the two states (02-14) and the overly simplistic nature of the descriptions (16-34). These echoed the comments of some of the

positive responses referenced above. 04-19 offered the valid criticism that the scenario “implies that a one-off cyber operation would have deterrence effect which does not take into account contemporary (and prevailing) theories of integrated deterrence and cyber persistence.” This was not the intention of the scenario, but perhaps that could have been made clearer in the introduction.

Two respondents offered a cultural perspective. 16-34, who did not find the scenario helpful, noted that “Liberal democratic values for instance are not universally held in regard around the world. Likewise, government influence and a level of authoritarian behaviour may be viewed by some as acceptable.” Another, while positive about the helpfulness of the scenario, and presumably commenting on the initial statement given about the context of the research, observed that “We often look at these situations for [sic] a western perspective. It is difficult to put yourself into another culture and take another view point. We also need to remember that there are no right or wrong answers here. Some of this is new ground.” (1E-08). Again, the simple one-sided scenario presented in the questionnaire differed from the original version in viewing the situation solely from the perspective of “your state”, whereas the original two-sided version had offered two distinct views of the two states from the viewpoints of each (see Appendix F). The two respondents had recognised the need to try to put themselves in the other party’s shoes, and such an empathetic approach would seem necessary to see how one’s own actions might be perceived by the other.

5.4.2 Additional factors

Following the scenario and the question about its helpfulness, respondents were then asked to indicate the five most relevant factors from the list of thirteen offered. In addition to the options offered, the questionnaire invited respondents to suggest further relevant factors, and many did so. The full list of these is at Appendix E.

Some of the additional factors were related to the listed factors, such as the other state’s ability to attribute the deterrer’s actions, which was mentioned by two respondents, one of whom commented “similar to B I guess” (respondent 00-27). Similarly, two respondents proposed factors closely aligned with the self-

confidence of the leadership of the other state: one focused on their leadership/military confidence in the effectiveness of their defence, while the second suggested overt disruption to the elite surrounding the state's autocracy. Others proposed imposing costs (linked with disruption to daily life, worry/anxiety of their leadership and citizens and impact on their services and economy) and the willingness of one's own state to escalate (aligned with the potential for escalation).

Other proposed additional factors were aligned to the overall focus of the research. One such was "The willingness of the deterring state to publicly announce Govt policy describing their position on the threshold for a cyber attack to constitute an attack serious enough to warrant a conventional kinetic or other military response" (respondent 06-11), which is related to the deterring state's political reputation and the research focused on how to address the other's perception of this. Similarly, "Societal support both as a deterree and within the state being deterred" (respondent 00-27, who was a policy lead for another military domain of operations) and "Whether there is a credible 'theory of change' linking our planned cyberspace activity to the necessary change in adversary thinking such that they become 'deterred'" (respondent 07-35) described what the research sought to explore across the factors.

A number of the proposed additional factors highlighted issues which are important in deterrence but were outside the scope of the research. Examples were clarity and consistency of signalling (respondent 07-05), confidence in own state's resilience (respondent 03-06), why other options were not valid (respondent 02-14) and making it costly for the other state (respondent 0B-29). These are all related to the factors identified by Goodman (2010) and thus are taken as given for the research, while being beyond the research focus of understanding how the factors relevant to the interplay between the two parties can be addressed.

Two proposals are particularly interesting and worthy of being followed up in future research. The first concerns "The extent to which the cyberspace activities expected to deter are integrated with a full-spectrum campaign plan, including

that cross-domain risk is being managed” (respondent 07-35). In a real deterrence situation cyberspace is unlikely to be the only domain of operations. Even if there were no kinetic activity (including exercises or declarations of potential punitive activity) at the least diplomatic levers would be used, possibly with economic measures (or the threat of them). Exploring the level of integration of different deterrence activities, and seeking to draw conclusions about the optimum approach to cross-domain activity and risk, would be a valuable area of research, potentially leaning on case studies of actual situations, although outside the scope of the present study.

The second interesting area, which also reflects the environment of real deterrence scenarios is the “Potential for multiple simultaneous escalations (i.e. polycrisis)” (respondent 18-36). An event such as the threat to CNI described in the questionnaire scenario would not, in reality, occur in a vacuum. The scenario notes that relations between the two states are not cordial, so the threat to a CNI asset may be the latest in a long line of potential incidents. It may also be that more than one threat actor is at play, meaning that deterrence activity must be in the context of multiple adversaries, and so seeking to deter more widely than simply the one other state mentioned in the scenario. Again the effect of a polycrisis on deterrence would be a worthwhile area of study, again probably using historic data, although such data are hard to isolate and explore objectively for the reasons described in the Research Methodology chapter.

5.4.3 Factors seen as most relevant

The complete list of factors proposed in the questionnaire was:

- A. Potential use by the other state of any deterrence threat to distract from internal unrest or other political issues
- B. Other state’s willingness to attribute your state for any actions your state may take in cyberspace
- C. Reassurance to other state that if they do not attack your CNI asset then you will not take further action

- D. Disruption to the daily life activities of the other state
- E. Worry/anxiety of the leadership and citizens of the other state
- F. Self-confidence of the leadership of the other state
- G. Perception of technology by citizens or businesses in the other state
- H. Impact on the services or economy of the other state
- J. How external stakeholders (their allies or neutral states) perceive the other state
- K. Internal morale of the citizens of the other state
- L. Your state's political reputation as viewed by the other state
- M. The credibility of your state's proposed action to the other state
- N. Potential for escalation of the situation

While respondents complied well with the instruction to identify the top five factors, they unfortunately were not so uniform in their compliance with the request for their top two, with some completely missing the instruction that these had to be selected either from their top five or from the additional factors they had offered, and some selecting considerably more than two. It was therefore decided not to count the responses to that question in the analysis, although review of the factors proposed for the top two indicated that their inclusion would not have changed the end result.

As noted above, the reason for using a Delphi study approach was to identify a small number of factors from a selection offered, together with any additional factors suggested by respondents. It was therefore intended (and expected) that a second, and possibly third, Delphi round would be needed to identify factors to forward to interviews. As the responses were received, however, it quickly became obvious that five factors were the most popular, and very few additional factors were offered, but these were either covered by other factors or outside the scope of the research. It was therefore decided to use these five most popular as the basis for the next phase of research, rather than running a second round

to arrive at the same conclusion. The results received are summarised at Figure 5-2 and the selected factors were (reference to Figure 5-2 shown in brackets):

- Potential for escalation of the situation (N)
- The credibility of your state's proposed action to the other state (M)
- Impact on the services or economy of the other state (H)
- How external stakeholders (their allies or neutral states) perceive the other state (J)
- Other state's willingness to attribute your state for any actions your state may take in cyberspace (B)

These five factors were taken forward for in-depth consideration in the interviews and are discussed in Chapter 7.

All comments offered in the questionnaire responses are listed at Appendix E.

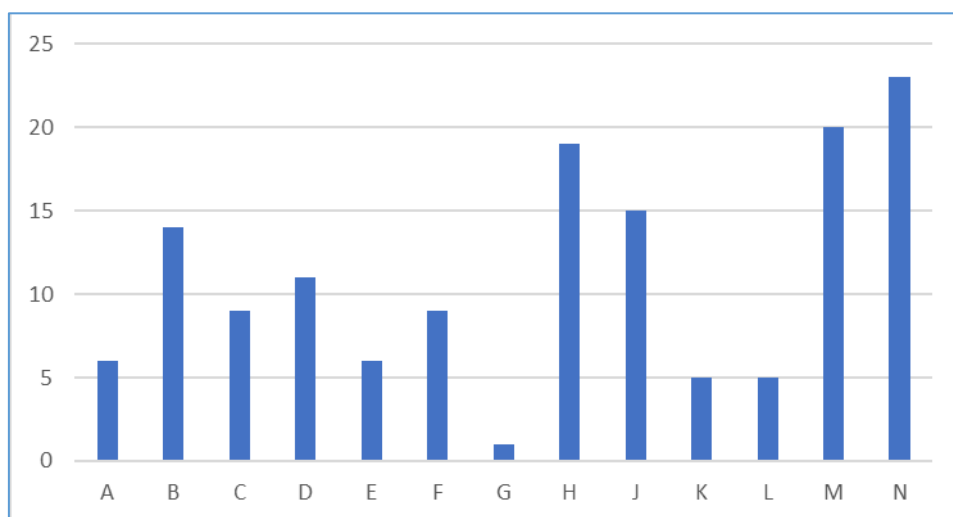


Figure 5-2: Questionnaire output: selected factors

5.5 Next steps

The objective of the questionnaire was to reach consensus about a short list of the most relevant factors and to identify suitable interviewees to take forward to the interviews. The five most relevant factors, as described above, were clearly identified and taken forward to form the basis of the interviews.

Several suitable individuals were identified as prospective interviewees. While most of these did subsequently take part in interviews, unfortunately two (1E-08 and 0E-22) were not available.

5.6 Chapter summary

This chapter has described and justified the approach to collecting and reviewing data from the questionnaire. It has contextualised the results received, including comments and additional factors, and identified the five factors considered most relevant by respondents, which are taken forward to the interviews. It has built on work of the Literature Review in support of answering RQ2: “What are the main factors relevant to the interplay between the deterrer and deterree?”

Where appropriate, the data outlined in this chapter is discussed and critically reviewed in the Discussion of Findings chapter.

6 Group Workshop: Data Collection, Review and Results

6.1 Chapter overview

This chapter describes the group workshop which offered an additional research opportunity to answer the questions:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

Although the interviews logically followed directly from, and depended upon, the questionnaire, in practice the workshop session (which was independent of the questionnaire and interviews) was the next activity conducted, and so is included in this chapter to follow chronological order.

The chapter outlines the structure of the workshop in three parts together with the data collected from each part. The first part was a group exercise built on the same scenario used in the questionnaire, but from the perspective of planning a course of action. This was followed by an individual reflection to ensure the views of those less prominent in the groups were fed into the research, in terms of their own thoughts and any disagreements with the group consensus. The final part of the workshop was a group discussion, beginning with each group introducing their proposed course of action followed by a short free-form whole group discussion, from which key points were noted.

6.2 Approach to data collection

The workshop was an additional research opportunity which presented itself during the research. It was held with course members of the Cyber Warfare in Military Operations module of the Cranfield University Cyberspace Operations Masters course on 19 October 2023, and immediately followed a lecture given by the researcher on Deterrence in Cyberspace which leant heavily on the content

of the Literature Review. Eleven students were present, and all consented to take part in the workshop, although it was made clear that this was optional.

The workshop took place following the questionnaire but before the interviews. Rather than use it as an activity aligned with the interviews, it was decided to take it as an opportunity to explore the thoughts of the military students about planning and cyber operations through a simulation, thus producing additional qualitative data. It therefore added an additional concurrent qualitative element to the sequential explanatory research design described in the Research Methodology in Chapter 4.

The workshop consisted of three parts: a group activity (where students were split into two groups), an individual activity, and a group discussion with the whole class. The group activity used a scenario where cyberspace had been suggested as a route for deterrence, and the students were asked to work in groups to make recommendations. After this, the students were asked to give a personal reflection on the exercise and their group's response. The group discussion then gave an opportunity to discuss further points relevant to planning. The workshop materials are presented at Appendix C and the workshop output at Appendix G.

6.3 Data collection

The output of the workshop was further qualitative data about options and the factors considered. Unlike the questionnaire and subsequent interviews, no factors were offered for consideration, meaning that participants were free to explore whatever they felt relevant. Since the workshop followed a lecture about deterrence in cyberspace which had stressed the cultural and cognitive aspects associated with deterrence, it would have seemed likely that these would be prominent in the participants' thinking. Interestingly, however, although perhaps unsurprisingly since they would have all received some training in military planning, the general approach was strongly aligned with conventional planning.

6.3.1 Scenario

The scenario used in the questionnaire was presented, with the students acting as advisers, as for the questionnaire. The groups were asked to list the courses

of action they had considered, and to indicate their selected course of action, together with the possible impacts considered and how they would assess those. They were then asked what intelligence reports they would find useful to complete this activity. Approximately 20 minutes was allowed for the group activity, which was conducted with the two groups in separate rooms. At the end of the allotted time the completed group activity forms were collected.

One group considered five courses of action: first strike (in cyberspace), setting up a honey trap, faking a team with a 'super exploit', demonstration/exercise and 'noisily' warning their own population of the impending attack. The selected course of action was the demonstration/exercise using conferences and videos to target messages to the leadership of the other state in order to deter the attack, alongside a publicised exercise along the lines of Cyber Warrior (which is a large multi-national cyber exercise run every couple of years). The group recognised that this could result in the possible loss or compromise of an intelligence asset (and that they may not know if that were the case). While an excellent course of action in that conference speeches could quickly be used to highlight capability, as when the then Secretary of State for Defence spoke of action against Daesh (Fallon, 2016), exercises are complex events which take many months to organise and so would only be useful if an exercise was already planned. The 2023 Cyber Warrior exercise was a clear precedent here, and we discussed afterwards the media coverage of that exercise, which was in many ways akin to the Red Square May Day parades by the Soviet Union during the Cold War in terms of demonstrating capability.

The second group considered three courses of action: do nothing, offensive cyber operations and defensive cyber operations, and selected the do nothing option. They rated each course of action against a traditional military assessment of availability, simplicity, surprise, cost/resource and time using a 0-5 scale. While their courses of action were all rooted in cyberspace this traditional approach was clearly within their comfort zone from military planning training.

Both groups focused on the impact at state level rather than the wider potential impacts on citizens of either state. While the first group considered a 'noisy'

course of action telling their own population to expect an attack and messaging that the state would respond at a time and place of its choosing, in their assessment of impact they did not consider the possible concern or panic this might cause to their citizens, or the potential for reputational damage from media or pressure groups (and possibly also allies) asking why the system was vulnerable and why they could not prevent the attack. While the difficulty of securing systems against sophisticated attackers and preventing cyber attacks is well understood in cyber security circles, this may not be the case more generally.

While the second group listed a number of technical questions they would like to have answered by intelligence reports, as well as information about adversary intent, their interest in citizens and the life of the state was restricted to search engine usage and social media exploitation, which would be useful for information operations. The first group, however, took a slightly wider view, listing pattern of life and cognitive reports to tailor their message as well as assessments of messaging and cyber locations. Both groups' lists clearly acknowledged the features of the cyber domain (Great Britain. Ministry of Defence, 2022, p7), although in different ways, although only the first addressed the impact of cyber on public life.

6.3.2 Individual reflection

The individual activity was introduced as an opportunity for them to record their own thinking around the course of action. They were asked to state whether they agreed with the consensus reached by their group and their reasons for this, and if they did not agree then what had been their preferred course of action and why. They were also asked about the impacts and assessments that they personally considered, and finally whether there were any points in the lecture that caused them to consider points which they might not otherwise have done. The whole group took the exercise very seriously and the room was in silence until all had completed their sheet and handed it in.

The individual responses were sought in order to allow voices and thinking which were less prominent in the group work to be heard. Most agreed with their group's proposed course of action and offered impacts and assessments which included

credibility, misinterpretation and compromise of assets. One of the second group noted the incompleteness of the information provided in terms of enemy capability and the vulnerability, and wondered whether defensive cyber operations might have been a better response given more detail (participant G-2g). Two participants disagreed with their group's decision. One of the first group (which proposed a demonstration and exercise) noted that they "wanted to prevent the attack without doubt" but thought that the group had selected "a more passive COA"⁶. This participant would have preferred to attack the adversary infrastructure to demonstrate capability and prevent the threatened attack: "Whilst it risks escalation, I think it prevents (hopefully) future attacks by demonstrating capability and increases reputation with local population" (participant G-1f).

The other disagreement was from a member of the second group, who felt their "Scoring criteria was flawed. Purpose-built criteria would need to be designed and applied" (participant G-2l). Instead, G-2l's preferred course of action was defensive cyber operations, amplified with human intelligence and cyber awareness to minimise social engineering. This participant's acknowledgment of the need for purpose-built criteria acknowledges the difference of action in the cyber domain, which the whole group addressed further in the subsequent discussion.

6.3.3 Group discussion

Following the individual activity, each group gave a brief summary of their proposed course of action with their considerations and rationale for selecting it. This then led into a whole group discussion, from which key points were noted on a flip chart. Again, the discussion was thoughtful and challenging.

On the scenario itself, some general observations were offered: one participant noted that their group had gone quickly into technical options rather than

⁶ COA is a common military abbreviation for course of action.

exploring more broadly first, while another highlighted that before conducting any offensive operation an exercise would be carried out as an indicator.

Moving to the general discussion, clear communication was briefly touched on in terms of whether deterrence could only be achieved if the other party knew they were being deterred, or whether they could be deterred even if they were not listening, or indeed whether the deterrer's actions might be viewed as escalatory and inflammatory. This moved to a short discussion on aggression. One participant felt that deterrence required some level of aggression, as no state has deterred "by staying in the corner and being quiet", but another challenged this. The question was felt to turn on the meaning of aggression: was it seen as exchanging like for like? All types of activity could be seen as a form of aggression, and decisions made could reflect this. While valid questions and comments, these are not unique to cyberspace and again possibly reflected the participants' military background alongside their roles in cyber. Similarly, the description offered by one participant of cyber as the infinite game, where one attacks and the other respawns and comes back, applies equally to other operational domains, and was reminiscent of Lindsay and Gartzke's (2022) discussion of a bargaining model in operational domains. As the group noted, although cyber activity will keep bouncing between actors, it was important to focus on the end state desired - again this situation is not unique to cyberspace, although it is highly relevant because of the speed and potential spread of cyber attacks.

Visibility of capability was another topic discussed. Having a visible deterrent is difficult in cyberspace, and some felt that this caused doing nothing, while always an option, to be higher up the priority scale than it might otherwise be. In the nuclear world, diplomatic effort over time led to the Strategic Arms Limitation Talks (SALT) which allowed inspection of stockpiles of both Cold War powers' nuclear weapons, which required a level of trust, and the group wondered how this might work in cyberspace. Showcasing zero-day vulnerabilities would not work, as these might expose vulnerabilities, and the lack of the existential threat associated with nuclear reduced the pressure to carry out inspections.

International military competitions such as Cyber Warrior offered opportunities to showcase skills, as well as for upskilling, and were overt approaches to support credibility. More covertly, one participant wondered whether in the future blockchain technology might offer a means of inspecting a capability without seeing what the capability was, as a record of a transaction without its details. A further interesting take on the issue of openness started from the UK's view of itself as a responsible cyber power, noting that in former times this would have implied accountability and record keeping, and international law could seek that capabilities are documented. Whether such an approach would be feasible would need serious consideration, but together with the other points mentioned above it does demonstrate how the discussion showed a clear understanding of the challenge of demonstrating credibility and some creative thinking to address it.

During the discussion the media promotion of exercises such as Cyber Warrior had been compared with the Soviet May Day parades in terms of their value in messaging to potential adversaries. The preceding lecture had begun with an image from a May Day parade which was used to introduce the importance to deterrence of messaging to demonstrate communication and credibility of strength. The observation about the similarity of exercises to these parades must be presumed to have been influenced by the lecture, and not treated as a finding of the research, as it is impossible to know whether it would have been made otherwise. It was, however, clear in the discussion during the lecture that the group immediately recognised the purpose of the parades in messaging, and that the leadership and citizens of potential adversaries had been a key audience.

The extent to which empathy with the other party was important was briefly discussed, together with red teaming and an understanding of theory of mind, the way psychological factors affect people. This chimed with two responses to the individual exercise on whether anything in the preceding lecture had caused them to consider something they might not otherwise have done. The two responses were "That cultural differences create a large potential area for misunderstanding and escalation" (participant G-1b) and "Deterrence actions from one viewpoint may be viewed as aggressive/escalatory actions and this may trigger an

escalatory spiral” (participant G-2h). It may be that highlighting cultural differences and the need to think about a situation from the other side’s perspective might increase the likelihood of greater consideration of their importance in preventing misunderstanding.

6.4 Reflection

Overall, the exercise part of the workshop was valuable in identifying that, even for those with a clear focus on cyberspace, planning a military course of action was seen in terms of traditional military activities (even when including cyber activities). While it would be wrong to generalise based on two groups in a single workshop, it does seem plausible that other groups of military personnel would approach it in a similar way. The discussion did not reveal any major insights, but did reflect the group’s understanding and thoughtfulness about cyberspace as a domain of operations even though their courses of action were more traditional.

It had been a deliberate choice not to prompt the workshop participants to think about the specific factors used in the questionnaire, and the results reflected that. If the opportunity had arisen for further workshops with similar groups, it would have been interesting to see if the choices and considerations were similar or not.

While delivering a lecture on deterrence in cyberspace immediately before the workshop was not ideal, and as noted above may have influenced some responses, this had been unavoidable in this instance. It did not, however, appear to have caused the bias in results which might have been expected, given that both groups took a very traditional military approach to planning their course of action.

6.5 Chapter summary

This chapter has described the structure of the group workshop, which aimed to gather information about the planning process to support the research questions. The exercise was taken seriously by the group and the workshop offered some useful insights about both the group courses of action and individual thoughts. An interesting finding was that even for a group of students on a course with a clear focus on cyberspace as an operational domain (particularly in the module

being studied that week), and despite having had a lecture immediately beforehand which had highlighted the importance of cognitive factors, military planning was seen very much in the same way as in the kinetic domains. This cannot be generalised on the strength of this single workshop, but adds an interesting point to take forward. The data outlined in this chapter is discussed and critically reviewed alongside the interview data in the Discussion chapter.

The group workshop contributed to answering RQ3 (How can these factors be included in deterrence planning for deterrence in cyberspace?) by demonstrating that, for the participants in this workshop at least, a very clear way of driving the inclusion of the factors was needed. This reinforces the need for a framework to support their inclusion as outlined in Chapter 8, Developing a Framework.

7 Interviews: Data Collection, Review and Results

7.1 Chapter overview

This chapter addresses the approach to collecting, codifying and reviewing data from the interviews, and then articulates that data within the coded themes. This continues the activity begun in the Literature Review and continued in the Questionnaire and Workshop in support of answering:

- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

The chapter begins by outlining the data collection approach used for the interviews, leading on from the overall approach to research data set out in the Research Methodology in Chapter 4. It then describes how the interview data was coded and reviewed.

Following this, the interview data itself is presented. This begins with a section on the definition of deterrence in cyberspace, followed by a section on each of the five factors rated most relevant in the questionnaire. These are followed by a section on culture and sections on further topics covered by interviewees.

7.2 Approach to data collection

The objective of the interviews was to explore and understand the rationale behind respondents' answers to the questionnaire, in order to gain an insight into the thought processes relevant to the selection of relevant factors so that these could be taken forward into further work. The interviews therefore built on the questionnaire outputs, exploring the selected factors with a range of experts drawn from those who had responded to the questionnaire. While the questionnaire had focused on the 'what', i.e. identifying the relevant factors, the interviews addressed the 'why' regarding the relevance of those factors.

The interviews therefore sought to understand the interviewees' point of view, as articulated in their questionnaire response, with an open discussion based

around specific questions. Semi-structured interviews were determined as the best route for in-depth reviews of expert reasoning and viewpoint, in line with Kvale and Brinkmann's (2009, p3) definition of an interview as "a conversation that has a structure and a purpose". The benefit of a semi-structured interview was that a fixed set of questions could be asked, thus obtaining comparable data from each interviewee, while also allowing for variation on specific areas to be added to reflect questionnaire responses. These allowed specific comments or variance from the five factors found most relevant in the questionnaire responses as a whole to be explored.

The basic interview script is at Appendix B. Interviewees were first asked for their definition of deterrence in cyberspace, and then each of the five most relevant factors from the questionnaire were explored in turn to understand why the interviewee thought the factors were (or were not) relevant, and how each could be measured. Where there had been a notable difference in their questionnaire responses from the 'top 5' this was also explored to give an insight into their thinking.

As noted in the Research Methodology chapter, the range of experts for interview was selected from questionnaire respondents using a purposive approach. Interviewees were selected to give both depth and range of expertise, and included some who were recognised as strong practitioners in their field. The question of how many is enough to give saturation, where further interviews will not yield additional insight, leads Guest et al. (2006) to conclude that twelve interviewees was sufficient for saturation in a study with a relatively homogeneous population and fairly narrow objectives addressed in structured approach where similar questions were asked of all participants, which was the case with this research. This also aligns with Kvale and Brinkmann (2009, p113) who note that 15 +/- 10 interviews is common.

Kvale and Brinkmann (2009) further stress the importance of quality over quantity. For them, effort should be focused on preparation and analysis, with only "as many subjects as necessary" being interviewed for the researcher to interpret the knowledge gained (Kvale and Brinkmann, 2009, p48). This approach

was followed, with trialling of the interview approach and careful selection of the sample. The initial sample of ten questionnaire respondents was then supplemented with two further interviewees (who had not completed the questionnaire) to ensure coverage of their specific expertise (one on military planning outside of cyber activity, the other on cultural issues). This resulted in a total of twelve interviewees, with expertise as shown in Figure 7-1. As Figure 7-1 shows multiple of areas of expertise as claimed, Figure 7-2 identifies how many areas were claimed by interviewees, and indicates that most claimed two areas, with one claiming four. These claims are not unrealistic (and are substantiated by their career paths); if anything, some have underclaimed their expertise.

Following each interview the record of the interview was written up and returned to the interviewee for their approval before it was coded.

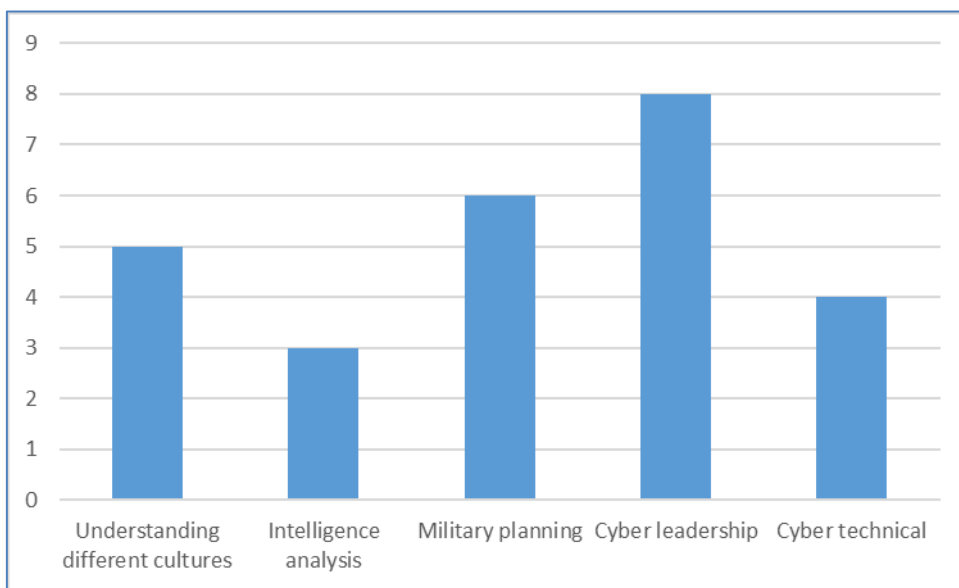


Figure 7-1: Expertise of interviewees (multiple responses allowed)

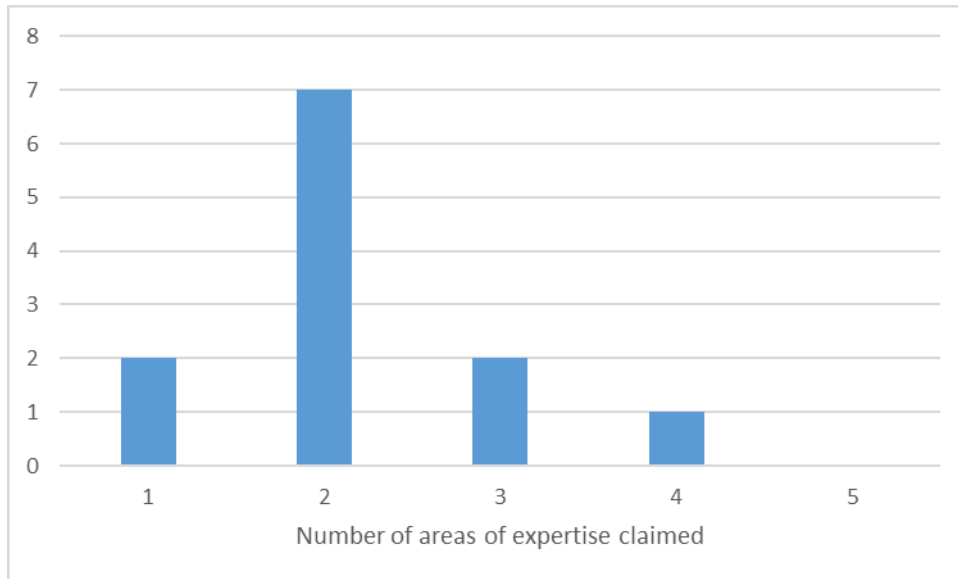


Figure 7-2: Number of areas of expertise claimed by interviewees

7.3 Codification and review

Thematic analysis was used because of its wide applicability and suitability for analysing qualitative data, enabling data from different transcripts to be integrated and thematic descriptions produced (Saunders et al., 2019, p651). In line with the critical realist ontology a retroductive approach had been used, as noted in the Research Methodology chapter, using the literature review to identify the initial factors for the questionnaire, which were then refined to the “top five” factors considered in the interviews. These same elements were used as the basis for the initial coding scheme, which addressed the top five factors and other factors derived from the literature review such as stakeholders, measurement and culture. Some codes, such as ML (Military) naturally subdivided into sub-codes for DIME, but this did not apply to all. While the initial coding scheme thus used up to two layers of code, it was acknowledged that this might need to break down to a third layer, but in the event, this was not needed. The initial codes are shown in Figure 7-3.

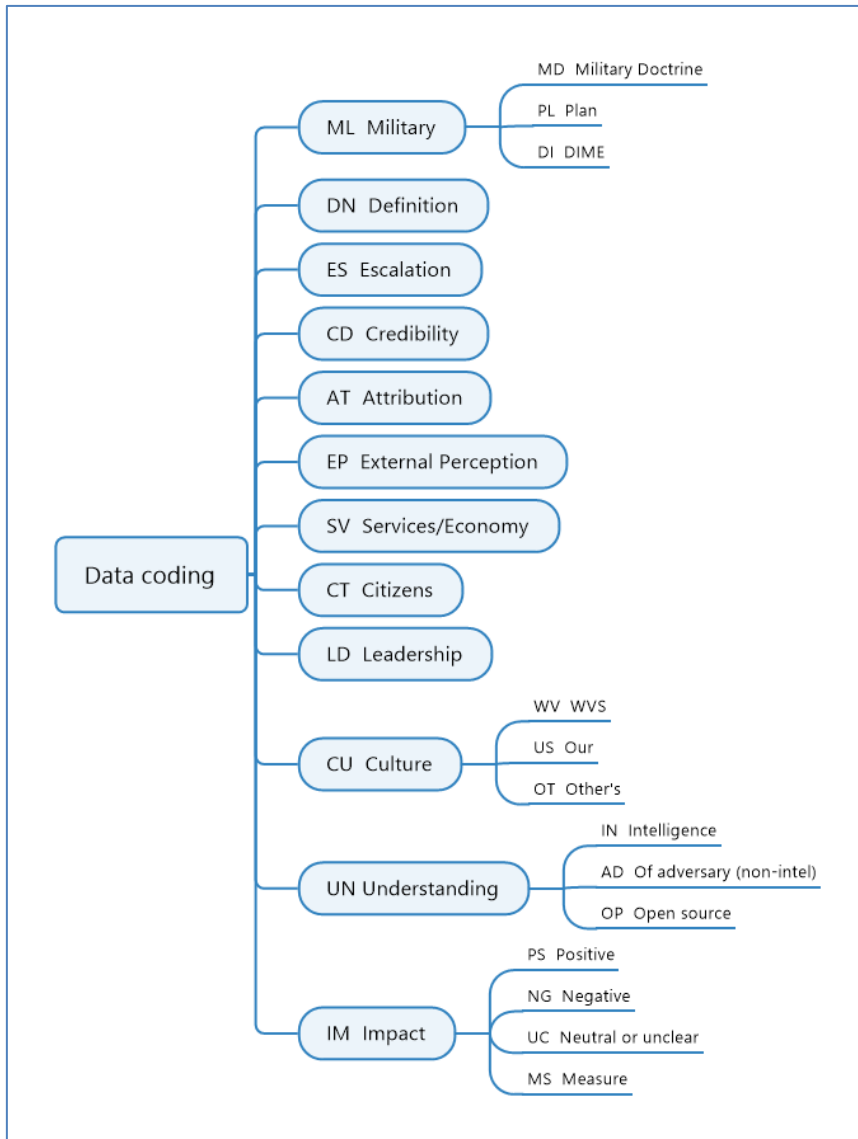


Figure 7-3: Initial coding scheme

As the interview scripts were reviewed the coding was modified to add additional codes, as indicated by Figure 7-4, which shows the amended coding after the first interview (with interviewee 07-05).

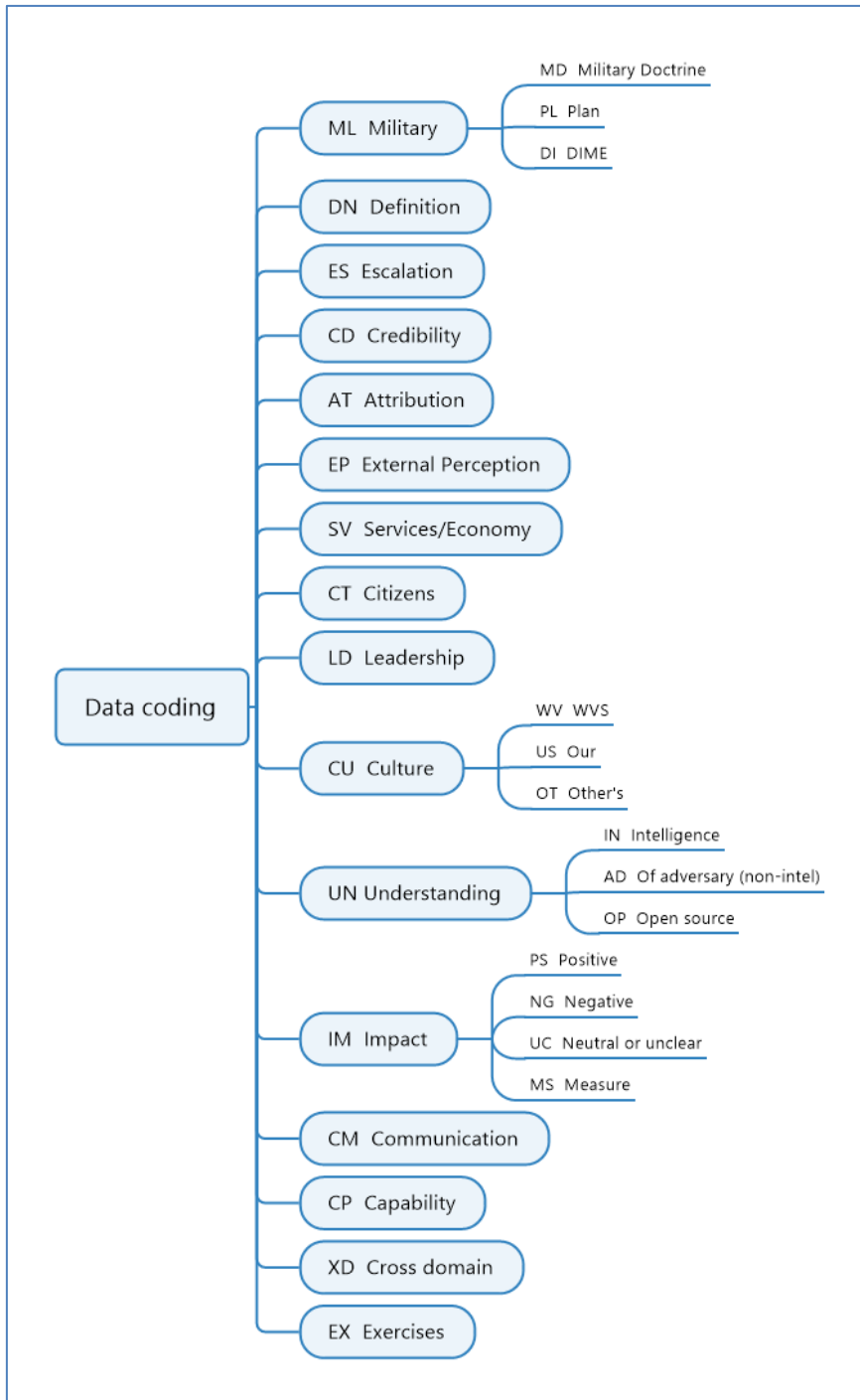


Figure 7-4: Amended coding scheme after first interview

Finally, when all the interviews had been completed, the coding was fully reviewed to ensure that it was consistent across all data and to draw out the themes. While the themes anticipated were largely those identified in the initial top layer codes, there was some redistribution of sub-codes and some reassignment of layers, for example SV (Services/Economy), CT (Citizens) and

LD (Leadership) all became sub-codes under a new code ST (Other State); XD (Cross domain) was demoted to sit under ML (Military); and EX (Exercises) which was only applied to 07-05 was removed after the data was reassigned. The final coding scheme is shown at Figure 7-5.

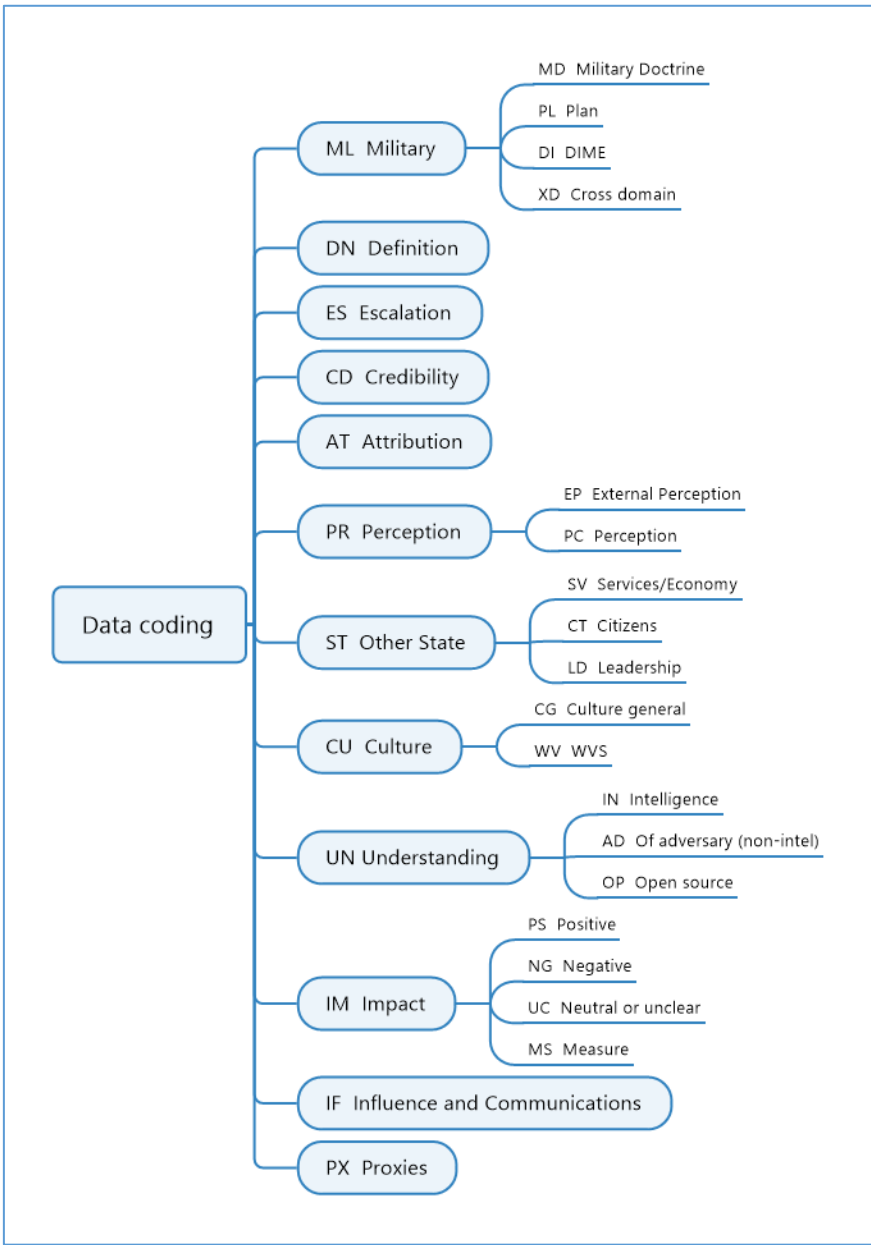


Figure 7-5: Final coding scheme

The coding record was entered on a spreadsheet for convenience in enabling data to be pulled together for ongoing review and subsequent analysis. The rows

were used for the codes, and columns for the interviewees: a screenshot of part of this coding spreadsheet is shown at Figure 7-6.

	A	B	C	D	E	F	G	H
1		top level 1		sub level 2	07-05	03-06	0F-07	09-09
2	ML	Military						
3			MD	Military Doctrine	201; 205-6; 210-1	41-3	21-3; 91-102	
4			PL	Plan		93-99; 140-5; 279-281; 328; 331-5; 343-351	53-62; 138-152; 271-9	220-230; 609-615
5			DI	DIME			335-341	
6			XD	Cross domain	99-101; 259-260			
7	DN	Definition			7-8; 76	7-16	7-12; 23-39; 118-123; 160-	9-16; 21-37
8	ES	Escalation			16; 18-21; 23-24	27-39; 298-303	68-71; 75-87; 108-114	45-101; 122-137; 476-9
9	CD	Credibility			76; 78-81; 85-6	17-21; 44-53; 106-8; 202-6	162-176; 187-201	239-279; 305-328; 332-347
10	AT	Attribution			26; 45-6; 115-6; 118-120; 125; 127; 131-2	154-8; 163-171; 198-200	234-246; 251-5; 259	238-9; 356-377; 385-407
11	PR	Perception						
12			EP	External Perception	156-7	88-90; 214-224	287-298	415-437; 441-6
13			PC	Perception			64-7; 123-8; 205-7; 210-2; 218-220	
14	ST	Other State						
15			SV	Services/Economy	198-9; 210-11	289-294; 329-331	306-314; 318-326	476-504; 508-17
16			CT	Citizens	248;			572-9
17			LD	Leadership	239-240; 242			553-568; 588-594
18	CU	Culture						
19			CG	Culture general	36; 280-1; 283; 295	373-380	348-355; 359-368	622-660
20			WV	WVS	291-3	385-391	373-399	665-672; 679-698
21	UN	Understanding						
22			IN	Intelligence	57-8; 68; 90-1; 147-8; 264; 301-2	273; 322; 396-8; 402-3	405-416;	704-732
23			AD	Of adversary (non-intel)	30-1; 33-4; 142-3; 304	80-5; 133-6; 320-1; 322-4; 413-5	224-5	

Figure 7-6: Screenshot showing part of final coding spreadsheet

7.4 Presenting the interview data

The presentation of the interview data begins by following the format of the interview script, with an initial discussion about the definition of deterrence in cyberspace, followed by a section on each of the five factors rated most relevant in the questionnaire, using summarised labels of escalation, credibility, attribution, perception of external states and effect on the other state. The presentation of the data ends with a section on culture. After these, further relevant topics identified through the coding process are addressed.

7.5 Defining deterrence in cyberspace

The opening question in the interviews (how would you define deterrence in cyberspace?) was intended mainly to get the conversation flowing, but some interviewees took the opportunity to make a wider point about the context of

cyberspace in relation to deterrence. 0F-07 was the most explicit, unpicking the question to explore the difference between deterrence *of* cyber activities and deterrence *using* cyber activities. For 0F-07, using offensive cyber activities “to deliver or complement wider influence activities” would be part of a cross-domain and multi-lever approach, recognising not only the five military domains of operation but also the broader aspects of DIME. This echoed the wider view articulated by some in the literature review (Nye, 2017; Fischerkeller, 2017; Burton, 2018), but, since “learning from conflicts, Military rarely resolves issues in isolation,” (0F-07) it encompassed the breadth of factors that none of those authors had included in full.

A similar point was made by 16-32, noting that cyberspace “could be seen as part of an overall deterrence posture,” and 12-28, who factored in a multi-domain operations approach because of the interactions needed between domains in operations. In 12-28’s opinion, “you can no longer ... simply regard a particular sphere of operations, the traditional land, air, sea, in isolation” as it will have interactions and effects in other domains, and 12-28 considered this to be equally true of cyberspace.

That said, how 02-25, based on their experience, thought about capability in cyberspace is different, because “you’re not necessarily thinking about what the adversary is up to, you’re thinking about how you’ll get round that general layer of security that’s in cyberspace.” While the opacity of cyberspace was recognised by others (e.g. 18-36), 02-25 went further, in terms of the role of cyberspace in deterrence:

“Nothing is hidden in this modern world ... you can see ships, you can see investments, open government talks about what it’s spending on its defensive capabilities and otherwise. Although we can talk about cyber, it’s really hard to get, especially for policymakers and so to get a really tangible grip on what capabilities might be able to do, what’s being held at risk or not, and what could be threatened, or is being threatened, and even the damage feels quite intangible and long term, which is hard. ... I have seen policymakers slightly nervous about signing off cyber plans, because

they have seen other nations do noisy, attributed other attacks and so that causes them worry. And in my book, that means they are deterred.”

(02-25)

But this has a downside, as 02-25 recognised that this may mean others are deterring the UK because of their actions, but the UK may not be acting to deter them.

Interviewees’ responses about each of the five factors considered most relevant in the questionnaire responses (escalation, credibility, attribution, perception of external states, and the services and economy of the other state) are described below, followed by a section on culture. These reflect not only the topics discussed under those headings in the interviews, but also those identified more generally from the coding of responses. Impact and understanding are then covered, and finally a short section addressing other relevant points.

7.6 Escalation

This section addresses questionnaire factor N: the potential for escalation of the situation.

Escalation was a concern for most interviewees even though some noted that there was to date no evidence that it had occurred (07-05, 09-09, 02-25). While there was “a huge amount of tit for tat cyber activity taking place” (09-09) the knowledge that many are capable of conducting offensive cyber operations does not seem to deter, possibly because, in 09-09’s view, cyberspace was “kind of borne out from traditional views of espionage rather than conflict” and espionage is an accepted form of behaviour between states. While 09-09 recognised that there were signs of a potential move towards imposing sanctions following cyber activity, “at the moment there is no backlash” leading to “plenty of scope for my state or for other states to escalate and retaliate in the cyber domain itself in order to establish some kind of norms of what’s accepted, what’s not accepted” (09-09).

The literature review suggested that even authors who promote a wider view of response to aggression that recognises potential interplay between conventional

kinetic activity and cyber activity, such as Nye (2017), tend to focus on the narrow view of cyber-on-cyber, in their examples. 02-25 reported seeing evidence of “a very cyber-on-cyber lens”, although they noted that this was beginning to change to include diplomatic measures or sanctions, but not military action. Their experience was that escalation beyond cyber was “always part of the discussion, but it always feels a bit strange to me that it is so prominent” (02-25).

A rather different stance was taken by 06-23. They initially saw escalation to mean moving beyond offensive cyber activity into a related kinetic activity that drew in different military functions, but then contrasted this with escalation in terms of who was being impacted. This might involve an offensive cyber action on critical infrastructure affecting a small group of citizens escalating to affect a larger group, or broadening into related functions within that critical infrastructure. Although this point was not made by any other interviewee and was not addressed in the literature, it offers a wider perspective on escalation which could apply also to kinetic activity. The potential for escalation, in that broader sense, could offer a means of influencing a potential adversary, which is obviously the purpose of deterrence.

Escalation could, however, cause issues. One party may cross a threshold which causes the other to respond in a way that is either unanticipated or (in the eyes of the first party) is disproportionate (07-05). Conversely, 03-06 suggested a gradual escalation, where a deterrence activity may not be strong enough to act as a deterrence in its own right, leading them to have to increase their deterrence activity. This would need an agile and flexible approach to project deterrence at an appropriate level to the other party, depending on their capability (such as bedroom script kiddies or high end Advanced Persistent Threats) (03-06). There was also a risk of misinterpretation and subsequent escalation, which 0F-07 argued was “much more nuanced within cyberspace than many other mediums” and could have unpredicted collateral consequences (0F-07). This view was shared by 18-36 who spoke of the “opacity of cyber” and “higher scope for misunderstanding” in cyberspace.

Asymmetrical response was a concern for 09-09, where sanctions might be imposed in response to a substantial cyber attack, or a pre-conflict strike activity triggered a cyber response, as 09-09 asserted was being seen more often, with cyber activity moving away from espionage and getting closer to a red line that might trigger NATO Article 5⁷. 02-25 agreed while also noting that asymmetry causes Western powers to struggle with operationalising cyber activity, because they either equate it too much with military activity, and so want to wrap the processes they have developed for the military instrument around it, or they worry about out-escalation. Together with concerns about the rule of law and norms, this struggle to operationalise had on occasions got in the way of planning. In order to be effective, escalation means signalling to the adversary – “showing some leg” as 02-25 and several others phrased it – and there was concern that the UK preference for offensive cyber to be covert and contained “completely I think undermines deterrence” (02-25).

Cyber activities often lay below the threshold of an armed attack, but such sub-threshold activity could still be serious. 12-38 referred to perceptions that cyber activities conducted by states would lie below the threshold because they might not lead to harm or direct deaths, “But obviously secondary kind of taking down critical infrastructure, that has the potential to lead to deaths anyway.” (12-38). They concluded that escalation in cyberspace was an unknown area compared to conventional kinetic means, as it would depend on the types of cyber activities conducted.

This leads to the question of whether escalation is desirable, to which the answer from interviewees was ‘it depends.’ Understanding the threshold to which the state would be willing to go was important to 03-06, while 06-23 focused on the consequences of escalation, both known and perceived, which could also be unknown or unintended. They suspected any escalation would be a graduated response based on the adversary’s actions, while noting that while cyber activity

⁷ “Article 5 provides that if a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked.” (NATO, 2023)

might be valuable for influence purposes it would be a “sideshow” compared with any kinetic activity taking place. That said, where the due diligence and consideration of consequences was in place, 06-23 thought escalation through offensive cyber operations could be seen as a positive, where it targeted specific audiences and layers of cyberspace, as it could avoid kinetic activity.

The potential value of escalation by a state to induce an adversary into conflict was noted by 16-32, allowing the first state to elicit the conflict without being blamed for it. While that might suit the first state’s narrative, 16-32 not only recognised the risk of eliciting something that one could not control but also the negative reaction that would result from such duplicity by a Western state.

Whether escalation was a positive or a negative was a “very interesting question” for 02-25, who had given this much thought in the past but not come to a conclusion. Their discussions with academics in the past about the dominant position the West had held since the Second World War had led them to the conclusion that the UK had not needed to build, and therefore had not built, “the mechanisms, the muscle memory, the policy, the kind of experience of finding alternative ways to deal with situations” (02-25). 14-26 also took a viewpoint of Western dialogue, which they thought “always assumes that escalation is bad,” although they felt that escalation was sometimes desirable and, indeed, necessary, such as to send a clear signal. However, they recognised that there was always a risk that an adversary would respond in a way one had not anticipated or really did not want. Similarly acknowledging the risk of unintended escalation, 0F-07 saw escalation as not necessarily a bad thing, and for them the ultimate measure was whether it helps to achieve one’s operational strategic ends, a point echoed by 04-37 in terms of cost-benefit analysis in relation to the consequences and objectives.

The responses to the questionnaire had indicated that the potential for escalation of the situation was a key relevant factor for deterrence, and the engagement with all interviewees clearly reinforced its importance to deterrence in cyberspace. Escalation may or may not be desirable depending on the circumstances, but the

type of escalation and the potential for misinterpretation of activities are relevant to planning.

7.7 Credibility

This section addresses questionnaire factor M: the credibility of your state's proposed action to the other state.

Credibility, like escalation, was rated highly for relevance by questionnaire respondents, and was one of the eight elements of deterrence identified by Goodman (2010). Most interviewees described it as an essential component of deterrence, but some made the point that credibility depended upon the adversary's view. As one observed, "you can have all the capability in the world, but if that isn't perceived by the adversary as credible, then they're not going to be deterred by that" (12-38). 04-37 made a similar point that one had at least to make them think it was credible, while in response to a question about the types of intelligence report they would like, another was clear that these would be "Very much credibility ... how are my cyber operations, how are my allies' cyber operations, seen by the other country?" (16-32).

Perception of capability, however, is subject to potential miscalculation. While 02-25 had seen the worry caused to policymakers by others' "noisy" attacks (noisy in that no attempt has been made to make them covert or discreet), and viewed this as deterring them, 16-32 was concerned by the "real risk" of miscalculation of capability, whether by over- or under-assessing it, and responding in an inappropriate manner.

Measurement of credibility was harder. 06-23 could not see how it could be measured, and 18-36 recognised that it was rarely done well, as "when we say how credibly the adversary sees us, what we mean is how credible do we think we would be [to them]" (18-36). They went on to question to whom specifically one might be credible, as in some states this, and its impact, might vary, with the President, the General Staffs and other key leaders each having different views (18-36). In contrast, 04-37 suggested that getting the adversary view might not be so important: "if you believe it's credible, and the SMEs think it's credible and

would work, then I can't see why any adversary wouldn't think it's credible as well" (04-37)⁸.

Published accounts of and pronouncements concerning capability, in terms of both defensive and offensive cyber capabilities, were identified as particularly useful by some. 07-05 considered that such statements were important and that if deterrence were effective that was because it was based upon such statements. 16-32 shared that view, highlighting the publication about the UK National Cyber Force (Great Britain. National Cyber Force, 2023) and comparing that to the effect of the Red Square May Day parades in the former Soviet Union. They noted that media coverage of the Cyber Warrior exercise, while carefully stage managed, was similarly valuable for getting the message out about the UK's credible capability in cyber operations, and offered a means of putting something in the public domain about a generally secretive capability.

Broader capabilities were also relevant for credibility. As well as trials and demonstrations, "being effective in other conflicts" contributes to credibility (0F-07). They also suggested that credibility could be comparative, where one simply needed to be more credible than the next person, although this would only apply in low-level cyber crime activity rather than state on state hostility. Making one's attack surface less attractive by having good defences and hardening networks also acts as a deterrent to others (03-06). Another interviewee seemed to take a different view, citing work by Daryl Press which indicated that track record might not be relevant, but then summed up by observing that "credibility is really hard, takes years to develop or achieve and ... a few seconds to lose it" (14-26).

Overplaying impact to try to gain credibility was seen as counterproductive by 09-09. They cited examples of an adversary misunderstanding the profile of a website they had brought down through a DDoS attack, and so claiming a major success although it was simply the website of a small town, and of other threat actors claiming responsibility for activities carried out by another party. Often the real-world impact of cyber operations did not seem high, and this raised the

⁸ SME: Subject Matter Expert

question from 09-09 about what cyber harm meant and how far cyber actors could have real-world effect.

14-26 linked credibility with attribution, as clear attribution leads to credibility. This could also extend to non-declared attribution: “it was quite clear who really benefits [from Stuxnet], and that raised their credibility” (06-23, who went on to agree that Stuxnet had been positive for the reputation of US Cyber Command, even though they had never claimed responsibility). In contrast, and despite their view noted above that published cyber capabilities were a key element in making deterrence effective, 07-05 questioned whether talking about our OC⁹ capability did deter: “the empirical record does not support this. US CyberCom has not shown a decrease in activity against the US” (07-05).

In summary, credibility depends upon how others perceive one’s capability. This perception may come from experience, including indirectly by third parties’ attribution, or from communications, including published accounts and media reporting.

7.8 Attribution

This section addresses questionnaire factor B: the other state’s willingness to attribute any actions your state might take in cyberspace to your state’.

While attribution is, as the previous point shows, strongly linked with credibility, it was also considered by questionnaire respondents as a relevant factor in its own right. Some interviewees (07-05, 09-09, 16-32) observed that attribution was more common than previously, and was sometimes accompanied by diplomatic response. Some states were brazen and did not care about being attributed, as noted by 07-05 and 03-06. 09-09 and 16-32 went further, in terms of the default positions of certain states, either to simply pretend that it was not them, or to blame everything on hostile Western states who are just out to get them. This applied both for their reaction to activities against them and to attributions of them (16-32). 09-09 added that some non-Western states used their own operating

⁹ Offensive Cyber.

systems and technology or bootleg pirated copies of Microsoft Windows, and therefore their systems might be so unreliable that they did not recognise an attack, or if they did suspect it they would default to blaming the West, and this was why 09-09 had not identified attribution as one of the most relevant factors.

While attribution required evidence (07-05), it could be hard for the victim of an activity to gather firm evidence, and “almost impossible” for the attributed state to demonstrate that it was not them (03-06, who had not marked attribution as one of the most relevant factors in the questionnaire). Gathering solid technical evidence may, however, not be necessary for the victim. 02-25 suspected that the West “overegged the technical attribution” as it was likely to be clear from geopolitical context. This was echoed by 0F-07: “They don’t need to attribute it to us, they need to correlate it with the outcome we’re seeking.” 0F-07 also contrasted private and public attribution: while it would be important for the victim to know the source or see it in the context of broader influence, calling it out publicly might help their aims and embarrass the attributed state, or could support the credibility of the attributed state to the victim and to other states (0F-07). 18-36 made the same observation about attribution supporting credibility, describing it as “free advertising.”

Context mattered, both in terms of the geopolitical context as noted above, and in what followed the attribution. 14-26 wondered whether the “whole international community” needed confidence in the attribution, or “just the US or a single adversary”, and whether anything actually happened as a result, or not.

This leads to the question of whether attribution was desirable or not. The answer was, unsurprisingly, that it depended on the context. As well as the views of 06-23 and 18-36 cited above, there was a clear acknowledgement from most that attribution was desirable in some, but not all, situations, and that needed to be factored into planning (explicitly stated by 03-06 and 02-25).

On the negative side, attribution could prevent “maintaining a presence on a target network” (06-23). It could be damaging if unintended consequences had led to an impact on civilians, particularly so for states such as the UK who “played by the rules” as 16-32 and 04-37 noted. The “touchiness” about attribution

mentioned by 02-25 was reflected by others' beliefs that the UK would not wish to be attributed for its actions: "I guess in general in cyber we don't want to be attributed" (14-26) and "the UK doesn't want to be attributed directly" (07-05).

For deterrence, however, several were definite that it would be important to do something to show capability and intent that the other side could attribute, at least privately (0F-07, 02-25, 13-26, 16-32, 12-38). This mattered from a messaging perspective as well as demonstrating credibility.

In summary, the main points concerned whether or not one would wish to be attributed, and whether attribution would be private or public. While deterrence would require at least private attribution, and was seen as desirable by some, others saw it as less so.

7.9 Perception of external states

This section addresses questionnaire factor J: how external stakeholders (the other state's allies or neutral states) perceive the other state.

Deterrence relies upon the deterree's perception of the deterrer's message, however that may be articulated through words or actions. Yet it is not only the perception of the deterree that may be relevant, but also that of their potential allies and of neutral states. These other states may be influenced in terms of whether or not to assist the deterree, and also more generally in how they perceive the deterrer's capabilities.

Almost all interviewees recognised the value of influencing external perception, even where they had not selected it as one of the most relevant in the questionnaire. 07-05 focused on how neutral or wavering states might be impacted by our actions and the influence that might have on their response, while some were more specific about trying to isolate the deterree by moving their potential allies away from them (0F-07, 09-09, 12-38). 03-06 highlighted the impact of undermining an external state's partner (as the deterree), particularly where that partner was the prime in the relationship. 09-09 went further, noting that for some states there were no allies, only those who were useful. This view was further developed by 12-38, who was keen to consider the deterree's

perception of their allies, including trade, economic and military dependencies in both directions, in order to create friction and influence the ally away from the deterree.

Seeking to bring neutral states over was suggested by 0F-07 and 14-26, although both recognised that keeping them neutral might be sufficient. Indeed, this was not specific to deterrence but a normal “broader military consideration” and “a key part of a joint operation and therefore relevant to deterrence” (0F-07).

While wanting external stakeholders to be “positive to your perspective” 16-32 noted the importance of balance: while it would not be good if they were negative towards one’s state, their being too positive could be seen by other stakeholders as being “a puppet.” Thus, the credibility of the external states, and how trusted they were, were important on the international stage, as was the standing of one’s own state in bodies such as the United Nations (16-32).

At a practical level, future economic prosperity was relevant: “You’ve got to work with these people, trade” (16-32). Another made a similar point about trade, citing how disinterested states in the Russia/Ukraine war had “leant into the grain issue because it was important to them” (18-36). They noted the need to balance military utility and neutral perceptions in target selection, and that activity in cyberspace was, by itself, unlikely to bring about major changes of viewpoint.

Focusing on military activity, 04-37 thought that other states would be “watching with interest” for their own future planning activities. 06-23 agreed and saw influence as “a long game” that was very important.

The only note of dissent came from 02-25, who had not rated it as one of their top factors in the questionnaire because “[one has] to build the line somewhere at the sort of risk you’re going to try and mitigate and worry about” and because they felt it was “very unlikely” that a third party would see what one was doing. Ironically, and despite this dismissal of external states in response to this question, 02-25 had elsewhere highlighted the importance of “showing some leg” to enhance wider credibility, and recognised that wider perception might be important in some contexts. In answering the particular question about external

stakeholders in the questionnaire they had felt that the directly engaged states were more important in planning.

Further points were made about perception more generally, including perceptions of a state being reinforced by one's view of their actions (16-32) and the difficulty of understanding and predicting how one's actions will be perceived. 0F-07 was clear that "getting in the mind of the other" and not seeing through one's own lens was vital but very difficult.

One final point about perception concerned the perceptions about one's own state by its allies and more generally, which would affect how its actions were viewed: "Are we regarded as a top tier table member? Are we regarded as something that sits in the corner of the room, on the cheap seats?" (12-28). Yet while the standing and partnerships of a state were important, they would not guarantee unconditional support if one were considered to have gone too far (16-32).

In summary, the perception of external states could be influenced to try to move allies of a potential or actual adversary away from them and to bring neutral states over. Both of these, however, were themselves dependent upon the standing of one's own state and of the other states to be influenced.

7.10 Effect on the other state

This section addresses questionnaire factor H: the impact on the services or economy of the other state.

While the interview question focused on the impact to the services or economy of the other state, the data from the interview was more wide ranging. This is reflected in the themes derived from the coding and the discussion below.

Impact to the services or economy of the other state was described as "a broad church" that could include "food security, energy security, physical security, education" as well as areas such as banking (06-23). While cyber activities were, in their view, unlikely to deliver sustained effect, disruption to areas such as banking ("block and stop transactions") would "have an enormous impact on daily

life” (06-23). While impact on the services or economy of the other state was included in the most relevant factors identified in the questionnaire, some interviewees had not selected it, whether through lack of impact (07-05, 06-23), because it was too narrow, excluding the wider aspects of influence on a state such as diplomacy (0F-07) or simply because it did not seem to be one of the top five, although it was still relevant (02-25, 16-32).

The “point at which cyber activity has an effect on the real world” was important to 09-09. They gave the example of the ransomware attack on the US Colonial Pipeline system, and noted how real-world impact would play into adversary decision making. 12-28 made the same point that cyber was “one of the metaphoric golf clubs in the bag” which could be selected to achieve disruption or influence, while 12-38 offered potential results of impacting the economy, which “could lead to them being able to do less militarily” and impact their relationships with the international community in terms of trade.

The future end state is a further consideration in planning. As well as considering the immediate impact to be achieved, 04-37 was concerned with the longer-term effect to be achieved, and whether one wanted the other party to be a fully functioning state afterwards.

The impact of cyber activity may be less severe than that of kinetic activity. 12-38 recognised the potential for “overt impact” on the state and on the daily business of its citizens but without leading to deaths. Impact may also be less enduring and cause less collateral damage: as noted by 14-26, who saw “cyber more as an irritant, and maybe as an enabler.” 06-23 made the same point about severity, contrasting kinetic destruction with cyber activity against SCADA¹⁰ facilities such as energy supply. The former would force long-term disruption and possibly require the population to move, whereas in the latter case, network administrators are likely to spot that something has happened and can more readily recover.

¹⁰ SCADA: Supervisory Control and Data Acquisition

Not all were so convinced about the need or potential for impact on services or economy. 07-05 asked “How do we really affect the economy of the other states?” and maintained that cyberspace in isolation could not achieve this. 0F-07 recognised the potential, noting that reversibility was one of the strengths of cyber as a domain of operations, but emphasised the desired outcome: “if our outcome is to focus their military elsewhere ... I don’t need to destroy their economy, I don’t need to impact their services” (0F-07). 16-32 echoed the point about the reversibility of cyber activity.

Several interviewees commented on the importance to the UK of being seen as a responsible cyber power. 03-06 referred to the moral and ethical issues about impacting a population as opposed to a more targeted effect. 07-05 asserted that impact on services or economy was “not an issue” because the UK would not target the economy and was clear that Offensive Cyber (OC) would only be used to support military operations and against organised crime. However, they acknowledged the possibility of causing worry or anxiety to citizens “if trying to get them to support a particular course of action” (07-05).

02-25 thought it “would have to be a very serious situation” for the UK to consider that sort of impact, and highlighted the approach routinely used of considering necessity, proportionality and justification (NPJ), which essentially address the question of whether the ends justify the means. A similar point about activities being within the law “because we play by the rules, unlike some of our opponents” was made by 12-28, and both 02-25 and 12-28 referred to the NCF’s publication (Great Britain. National Cyber Force, 2023) in support of the UK’s responsible approach.

16-32 agreed that while maintaining our status as a responsible power and staying true to the rules of war, in time of actual conflict it was necessary to achieve the ultimate aim. 18-36 was more specific, not wanting to disrupt the economy “in the opening months of a conflict, but when it is starting to become personal to the leadership, their options are fewer and their failures are being noticed” (18-36).

While impact on the other state's citizens caused some concern, the same did not apply to the state's leadership. 07-05, 09-09 and 18-36 had all included worry/anxiety of the leadership and citizens of the other state as one of their most relevant factors on the questionnaire, and were invited to comment on their choice. 07-05 was definite that "the point of deterrence is to give [the leadership] dilemmas." 09-09 noted that many potential adversaries were autocracies where the leadership's opinions held greater sway than in Western democracies, and even paranoia at a personal level could cause them to direct the activity of their cyber capabilities. They contrasted the collaborative approach in the UK and other democratic states, where advice is sought from civil servants and the military, with autocracies where "reaction can be a lot more irrational, more emotionally based" leading to "everybody jumps and does that" (09-09). 18-36 made a similar point about the highly personalised nature of some autocratic states, and the understood relationships and established norms for interaction between key figures ("elite bargains"). Within the autocracy this might include an expectation that the leader may direct military activity, while for a state considering action against it, target selection might take into account factors such as where the target is an industry owned by a friend of the leader (18-36).

Leaders could also use a situation to distract their population. 12-28 noted that this was nothing new and "if you can create an external problem to a state and focus the minds of the population of that state on the external problem, it can alleviate your own internal problems" from internal unrest or political issues (12-28). They gave examples of the Iranian people uniting behind their government against an Iraqi threat in the 1980s, and the Argentinian invasion of the Falkland Islands in 1982 so that the British response could be used as a distraction from domestic issues.

Thus, in addition to the impact on the services or economy of the other state, there are other related factors which may align with that impact, and need to be considered alongside it. These include relationships within the state and the potential for responses to their actions to be used as a distraction. For the UK, or another Western state considering cyber activity to influence and deter, there is

also the need to adhere to international law and maintain their status as a responsible cyber power.

Given the sample population who contributed to both the questionnaire and the interviews, discussions on this area were inevitably centred on the viewpoint of a Western democracy. Some interviewees (particularly 09-09) highlighted throughout their responses that other states had different views and approaches to cyberspace from the West. The inclusion of culture, which had not been addressed in the questionnaire, in the interviews gave an opportunity for a wider exploration.

7.11 Culture

All interviewees confirmed the need to consider culture in planning any cyber activity, and indeed, as noted by 07-05 and 04-37, any military activity. Some attempted to define what was meant by culture, with 0F-07 using their background in organisational culture to focus on values, beliefs and behaviours, and the relationship these have with history and how the state will act when challenged. 06-23 saw the word culture as “a broad church” and unpicked some of the elements within it: religion, gender, identity, how a society is governed in terms of “autocratic versus democratic, technocratic, theocratic, how that's played out” (06-23).

02-25 said they had long pondered what was meant by culture, but without a satisfactory answer. They had previously considered the work of Hofstede (2011, as noted in the literature review) but continued to question how far culture was similar between groups of people within different societies: “if you're a kind of cyber nerd or geek, do you have more in common with adversary geeks?” (02-25). In common with others, they saw the ultimate aim of any activity as cognitive effect, which might be to make decision makers less trusting of their data and so unable to make a decision. For 02-25 it was important to understand what might cause the other party to question their operational premise.

03-06 and 16-32 took a similar cyber-focused view, where the other's culture would determine “their approach to cyber and conducting cyber, their willingness

to take risk. Their willingness to potentially be attributed?" and whether they care about being attributed "because they're working on different standards to your own" (03-06). A similar view about whether certain other states care about being attributed, or indeed care about the actions they undertake, was made by 09-09, who was clear that cultural issues "play a huge driving factor" in the cyber and wider landscape that need to be worked around. They gave the example of whether an exit strategy should be offered to Russian President Putin following the Russian invasion of Ukraine in 2022, as Russian culture meant he could not back down and "look weak in front of his generals and the rest of this government" (09-09). Continuing the post-conflict theme, 04-37 was clear about the need for planning to take account of the future end state:

"how do we want that state to be functioning after we have achieved what we want to achieve. So thinking right through to the sort of handover transition period is something that we always talk about. It's not being too heavy handed and then causing issues long term. It's using the proportionality to just do the minimum you need to do to achieve what you want to do, and whether the second order and third order effects are acceptable in the long term" (04-37)

A different aspect of culture was also touched on by 09-09 and 02-25, namely how culture affects national strategy. 09-09 saw that "China seems to be a lot more a rational process" which stems from a strategy of wanting economic dominance and seeking this through gaining research and development information from others. Russia's strategy came from their "combative culture, us against them, us against the rest of the world" (09-09) but again this stemmed from their clear strategic view of their place in the world. 02-25 contrasted states like China, who set a long-term strategy and "then employed the cyber vehicle to get after it" with the UK and other Western powers, who lacked the same strategic focus. They noted that while the UK was very good at responding to crises it was not so good at working out longer term strategies but tended to be more reactive, seeing itself as important and others "having a go at us because they can, ... they want to adjust the status quo" (02-25), although this was beginning to change,

particularly over the last couple of years. 02-25 also saw a struggle in the West's approach to operationalising cyber activity because they wanted to put military processes around it but "although it will have a bearing in a military context, it's not just military" (02-25).

12-38 focused upon the need to be considerate of the other party's culture, particularly in terms of their "sacred values" driven by historical, religious or ideological factors. For them it was key to understand the adversary perception "before you can think about having an effect" (12-38). 14-26 similarly noted the importance of sacred values, but also made the corollary point that there may be "things that they don't value that we might expect they will value" (14-26).

Moving on to the potential use of a tool such as the World Values Survey (WVS, 2022), only two interviewees had previous knowledge of the WVS. Most interviewees were generally positive about the potential value of such a tool to help think about culture, although several were less sure, with 07-05, 06-23 and 12-38 (who was familiar with it) concerned that it might risk oversimplification and stereotyping, and failing to recognise the different cultures that exist within a single state. 12-38 did, however, consider it good in giving an overall picture of where different states lie in comparison to others.

The two axes used in the WVS model also caused debate. Looking first at the survival versus self-expression axis, 07-05 and 03-06 both suggested that this largely depended on wealth (scaling from poorer to richer states, or in 03-06's words, survival versus prosperity), while some questioned whether "survival" referred to individual or collective survival. 16-32 began by taking it as "a day-to-day struggle for life", but could not reconcile that with "the ability to get out there and sort of live your life as you want to" (16-32). Once it was confirmed that it was about collective survival and whether they felt generally threatened, the contrast began to make sense to them.

0F-07 initially questioned the validity of both axes but suggested that the survival versus self-expression axis felt similar to Maslow's hierarchy of needs¹¹, and wondered whether there was more fidelity in that axis. They explained their thinking, with the bottom row of Maslow's hierarchy as survival and the top one as self-actualisation, with various layers between. While this again suggests individual rather than collective security the model would still work with collective security. They also noted that the interpretation depended upon the international relations lens to which one subscribed, and that as a realist they saw that "every country is looking out for itself, and coalitions are there not through pure altruism, it's because it helps itself. And therefore you could look at that bottom one and go actually is it about survival or is it about benefit to self?" (0F-07). Overall, though, they concluded that both the axes shown were relevant but were not the sole dimensions.

Generally, the traditional versus secular axis, caused less comment. Apart from 0F-07 mentioned above, the only other support for its relevance was from 16-32, who observed that religion, or the lack of it, played a part in many nations. In contrast, 09-09 saw a huge range in how religious expression played out in different states in terms of their values, priorities and activities. They gave the example of Qatar, where many things stemmed from their religious expression as an Islamic state, but they thought that the specific religion would cause further difference, so a strongly Islamic state would demonstrate the effect of religion on individual values in a different way from highly Catholic states in Latin America. "The implications of these different elements ... can still change the dynamic considerably" (09-09).

03-06 wanted to change the axes completely, suggesting those bound by cyber norms versus those not, while 02-25 thought it should perhaps cover how hierarchical and how obedient the system was, or how far those affected by

¹¹ Maslow's hierarchy of needs (usually depicted as a pyramid) demonstrates the needs that must be in place for individuals to reach their full potential (self-actualisation). The pyramid base addresses physiological (survival) needs, moving up the hierarchy with layers for each of safety, social (love and belonging), esteem, and self-actualisation. The needs at each layer must be satisfied before an individual can approach those at the layer above (Maslow, 2000, p1).

degraded systems had the power to shout about it and change it or just having to get on regardless. This more tactical approach was derived from 02-25's experience in focusing on quite specific groups of people to be influenced rather than a nation or other cultural level, and so while the WVS might help at the macro level it would not be so useful for particular groups.

In summary, having an expression of cultural contrast was seen as worthwhile, despite the level of questioning of the detail of the WVS approach.

7.12 Impact

Impact has already been addressed in some of the factors above. On the positive side, many interviewees suggested that activities carried out in cyberspace can support credibility by demonstrating capability. If it had not achieved the desired effect, however, that could result in a loss of credibility to some degree (03-06), or if made public by the other party could have a negative effect on one's own population because "we've got found doing stuff, either we shouldn't be doing or we're not very good, or both" (02-25).

Measuring impact was seen as more of a challenge. Some doubted whether it was possible (03-06 considering escalation and attribution; 09-09 about credibility and external stakeholder perception; 14-26 about escalation and credibility). 02-25 noted that it was hard to prove a negative: if nothing happened was it a result of one's own actions to deter? While generally positive about measurement, 04-37 did not think one could measure escalation before an action, but only afterwards, although they offered a very direct approach to measuring credibility: "What are they actually doing about it? And if they're doing nothing, then I'd suggest that they probably don't think it's credible" (04-37).

Some (09-09, 14-26, 12-38) pointed to looking at adversary actions in response to one's own actions, and whether we could baseline these. 09-09 recognised that measuring these was challenging because the adversary would deny, downplay or spin the impact, while 12-38 questioned whether a causal link could be made, and 14-26 noted that the response would be very contextual and actor-specific in terms of what the other party considered to be a proportionate

response. 09-09 also pointed out that, unlike for other threats such terrorism, the UK had no agreed threat level for cyber.

Similar but possibly longer-term suggestions came from others. 07-05 proposed seeing whether the overall intensity/quantity of cyber attacks decreases, alongside whether it changed adversary behaviour. Technical defensive measures played an important role for 03-06, looking for fewer attempted attacks measured by a reduced number of probes on and attempts to gain access to systems, and 0F-07, who combined deterrence through effective cyber defence with influencing the narrative and public relations exercises.

More direct impact on the adversary in battle damage assessment (BDA) terms of systems taken down, financial impact and how many streetlights went out was favoured by 14-26, who described themselves as “very much an effects-based person.” They saw planning as based on the effect to be achieved, together with determining metrics which could give a measurement of success. 07-05 agreed that measures of effectiveness should be defined at the start, while 04-37 was also keen to have a metric in mind from the start alongside determining the outcomes. Unintended consequences and second and third order consequences were also important to 0F-07.

In summary, while impact was recognised as supporting credibility, its measurement was seen as challenging, not only because of the difficulty of seeing the real impact but also because of the difficulty of proving the causal link to one’s own actions.

7.13 Understanding of the context

Having the right information to understand the situation was a recurring theme, particularly for measuring the impact of an action. This included both covert and open source intelligence¹².

¹² Open source intelligence is “publicly available information that has been discovered, determined to be of intelligence value, and disseminated by a member of the [Intelligence Community]” (Williams and Blum, 2018, p8).

Covert intelligence was important for some, including 03-06, 02-25 and 18-36. 07-05, 04-37 and 12-38 focused particularly on intelligence about the other's military capabilities and understanding the impact of one's actions upon the other state. It was hard, though, to link this back to one's own actions because "They could be concerned about something else entirely, another state's capabilities" (12-38). 16-32 was keen to understand the impact of targeting particular areas in advance, while 07-05 was explicit about wanting intelligence before and after our actions.

The need for monitoring and assessing intelligence was recognised by 02-25 to inform on how the other's actions varied from their rhetoric. 03-06 took a similar stance, but acknowledged that it was difficult, while 18-38 considered the strategic intelligence that could be obtained through this analysis and assessment, including the reactions of decision makers. The Defence approach of having "desks for countries or regions" was applauded for allowing "a continual focus on that country, region, area to be in a position to not just anticipate stuff emerging or evolving, but to have insight." (0F-07).

An area supported by both covert and open source intelligence, such as reports from commercial cyber security companies, was threat intelligence. This was highlighted generally by 03-06, while 07-05 was again more specific, looking for information on the main cyber actor groups, their services, tactics, techniques and procedures (TTPs) and intrusion sets.

Open source intelligence was also acknowledged to be very valuable. This applied not only to media communications (cited by 07-05 and 18-36) and social media channels (03-06, 18-36 and 04-37), but also to more formal communications. Military and professional journals (such as equivalents of the Royal United Services Institute, RUSI) and government communications including strategies and doctrine were highlighted in order to understand the other's thinking (07-05), to help identify the other's red lines (02-25), and to inform on changes of direction (14-26 and 12-38).

Cultural values and understanding the other state's sacred values were an important area for understanding for some: "why are they different to me, what

would I not understand about them and what assumption should I not make?” (14-26). 12-38 offered a similar focus on cultural profiles and sociocultural assessments, as well as psychological profiles of key figures. Societal issues such as pattern of life were cited by 03-06, 06-23 and 18-36 (who acknowledged that their example of “full car parks outside certain buildings” was difficult to measure). 06-23 was also keen to understand the depth of adoption of technology by the other state together with relevant demographics in order to gain “an understanding of the attack surface that is exposed.”

09-09 contrasted the difference between strategic intent and operational intent. “China’s strategic intent is ... to position itself as a global dominant economic power. That’s a strategic intent, it’s writ quite large, it’s not going to change anytime soon” and we can understand it (09-09). Understanding the other state’s operational level intent is, however, an area where we “really struggle” to work out whether they will attack a particular organisation or another one, or how they will attack, “and most of the time we say, well, we don’t know” (09-09). This is an area where they would like to see more intelligence on

“[other states] operational priorities of targeting, the decision making processes and factors, for what they see as important and worth going after, prioritising or not prioritising. So intelligence in that sense would be super helpful, it would be useful, and is something that is very difficult to get. And so that would play into that whole deterrence piece quite well.”
(09-09)

One final point made about understanding was that it allowed one to be in charge of the narrative, and thus, as 16-32 noted, to counter disinformation. They further argued that this is not just about the other’s narrative, but also about how they see our credibility and the operations carried out by ourselves and our allies. Understanding the other’s perception of us is as important as our perception of them:

“And equally, you’ve got to do your own assessment of yourself as well, your capabilities, ... how much of that is known in the public domain. So

things like National Cyber Force pushing out a document recently ... That wasn't necessarily just for the UK" (16-32)

Understanding the context of the situation was important to interviewees, and included a variety of intelligence sources, both covert and open source. While many factors contributed to understanding strategic intent the detail of operational intent was more difficult but would be valuable for deterrence.

7.14 Other remarks

In addition to the topics covered above, some further points were highlighted by interviewees. These included communications and influence activities, technical versus human effect, and the suitability of a capability.

03-06 viewed active influence activities and working to change the narrative as a proactive part of deterrence. As noted in the section on Understanding, clear communication was seen as key: "If our deterrence is effective it is because it is based upon published cyber capabilities (e.g. NCSC tools for defence and MOD OC capability)" (07-05). Exercises played an important part not only in demonstrating capability but also in reassuring allies (07-05). However, exercises such as NATO's Cyber Warrior were about training and development, but 16-32 noted that the media coverage of Cyber Warrior would emphasise where capability succeeded, rather than where things did not go to plan.

Contrasting the technical effect sought by law enforcement with the focus on human effect from offensive capabilities, 09-09 suggested that technical effects can be counterproductive in the long term as they can make an adversary consider how to make themselves better and harder to stop. Instead, "proper well-coordinated OC and reaction capabilities" were needed to have a human impact to deter the person at the other end of the keyboard (09-09). 09-09 also noted that at the working level, threat actors could be unpredictable as they might be acting on direction or working for their own ends, so unconstrained by any direction. A similar point was made about cyber proxies who "don't operate by any particular rule of law" and "present not quite the same level of risk, but

certainly a level of risk” (03-06). Both 03-06 and 09-09 saw deterrence as applicable to these groups as well as at state level.

One of the points often associated with offensive cyber exploits is their single use, in that once an exploit has been carried out and is known about it cannot be used again because defences can be put in place against it. An exploit kept on the shelf, however, may become useless if the vulnerability it exploits is removed by defences or system changes. Only 18-36 specifically raised this point, referring to the “opportunity cost” and the question of whether the capability might be better suited to another target, either in the same or another state.

While these additional points were outside the scope of the main factors being addressed, they offered additional insights from the experience of the interviewees. Therefore it is worthwhile capturing these, even though they may not directly influence the conclusions drawn from the data collection.

7.15 Chapter summary

This chapter has described the approach to codifying and reviewing the data collected in the interviews, and articulated the data within the coded themes. Following an opening section on the definition of deterrence in cyberspace, each of the five factors rated most relevant in the questionnaire was explored, followed by a section on culture and further sections identifying other topics which interviewees covered within the given semi-structured interview framework. This continues the response to RQ2: “What are the main factors relevant to the interplay between the deterrer and deterree?”

The interview data was wide-ranging and supported the relevance of the five factors selected from the questionnaire. The varied backgrounds of the interviewees, and the real, and in some cases very deep, experience that they brought helped to give a rounded picture of the considerations, opportunities and challenges of cyberspace activities and of deterrence in cyberspace.

The data outlined in this chapter is discussed and critically reviewed in the next chapter, Discussion of Findings.

8 Discussion of Findings

8.1 Chapter overview

This chapter brings together the findings of the literature review, in line with the conceptual framework, with those of the primary research to answer:

- RQ1: What is meant by deterrence in cyberspace?
- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

The literature review showed that the basic concept of deterrence still applies in cyberspace, although the operational domain presents new challenges, particularly with credibility. A simple cost-benefit calculation approach (Snyder, 1961) may have been appropriate in the Cold War but is not fit for purpose in cyberspace and does not address issues of perception and cultural environment which are so important in cyberspace.

Following the literature review, the conceptual framework was developed which used key elements identified in the literature and refined these to set out the direction for the research. This in turn informed the research methodology which led to the various parts of the research, each of which has been described and the results given in the relevant chapters.

This chapter draws together the literature review and the research data to identify and reflect upon common themes and differences. It starts by considering the definition of deterrence in cyberspace and then reviews the findings about each of the factors considered in the interviews, namely escalation, credibility, attribution, perception of external states, the other state and culture. This is followed by a general discussion drawing together key points, concluding with the need to see the situation from the other party's perspective, in order to give one's deterrence declaration the best chance of success. Having discussed the findings of the research, the chapter reflects upon the approach taken and ends by developing the conceptual framework to reflect the findings.

8.2 Defining deterrence in cyberspace

Some interviewees (particularly 0F-07, 12-28 and 16-32) were clear about the need to see deterrence in cyberspace in a wider, multi-domain approach. 0F-07's distinction between deterrence *of* cyber activities and deterrence *using* cyber activities was particularly pertinent to drawing deterrence in cyberspace away from the narrow cyber-on-cyber view of "cyber deterrence" adopted by many authors in the literature review. Others tended to stay within the narrower bounds, or focus on defining deterrence, but this was probably affected by this being the initial question in the interviews and really intended as a conversation starter.

All the definitions of deterrence were very much in line with conventional thinking on deterrence as articulated in the literature review: seeking to prevent an action through fear of the consequences (Schelling, 1966, p71; Great Britain. HM Government, 2015, p23). Cost-benefit, changing the other's intent, and the need for deterrence to be clear, capable and credible were all offered, all of which aligned with the literature and with the approach determined in the conceptual framework.

The definition of cyberspace was either implicitly or explicitly in line with the UK MOD definition chosen in the literature review. 12-28 referred to the six layers and to information influencing the cognitive, virtual and physical dimensions, while 06-23 referred to the layered definition in the MOD Cyber Primer (Great Britain. Ministry of Defence, 2022). This alignment with the MOD definition was hardly surprising given that all the interviewees came from the UK and were working, or had done, in cyber-related roles either in or alongside the UK military.

This leads to the question of whether the UK MOD definition of cyberspace (Great Britain. Ministry of Defence, 2022, p7) was the right one to use for this research. Given the sample population for the research and the clearly articulated UK focus of the research, it was the most appropriate definition. It aligns with other Western definitions, as noted in the literature review, and takes a broad view of cyberspace which includes not only technology but also cognitive effects, including interactions between people, and therefore fits well with deterrence. Deterrence in cyberspace can thus encompass everything from physical effects on networks

(such as disabling or moving communication links), to causing loss of confidentiality or integrity of information (through espionage or changing the content of information as a warning of capability) and impacting the perceptions and interactions of individuals, and thus their behaviour. This also allows for its relationship with other strategic levers to be recognised, including DIME and the other military operational domains. A purely technical definition would not recognise the breadth but would only allow focus on the network infrastructure, servers and data in terms of bits and bytes, missing wider cognitive aspects. It would be analogous to considering arms purely in terms of their technical firepower and not the physical impact on the target they were aimed at.

That said, whether this research would hold in other cultures, including other Western ones, cannot be inferred because of the UK bias. Future research might well consider how other states' definitions affect their view of cyberspace activities as well as how they affect the view of cyber and planning experts, and whether the factors identified here as relevant to deterrence in cyberspace match the views of those experts.

8.3 Escalation

The initial conceptual framework (Figure 3-1) included the security dilemma, which was subsequently taken forward in the research as escalation (see the developed conceptual framework, at Figure 3-6). The mutual distrust between states can easily spiral, as shown by the examples in the literature review. While Sample (2000) saw a generally consistent positive correlation between arms increases and escalation of disputes, this was not the case during the nuclear age because of the existential threat posed by nuclear weapons. This suggests that where the threat is not existential (as in cyberspace) the security dilemma will hold, bringing escalation. A related question raised by 02-25 in their questionnaire response seems pertinent, even though this was ostensibly about the offence-defence balance. 02-25 noted that in kinetic domains it swung between dominance of the offensive or defensive, while in the nuclear age it tended towards coercing the opponent. They wondered about a potentially different dynamic in cyberspace. While nothing in the literature review or in the

interviews suggested an answer to this question, it does seem to be answered by the implicit conclusion drawn above.

Weapons (including nuclear) are usually applicable to both offensive and defensive use: one can use a sword to attack, but can also use the same sword in self-defence if attacked, or indeed display the sword to deter a would-be attacker. There are, however, some entities which are purely defensive, such as fortresses or walls, which are intended to keep adversaries out (defence) and deter attack. This is very much the case in cyberspace, with sound defences such as firewalls or access control features being clearly purely defensive, but other activities, such as penetration testing, being potentially defensive (to prove the security of one's own system) and offensive (to attempt to break into another's system). The creation of the UK's National Cyber Force was clearly intended to display offensive capability ("to counter and contest those who would do harm to the UK or its allies" (Great Britain. National Cyber Force, 2023, p11)) as was US Cyber Command. While purely defensive measures (such as fortresses or firewalls) are unlikely to cause escalation, offensive ones (such as weapons and organisations with an offensive mission) might. Whether the detailed breakdown provided in the "offensive" tables for capability and intent in the Belfer Center's National Cyber Power Index (Voo et al., 2022) might fuel competition to ensure a state is "better" than its adversaries remains to be seen, but the idea of a public scale runs counter to Beckermann's dismissal of the cyber security dilemma as a red herring (Beckermann, 2022, pp2, 6).

Yet capability does not seem to deter. Buchanan (2016, pp33, 48) noted the difficulty of distinguishing between intrusions for espionage and those preparatory to offensive activity. 09-09 took a rather different view, that cyberspace was "kind of borne out from traditional views of espionage rather than conflict" where espionage is an accepted form of behaviour between states. Espionage is generally accepted (Lewis, 2022, p15; Kosseff, 2024, p229) - or rather, it seems, it is accepted provided one does not get caught, and certainly not if one then releases the information (Wilner, 2017, p315, discussing the different treatment of the espionage activities against the DNC and OPM). Given

that much activity is information gathering (i.e. espionage) and that all cyber incursions start in the same way with a presence on the system (whether solely for espionage or for more subversive effects) there may be some truth in 09-09's view, although they also noted moves towards imposing sanctions on other states following cyber activity. Certainly, however, the increasing number of states developing offensive cyber capabilities suggests that the cybersecurity dilemma may be at play, with or without the encouragement of a publicly available rating.

A rather different approach to escalation was the gradual escalation described by 03-06, where a deterrence activity was not sufficient by itself, leading to increasing deterrence activity. While this seemed a valid point, it did suggest that a cycle was occurring of deterrence failure leading to attack, or of a stand-off of threats followed by deterrence declarations. In either case deterrence was not working as the deterrer would wish, echoing Gray's (2003, p13) point that if costs have already been imposed then deterrence has either failed or not been tried.

Escalation beyond cyberspace was suggested but not well developed within the literature. The interviews generally bore this out by not highlighting this aspect. Of those that did, 02-25 was surprised that discussion always included escalation beyond cyber, while 0F-07 was keen to see offensive cyber activities used within a multi-lever approach including all the elements of DIME, and 16-32 referred to cyberspace within "an overall deterrence posture." While 12-28's reference to a multi-domain operations approach might seem to include kinetic activity, they were clear that this referred to the interactions between domains, as where a cyber attack on a military platform impacts on that platform's ability to operate in its own domain (e.g. a cyber attack on the control system of a ship might impact on its effectiveness in the maritime domain). Even 06-23, while acknowledging that escalation could be into kinetic activity, quickly moved on to talking about escalating to impact on a larger group or broader functions in cyberspace. Interestingly, only 12-38 highlighted the potential for cyber activities to have potentially serious indirect effects. So while in theory escalation is recognised as moving beyond cyberspace into kinetic activity, this does not seem to be borne

out by either the literature or this research, although the link to the non-military aspects of DIME was acknowledged.

In summary, the security dilemma does seem to be an issue in cyberspace in the way described by Buchanan (2016) and may be exacerbated by the readily available league table (Voo et al., 2022). However, there is no indication at present of this spilling over into other operational domains, so any spiralling of hostilities seems likely to remain in cyberspace, at least in the short term.

8.4 Credibility

The literature review had found that credibility was a complex matter that required both capability and willingness but could be undermined if words were not seen to be followed through into actions. Further, demonstrating capability without giving away competitive advantage could be challenging. Both of these issues could adversely affect the deterree's perception of the deterrer's capability, as confirmed by the views of interviewees.

An interesting, and concerning, point was 02-25's description of how others' "noisy" attacks worried policymakers. Policymakers may not have the depth of understanding of every operational domain and therefore could over- or underestimate what is possible, both in defensive and offensive activities, and this could be exacerbated by the effect others' actions might have on their perceptions. While this could, as 02-25 recognised, result in the UK not acting to deter other states, this is a situation that should improve over time as more people come into lead roles with a better understanding of cyberspace and its challenges.

Measuring perception of credibility was seen by interviewees as a challenge, which aligns with the literature about misperception. Although a possibly pragmatic approach, it was hard to fully agree with 04-37's view that if subject matter experts think it is credible then so would the adversary, as they might not have a complete understanding of one's capability, especially if one preferred covertness and containment of one's offensive cyber activities. That said, openness about the creation of an organisation such as the NCF will help, as

indeed will exercises, as suggested in the group workshop and by 07-05 and 16-32 in the interviews, and wider communications such as the Belfer Center's National Cyber Power Index (Voo et al., 2022).

A point not explicitly addressed in the literature was that credibility is a relative rather than an absolute attribute from the viewpoint of other parties. One knows one's own capability and willingness, and will make a judgment about the capability and intent (willingness) of other states, but how credible a threat from another state is will depend upon one's own capability (and willingness) to defend or deter. If state A judges state B as more capable and willing to mount an attack than state A is able to defend against it, or that state B's capability and willingness to act exceeds state A's own ability to successfully deter them through threatening to impose costs on them, then state A will perceive state B as having greater credibility than state A. If the opposite holds, then state B has less credibility. Another state, C, will reach their own judgment about state B in the same way, but may determine the opposite of state A because its own capability and willingness is different to A's. Thus credibility is an attribute determined by the other party relative to themselves.

This can clearly be seen in the Belfer Center's National Cyber Power Index (Voo et al., 2022) included in the draft proposed framework at Appendix H. In the overall rating, shown on p2 of the framework, the United Kingdom is ranked below Russia and China but above the Democratic People's Republic of Korea (DPRK). Looking at the component criteria (p5-8) these indicate that for defence (strengthening and hardening national cyber defences) the United Kingdom is placed above all three (although to differing levels), while for offence (destroying or disabling an adversary's infrastructure and capabilities) the United Kingdom is below Russia and China but above DPRK.

It is, however, important not to overegg the importance of a document such as the Index. While it offers a useful insight, it should not replace one's own intelligence gathering, as the biases of the specialists used, including their nationality and specialisms, and any disagreements, are not addressed (Voo et al., 2022, p17). Further, the assessments will change over time as has already

happened since the 2020 publication (Voo et al., 2022, pp10, 13) and the latest version is already two years old (published September 2022) so the assessments would have been slightly older than that. This is aside from the use of estimated scores for some states (particularly DPRK). However, the Index remains a useful tool to supplement other intelligence.

In summary, while it is hard to measure the credibility that another party will attach to one's capability and intent, intelligence and other sources can help, although their limitations need to be understood. The nature of credibility as a relative attribute should also be remembered.

8.5 Attribution

The offence-defence balance, like the security dilemma discussed above, was included in the initial conceptual framework. It will influence a state's strategic direction with respect to security. Attribution is of particular relevance to cyber activities because the apparent difficulty of definitive attribution of an attacker's remote access is perceived as favouring an offensive strategy (Libicki, 2009, p5, 41; Nye, 2011, p21). So while the deterrer cannot *directly* influence the deterree's strategic intent, they can at least try to influence their attribution of any activity the deterrer conducts in cyberspace.

The literature review included a description of the model of the "Blame Game" by Edwards et al. (2017) to determine the costs to an attacker or attacking or not, and to a victim of blaming (attributing) the attacker or tolerating the attack. While it did not focus specifically on deterrence, and its shortcomings were acknowledged in the literature review, it did try to offer an insight into the wider factors about attribution.

The interviews focused on similar questions about whether or not one would wish to be attributed, and whether this would be private or public. Despite the claim of one questionnaire respondent that an attack in cyberspace could "never truly be attributable" (07-12), and another that "If they know it's you then you are not good at Cyber Ops" (02-14), attribution was increasingly common, as several

interviewees observed, and it was often likely to be clear from the geopolitical context.

While the decision to attribute lies with other parties (the deterree or possibly others being impacted), the questions of whether or not one would wish to be attributed, and whether attribution would be private or public, need to be considered in planning. Without at least private attribution (or at least a recognition of some activity which can be associated by the deterree with their own behaviour) there can be no deterrence, as deterrence requires some kind of declaration that must be received by the deterree. Thus, although Healey and Jenkins (2019) describe their “rough and ready” approach as determining whether cyber deterrence is working in terms of the US policy of ‘persistent presence’ (Nakasone, 2019), persistent presence cannot deter directly, since, as 06-23 observed, attribution could prevent “maintaining a presence on a target network.” It might, however, deter through fear that the US might seek such access.

In some circumstances private attribution might be preferable for the deterree to prevent their having to admit that an exploit was successful, thus signalling to the deterrer and to others a potential weakness in their defences. If they subsequently change their behaviour that might of course signal this to the deterrer, but at least that might avoid wider awareness, including highlighting to their own citizens their inability to stop the exploit.

Some interviewees, including 18-36, noted that public attribution was, essentially, free advertising, in that it spread the word about one’s capability and credibility, and this chimed with Rid’s view that the credibility of the US benefitted from speculation about their role in Stuxnet (2012, p19). The downside, however, is that it could portray the deterrer as the aggressor, particularly if they have not made public the threat which they are seeking to deter. Coordinated statements from allies may help, as with some of the complementary statements made about Chinese data exfiltration by Five Eyes’ partners, but even these could be refuted or brushed off by the attributed party, as noted by 09-09 and 16-32.

This discussion reinforces the need for potential attribution to be carefully considered in planning. Neither public nor private attribution can be guaranteed, in that public attribution is in the gift of the victim of the activity (so in a deterrence situation the deterree, not the deterrer), and both would require them to receive the deterrence message (which itself is not an automatic given). Consideration of attribution is still, however, worthwhile as it might point to a preference for a more or less obvious approach in keeping with the expectations on a responsible cyber power.

8.6 Perception of external states

As Bunn (2007, p6) noted about credibility, a message to one will be heard by all, including states not involved in the specific deterrence situation. This may include allies of both parties as well as neutral states, all of whom may be influenced nearer to or further from either party. This was a widely accepted factor in the interviews, even for those who had not selected it in the questionnaire.

While any two allies will have their own perceptions of the relationship between them, including trade and economic dependencies as well as military agreements, 09-09's assertion that for some states there were no allies, only those who were useful, risks overstating the issue for states that do not adhere to Western values. It was clear in the interview that 09-09 was speaking about a non-Western state, but while relationships might be closer between members of groups such as the Five Eyes or NATO, a degree of expediency could come into any relationship, and may not be unique to those who do not share Western values.

An interesting point was made by 12-28 and 16-32 about the place of both the external states and one's own state on the international stage. This was especially important for Western states such as the United Kingdom, who wanted to be seen as responsible cyber powers who observed international law. Non-adherence to international law could not only cause allies to withdraw their support, but could also undermine a state's credibility where they had adopted the moral high ground at international bodies such as the United Nations.

A similar point was made in the questionnaire by 00-27, who offered an additional factor “Adherence to established rules, norms and principles (legally binding, political statements, etc) and ensuring legitimacy.” This was echoed by 00-30 in their questionnaire response, who suggested “Home state public support/trust/ethical-concerns.” These two were unique not only in making such a suggestion, but also in being the only questionnaire respondents who did not claim one of the requested specialisms. While it was clear from the interviews that their views were not unique, it was surprising that they were the only ones to suggest adding these factors to the list.

In summary, the perceptions of external states are important to consider, but relationships will vary in nature although they may be affected by deterrence activities. Consistency with one’s own stated stance is also important, and needs to be maintained.

8.7 Effect on the other state

The points made above about the United Kingdom’s stated objective of being a responsible cyber power were relevant when considering the impact of potential cyber activity on the services and economy of the other state. While these were listed by 06-23 as including “food security, energy security, physical security, education” as well as areas such as banking, their list stopped short of impact on health services, but these present an ethical issue which requires indirect impacts to be considered, as impacts affecting access to medical records or power disruption could easily lead to unintended consequences that overstep the line.

Activity not presenting that ethical dilemma was recognised by several interviewees as valuable and the reversibility of some cyber activities was noted. Although only 12-28 specifically used the phrase it was clear that many saw cyber activity as “one of the metaphoric golf clubs in the bag.”

The first interview held was with 07-05, who was adamant that impact on services or economy was “not an issue” because the UK would not target the economy. For them, the role of a responsible cyber power operating with legal and ethical norms was paramount. Although others were less forceful in expressing that view,

recognising that in actual conflict the focus would be on the ultimate aim, and that more generally necessity, proportionality and justification (NPJ) addressed the issue, the role of a responsible cyber power who played by the rules (even if others did not) was a recurring theme throughout the interviews.

Impact on the other state's leadership was not subject to the same level of restraint. Some contrasted the different natures of the UK's democratic society, and the role of the military and civil servants in advising, with those of more autocratic states. While this may generally be the case, it is not unknown for some Western states to have less collaborative approaches when more autocratic leaders have been elected, but even in those circumstances there are still some checks and balances.

Being a Western democracy can lead to a touch of complacency. 02-25 observed that the West had largely been in a dominant position since the Second World War, and they felt that the West had generally relied on this fact. The role and status of being a Western democracy needs to be constantly tempered with the ethical requirements which are fundamental to being a responsible cyber power.

8.8 Culture

The literature review found evidence of the need to recognise other actors' values (Maxwell, 1968, p3) and to understand their rationality in terms of their culture, including their political, economic, religious or ideological context (Bar, 2011, p428; Payne, 2011, p399). Despite this, deterrence literature largely focuses on the cost-benefit calculus and ignores the cultural context. None of the models discussed in the literature review acknowledged the importance of culture.

In contrast, all interviewees confirmed the need to consider culture in planning any cyber activity, although they varied in their definitions and approaches. Some also recognised the part culture plays in national strategy and in willingness to take risk, and in how leaders were viewed. Two interviewees expressed how culture was reflected in "sacred values" – tangible or intangible things a party values and will not give up.

How this concern with culture can be articulated and brought into the planning process, however, was not so clear. Rather than attempting to address strategic culture, the interviews explored the practical approach offered by the World Values Survey (WVS, 2022). While most interviewees were positive about the concept of such a tool, the detail was less well received. An interesting question was posed by 09-09 as to whether the specific religion (e.g. Islam or Roman Catholicism) would create difference. The WVS mapping suggested not, and the variety of placings of states where these religions dominate seemed to suggest that strong religion tended to the conservative so the strength of the religion, rather than the specific religion, is the major factor.

Overall, the WVS model appeared to be comprehensive and well researched, but some raised concern that it risked oversimplifying and stereotyping, and there was a general sense that it failed to answer the “so what?” question. It would need considerable work to translate the detail from its extensive data set into a form that planners could use.

Meyer’s (2014) culture map offered a different approach, although this was not included in the interviews, partly because of the lack of clear academic rigour behind it and partly because it was specifically aimed at business executives. It does, however, offer a simple and pragmatic approach, and the underpinning cultural styles are likely to apply across the population more generally, including national leaders, since the styles are not solely the preserve of business executives. Meyer’s scales for communication, leadership and confrontation might be particularly appropriate, as these give an insight into the different styles applying to oneself and to the other: as she stressed, it is the relative positions of the parties that matters, not their absolute position on the scale.

The apparent lack of academic rigour in Meyer’s (2014) work was understandable in what was intended to be a practical guide for business executives, and she did discuss its origins in her work at the INSEAD business school. Yet despite searches no further literature by her offering information on its background could be found. That calls into question how she arrived at the positions on her scales for different nationalities. If state A was marked as a quarter of the way along the

scale, and state B as halfway, whose interpretation was this? Was this the view each state had of itself, was it one state's view (e.g. A's view of itself and its view of B) or was it derived by an independent source from extensive research (as WVS appeared to be)? Meyer's assertion about her work at INSEAD was clearly intended to suggest the third option, but in the absence of any evidence to support this, one has to question the validity. That said, it may still be a potentially useful and easy to apply tool that might be helpful, provided it is used only as a starter for a conversation and not as the absolute answer.

In summary, what was clear from the literature review and the research conducted was the importance of cultural factors. How to assess and articulate these was not clear, and this difficulty explains the lack of inclusion of cultural values in existing models and research. Their importance, however, requires that a way is found to try to assess them, including determining the deterree's sacred values, and to take this assessment into account in planning.

8.9 General discussion

Observing the failure of deterrence is straightforward: the deterree carried out their threatened action. Observing successful deterrence, however, is not. While it is tempting to see a causal link between one's deterrent declaration and the deterree not acting, the cause of their inaction cannot be definitely proved: did something else happen to distract them, or did they never intend aggression?

Yet even with failure of deterrence the cause of failure is not necessarily clear: did the deterrent declaration fail to convince them for some reason, or did they not recognise it as a deterrent declaration (perhaps seeing it as aggression requiring a response), or did they simply not see it? There are, therefore, flaws in the direct approach suggested by 04-37 that if they are not changing their behaviour "then I'd suggest that they probably don't think it's credible." This assumes direct causality that can never be assumed in cyberspace in the way it can with other operational domains. A deterrent declaration may be less obviously visible in cyberspace. System issues may not be associated with any form of external action and just put down to a bad day, even if they are noticed, and depending on the quality and attentiveness of the system administration staff

and the monitoring facilities on the network an intrusion may not be recognised. So in the absence of a clearly articulated direct verbal or written conversation, such as the letters exchanged between Kennedy and Khrushchev during the Cuban missile crisis (Kennedy, 1968), it is very difficult to know for certain whether deterrence succeeded or failed, but only that some action was or was not taken.

To be effective, deterrence must be a dialogue. The deterrer makes their declaration, the deterree reviews its credibility and makes their cost-benefit decision about whether to act against the deterrer or to be deterred (Figure 8-1). The deterree's action (whether they are deterred or not) is in turn heard by the deterrer as the parties change places, each seeing themselves as the victim and the other as the aggressor, as discussed in Chapters 1 and 3.

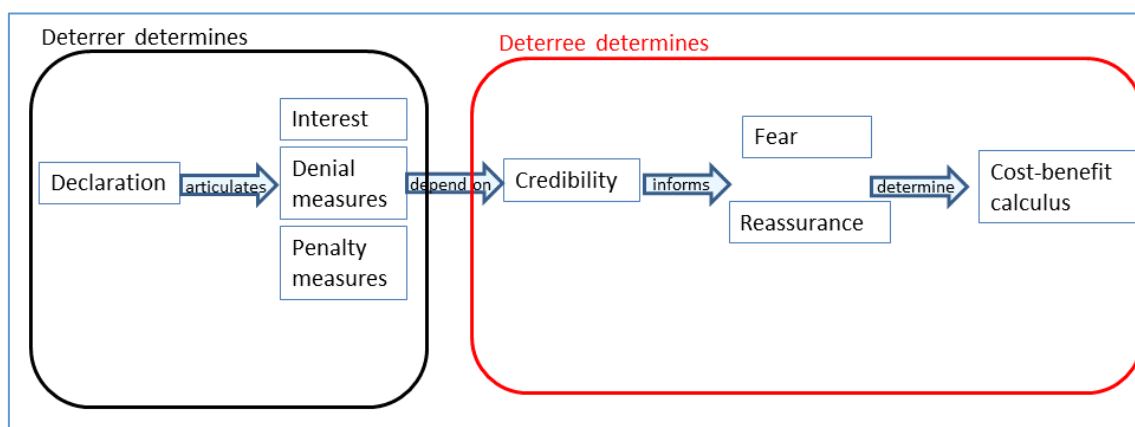


Figure 8-1: Interpretation of relationships in Goodman's (2010) 8 elements of deterrence

In the literature review, several examples were given of misperception, whether through one party ascribing its own version of rationality to the other, or through suspicion of the other's motives, as with Reagan's suspicion of Gorbachev. Consideration must be given to how that can be avoided, and how one party can try to take into account the other's cultural context so their message will be received as intended.

Heuer (1999) described how humans use simplified information processing strategies which introduce cognitive bias in evaluating evidence. Although he was

writing specifically about intelligence analysis, Heuer's work has wider applicability, including to the parties in deterrence. This suggests that finding a way to challenge these strategies might help to reduce cognitive bias.

A good start point might be to try to see the situation from the other party's point of view. What are their sacred values, and how has their experience (their history) shaped their beliefs and culture (as noted by 0F-07)? How could they perceive one's own actions? How can what are intended as deterrence actions avoid being viewed "as aggressive/escalatory actions and ... trigger an escalatory spiral" (workshop participant G-2h)?

Sharp (2017) gives the example of the North Korean cyber attack on Sony to describe his model. In evaluating this model in the literature review it was suggested that the situation could be viewed from the North Korean perspective, which gives a rather different interpretation. Similarly, one of the questionnaire respondents criticised the scenario described in the questionnaire for being too simplistic, noting that "Liberal democratic values ... are not universally held in regard around the world" (16-34). Ironically, for the original plan to play out the scenario as a simulation with individuals taking the two sides, two different versions of the state descriptions were produced to reflect their different viewpoints (see Appendix F). In a real situation intelligence (including open source media) could be used to create the other state's views of itself and one's own state. As an example, the narrative from the Russian President Putin describes NATO as an aggressor wanting to destroy Russia. This may be Putin's real belief, or may just be rhetoric, but many Russians will believe it because it is the message they have been told, a point made by 16-32 when discussing attribution.

Another possible approach is to think about how one's action could be perceived (or misperceived). Table 8-1 gives examples of favourable and unfavourable interpretations of factors by the deterree from the point of view of the deterrer.

Table 8-1: Potential impact of factors on deterree from point of view of deterrer

Note: for simplicity, the two parties are referred to as “us” (deterrer) and “them” (deterree)

Factor	Negative impact	Positive impact
Potential for escalation	Inflame situation	Showing our strength will calm the situation down
Credibility of our proposed action	Show us as aggressor	Confirm and enhanced our credibility
Other's willingness to attribute	Show us as aggressor	Confirm impact of our deterrent declaration
Perception of external stakeholders	Sympathy and support for deterree	No support
Impact on other's services or economy	Blame and hostility to us	Lose faith in their leadership

None of this is easy, and one interviewee (14-26) told the researcher (in a separate conversation to their interview) that an intelligence specialist who had tried to point out to senior officers how another state viewed a situation had been accused of “going native” and ignored. Yet seeing the situation from the deterree’s point of view requires empathy, which is not agreement with their position but simply the recognition that they may have a different perspective. President Kennedy’s recognition of that during the Cuban missile crisis resulted in successful deterrence of the Soviet Union (Kennedy, 1968). In contrast, Owen and Ludlow (2017, p165) and the House of Lords’ European Union Committee (Great Britain. House of Lords, 2015) commented on the absence of empathy from post-Cold War Western attitudes towards the Soviet Union and Russia, leading to distrust.

Producing the state descriptions from the “other side” for the original plan for the research, as a simulation of the two sides, was a valuable lesson in thinking about perspectives. An intelligence team could use open source material to do this in a real situation to inform decision makers, seeing behind the rhetoric to reveal truth about the other state’s viewpoint from their published strategies and actions. To some extent planners already try to see the other’s point of view by determining not only what they think is the adversary’s most likely course of action, but also

the adversary's most dangerous (for the planners' state) course of action. Supporting this by creating an empathetic understanding of the other's perspective could offer real benefit to decision makers, provided they could accept this not as "going native" but as a helpful statement to inform them. While the cognitive bias described by Heuer (1999) will make this difficult for many, it offers an opportunity to give deterrence messaging and actions the best chance of success by not unintentionally reinforcing the deterree's negative perceptions.

Dodd recognises this in her concept of choose-ables: where individuals are willing to consider the perspectives of others, then they may include compromises in their choose-ables to meet not only their own needs but also those of the other party (Dodd, 2019, pp104, 107-8). A pertinent example is described by Davis (2015, p330-1) "in the most famous alleged example of deterrence", the Cuban Missile Crisis" where US President Kennedy and Soviet Premier Khrushchev negotiated a bargain acceptable to both sides, succeeding because they both "rose above their advisors" and recognised each other's commitment to their respective states. Kennedy's promises to Khrushchev indicate that he knew the latter needed a face-saving exit strategy, as confirmed by Kennedy (1968, pp103,122) and that his own thinking was along the lines suggested by Dodd. This need to understand the exit strategy was echoed by 09-09 and 04-37 in the interviews.

To summarise, deterrence needs to be a dialogue where the intended message is received and understood by the deterree so they can respond by acting upon it or not. The message may be misunderstood if either party relies on their cognitive bias in interpreting the other's viewpoint, and instead the deterrer needs to acknowledge that the deterree's viewpoint is likely to be different to their own. Attempting to understand the deterree's culture and values, or to consider how one's own messaging and actions may be perceived by the other, will allow the deterrent declaration to be refined so that it not only meets the deterrer's own needs but also those of the deterree.

8.10 Review of the approach

Having completed the research it is appropriate to reflect on the suitability of the approach taken. Has the research been successful in doing what was intended, and was the approach appropriate to deliver this?

As already noted, the original plan for the research had involved participants taking the roles of one or other party and playing out a deterrence scenario in turn. This idea was abandoned because it was feared that this might not reflect reality as it could not guarantee that participants would be able to immerse themselves in the thinking of a different culture. That would essentially bring misperception and false views of rationality into the research, thus invalidating its findings. Further thought on the purpose of the research led to the realisation that, as the parties cycle between deterrer and deterree, considering themselves as the innocent victim and the other party as the aggressor, there was no need to explicitly simulate both sides. The modified version described in this thesis was therefore developed and used.

That would seem to be at variance with the criticism in the literature review of the “three-player behavioural game” (Cui et al., 2017) where there is in fact only one real player, the attacker, with the other two parts of system administrator and user being simulated. The critique notes that while this imposes control it prevents the interaction between the parties being fully explored. If it had been the case in this research that the *interaction* was being explored then it would have been a reasonable argument that there should have been two parties, and that would certainly have been the case if a simulation had been used. That was not the case, though, as this research sought to explore the deterrer’s view of the factors which were *relevant* to the interaction with the deterree. This might seem a minor distinction but it is an important one for the approach.

The scenario was included in the questionnaire, but it was made clear that it was intended as a handrail to help thinking and that the point of the research was to determine the most relevant factors for the deterrer to consider. Asking questionnaire respondents what their course of action would be was considered, but was dismissed to prevent it distracting respondents from what mattered,

namely the factors. The scenario was similarly used in the group workshop, but again only as a vehicle to allow the groups to determine different courses of action and to describe how they arrived at those and the factors they had considered in so doing. The interviews did not use the scenario but explored why the various factors were important and how they could be measured and incorporated into planning.

This research, therefore, was focused on the deterrer's view of the deterree, not directly on the interaction between them. To do that effectively would have required access to two parties who could reasonably act out the roles, and while this might be feasible in a wargaming environment using classified intelligence it would be very difficult to simulate without appropriate resources or the use of classified material. The specific focus of the research, coupled with the recognition that deterrers and deterrees swap places over time as a situation develops, permitted the research approach used and enabled it to be considered valid.

8.11 Conceptual Framework revisited

The conceptual framework in its developed state indicating the factors for the research was shown at Figure 3-6 in the Conceptual Framework chapter. The research identified the five most relevant factors which were the subject of the interviews, together with culture. While some of the original set of factors (such as distraction) were removed, others remained in some form as discussions in the interviews about the impact on services and economy touched on other areas, such as disruption to daily life. Other factors subtly changed their direction, as questions about the perception of external stakeholders morphed into discussion about the perceptions of the deterree itself.

Figure 8-2 develops this to show the factors identified in this research as relevant to the deterree's cost-benefit calculus which the deterrer should consider. These include the factors discussed above and cultural factors specifically addressing the deterree's sacred values and their leadership, the latter in terms of the type of government and any national cultural traits. This refined conceptual framework describes the view taken forward into the creation of a deterrence planning

framework in the next chapter to support RQ3: “How can these factors be included in deterrence planning for deterrence in cyberspace?”

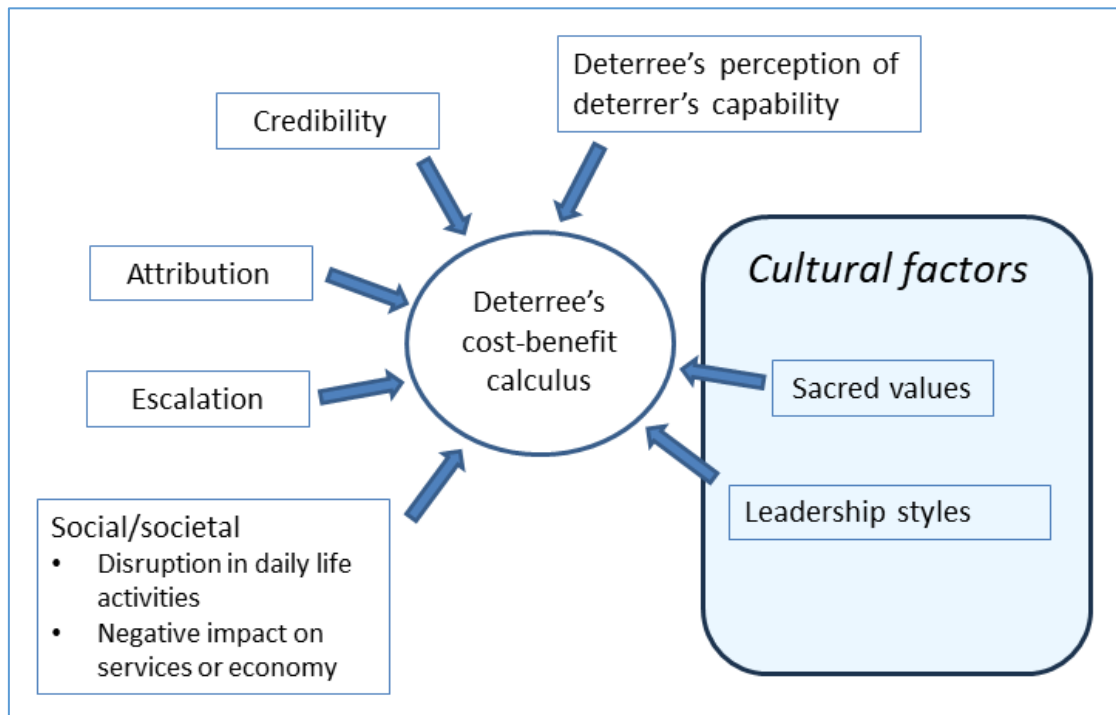


Figure 8-2: Factors affecting the deterree's cost-benefit calculus which the deterrer should consider

Finally, putting this together with Goodman’s eight elements of deterrence gives Figure 8-3. This shows a view of the whole picture including not only the factors which inform the deterrer’s determination of Goodman’s elements, but also the elements which are within the deterree’s determination. It is important to remember, though, that the deterrer’s perception of the deterree’s view of the deterrer’s credibility will not necessarily match the deterree’s actual perception. This dichotomy is supported by critical realism, as was shown in the Research Methodology chapter with the example of the obscured sun. In that example, A perceived the sun to be obscured by a solar eclipse, while B, who believed the sun was a god, perceived it as an expression of the sun god’s anger. While A can cite scientific evidence to support their view and can present this to B, it does not mean that B will be convinced, particularly as they can cite evidence for their perception in that the sun god was clearly placated by their prayers and sacrifice because the sun appeared as normal the next day. This is a major strength of

critical realism for research into a subject such as deterrence: it allows for and accepts the different empirical realities created by experience, and for the difference between what one party *thinks* the other will perceive and what the second party *does* perceive.

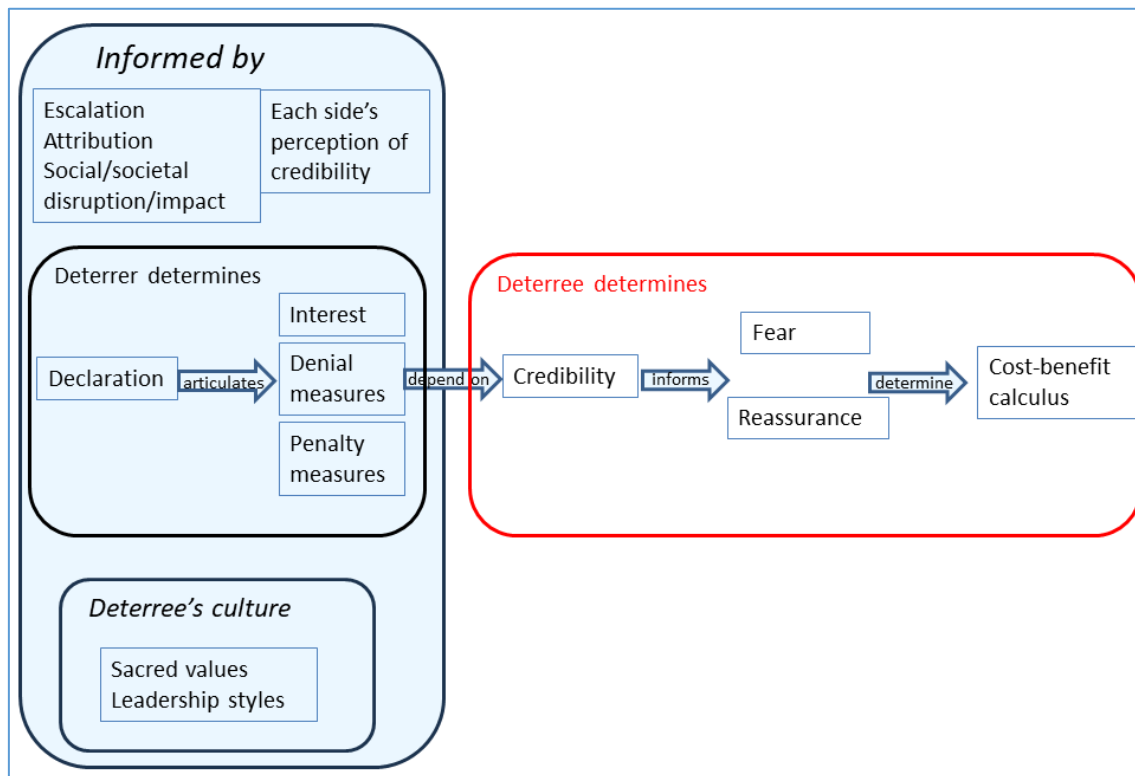


Figure 8-3: Factors for deterrer consideration to inform their viewpoint in line with Goodman's 8 elements of deterrence

8.12 Chapter summary

This chapter has confirmed the definitions of cyberspace and deterrence identified in the literature review together with the broader view of a multi-domain approach to deterrence in cyberspace. It does, however, recognise that this aligns with the UK bias of the research and that future research might explore other states' definitions and whether the findings of the research were more widely applicable.

The chapter explored each of the factors determined most relevant in the questionnaire and considered in the interviews. Escalation, as an articulation of the security dilemma, was found to be an issue in cyberspace although it seems

at present to be confined within the cyber domain. While credibility as perceived by the deterree was recognised as difficult to measure, strategic declarations and other publicly available statements were helpful. The apparent difficulty of attribution was perceived as favouring an offensive strategy, and neither public or private attribution could be guaranteed. However, the absence of attribution was also related to the aspiration of some states to be seen as responsible cyber powers, as was the need to maintain consistency of one's own stated stance with the perceptions of external states. A similar focus also applied to the potential ethical issues regarding impact on the services and economy of the other state.

While the literature review recognised the importance of culture, as did the interviews, deterrence literature tended to ignore this and focus instead on the cost-benefit calculus. This seemed likely to result from the difficulty of articulating culture, which was clear from the exploration of the WVS (2022) in the interviews. Finding a way to articulate culture was seen as important, and key to effective deterrence planning.

Deterrence is a dialogue between two parties, and empathy was seen to be a key factor in reducing cognitive bias on the part of the deterrer. While this was recognised as difficult for many, it was considered worth the effort to give deterrence messaging the best chance of success through understanding the deterree's viewpoint.

The chapter ended with reflection upon the approach taken in the research and a final development of the conceptual framework taking forward the work begun in Chapter 3. This concluded the research addressing RQ1: "What is meant by deterrence in cyberspace?" and RQ2: "What are the main factors relevant to the interplay between the deterrer and deterree?" The next chapter explores the creation of a framework to assist decision makers planning deterrence in cyberspace as the final part of the response to RQ3: "How can these factors be included in deterrence planning for deterrence in cyberspace?"

9 Developing a Framework

9.1 Chapter overview

This chapter explores the creation of a framework to help those planning a potential cyber activity to understand their own situation and that of the potential target. It follows the identification in the research of relevant factors and addresses the research question:

RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

After an introduction summarising the relevant findings from the literature review, the purpose of a framework is considered, followed by a description of how the framework was developed, including an outline of its content, and the format used. Finally, the review of the framework is described.

9.2 Introduction

The overall research question addressed the wider context of the deterrer and deterree when planning deterrence in cyberspace, and a goal was to develop, if possible, a model or framework to help in planning. The exploration of relevant factors in the research suggested that these offered a good starting point. A number of models which might offer approaches were considered in the literature review, but while some offered promising features, all were in some way inadequate.

Snyder (1961) took a very clear and straightforward approach to what was, essentially, a straightforward problem in the context of bipolar nuclear deterrence in the Cold War, although it is not transferable to cyberspace. Straub's (2019) model was likewise simple but limited in scope and lacked detail necessary for its practical use. A mathematical approach to cost/benefit analysis was also taken by Lindsay (2015), but this was necessarily focused solely on economic factors and on a single event. While Healey and Jenkins (2019) counted incidents and their type, this was retrospective and could not be used to determine whether deterrence would be effective.

In contrast, Sharp (2017) introduced factors to measure the credibility and persuasiveness of a cyber threat. The factors were very one-sided and are binary in their scoring, although some were used to inform this research. Another model focusing on the deterrer's viewpoint was Halas (2019), which attempted to use Boolean logic to explain whether a lack of action was because of deterrence or lack of adversary interest or opportunity. Both Sharp (2017) and Halas (2019), thus missed the vital element of the deterree's perception. Edwards et al. (2017) in their "Blame Game" also took a mathematical and logic approach, this time represented graphically in a game tree, but this was focused on attribution and, like others, on a single event rather than the wider context. While the "Blame Game" modelled two parties, interaction was limited to the victim's decision whether to blame to attacker. Bargaining theory (Powell, 2002) is focused on that interaction, but handling anything more than a simple case would be very complex and issues about declaring capability, together with the speed and nature of activity in cyberspace, may make it less useful there.

A comprehensive approach of exploring different aspects of cyber power was offered by the Belfer Center's National Cyber Power Index (Voo et al., 2022) using league tables for each aspect as well as a combined scoring. While this appeared well-researched and transparent, the details of the scores and how they were reached was not clear.

Wider factors including personality and emotion were at least mentioned, although only as limiting factors that had not been addressed, by Cui et al. (2017) in their "three player" game, which was actually one player so that interaction could not be explored. The value of the game is therefore limited. Emotion was, however, recognised by McDermott (2019) in her taxonomy of conditions, emotions and responses, as was the unique personality of individual actors. While her very brief taxonomy did not align with the focus of this research it is notable for acknowledging that threats such as election meddling, the emotions they generate and the response of the recipient can be considered in psychological terms.

While Valeriano and Maness (2015) described a taxonomy to describe cyber incidents and disputes, it defined interactions crudely in terms of their effect (nuisance, defensive or offensive) and so did not help to identify factors relevant to deterrence. The taxonomy of cyber harms from Agraftotis et al. (2018), on the other hand, although rooted in criminology rather than state threats, offered broad themes and broke these down into sub-types, some of which were used to inform this research.

As noted in the literature review, none of the models explored addressed culture, and only McDermott (2019) acknowledged the viewpoint of the other party. If a model or framework is to be produced to help those involved in planning cyber activities to understand their own situation and that of the potential target then it needs to consider both cultural factors and seek to understand the deterree's, as well as the deterrer's, viewpoint.

9.3 Purpose of framework

The first issue to be determined before developing a model or framework is its purpose. No model can provide a definitive answer as to whether deterrence will or will not work because of the dependencies on perception and the deterree's understanding of the deterrence declaration. It might, however, be able to advise on the *likelihood* of deterrence working. While the literature review suggested that a definitive answer might have been easier to determine in a simpler bipolar nuclear standoff (as put forward by Snyder, 1961), it is not feasible in a multipolar cyberspace environment, despite the well-considered proposed approach of Lindsay (2015). Lindsay's paper has much to commend it: it is bold, well-researched and well-argued, and often cited. Yet it has not influenced other work greatly, nor has it been developed in Lindsay's later work. Its simplicity is attractive but it fails to recognise the wider context within which cyber activity takes place.

The research conducted in the present study bore out that view. No absolutes have been established, and when asked about whether a factor was likely to have a positive or negative influence on their state, most interviewees explicitly used the words "it depends" and those who did not made clear that this was their view.

Even where factors were seen as positive or negative, this was almost always qualified as “generally.”

Developing a simple model which lists variables and determines whether deterrence is likely to occur (essentially an if x then y statement) was therefore not feasible, because there are too many uncontrollable (and often unknown) variables. It would be more appropriate to create a framework to highlight specific factors so that information could be elicited about them to inform discussions and decisions. In many ways this was what one of the groups in the workshop (group B) was trying to do but, rather than the strong alignment with traditional military planning activities used by both workshop groups, factors more relevant to activity in cyberspace should be applied.

The term framework (as opposed to model) is deemed appropriate in order to indicate that it is an aid to inform rather than being a tool that delivers a definitive answer. This term is used throughout this chapter.

9.4 Structure of the framework

The five factors highlighted in the research (escalation, credibility, attribution, external perception, and the other party’s services and economy) together with cultural factors were used as the basis for the framework. The key issue to be drawn out of each was considered from the research findings, and a set of questions which could be used during the planning process was developed.

Simplicity was considered important. Those involved in the planning process have many things to consider and the benefit of a framework must be offset by the effort required to use it. While a lengthy and complex process might be feasible if it could produce a categorical answer, that is not the case where the purpose is to gather thoughts to inform discussions, which are still needed to help arrive at decisions. A short and simple set of questions was therefore developed using the relevant factors.

The following sections outline the questions and the rationale behind them. The questions are captured in the framework for planning (Appendix H) as a document that can be given to those planning cyber activities to highlight factors

for consideration. The questions are therefore deliberately posed in the first person to ask about "we" or "our state" and "the other party" in order to ensure engagement and to seek considered and meaningful responses.

9.4.1 Escalation

Before embarking on any action, a decision needs to be taken as to how willing one is to escalate the situation. Greater caution will be needed in setting direction if one is not willing to escalate, and if escalation is likely then a clear exit strategy will be needed. For both parties this would involve stepping back without appearing weak and damaging credibility, whether against the other party or more generally, and it should be recognised that maintaining the status quo may require giving the deterree a face-saving way out of the situation.

A simple Likert scale was proposed, with scores from 0 (no appetite) to 5 (keen to escalate). This allowed for a greater degree of nuance than a scale of 0-3 would, while avoiding excessive granularity from a more gradual scale (such as 0-9) where unnecessary effort could be expended determining whether one means, for example, 7 or 8.

Other considerations required simple yes/no questions about having a clear exit strategy (if escalation is not completely ruled out) and a face-saving way out for the other party's leadership.

Questions:

- How willing are we to escalate the situation? Likert scale 0 (no appetite) to 5 (keen to escalate)
- If score ≥ 2 then do we have a clear exit strategy? Yes / No / N/A
- Does the other party's leadership need a face-saving exit strategy? Yes / No

9.4.2 Credibility

As was discussed in the literature review and during the interviews, credibility is hard to measure as it is the other party's view of one's credibility, rather than one's own, that matters. Credibility is closely linked with capability, but that capability

must be perceived and believed by the other party. An objective approach to measuring capability was offered by the National Cyber Power Index (Voo et al., 2022), which gave listings against eight criteria for each of thirty nation states, as well as individual breakdowns, which are shown in the framework at Appendix H.

What matters in this question is the relative position of the two parties, one's own and the other party. If the nation state that is ranked fifteenth in the table is looking to deter the state ranked twenty fifth, that will probably be more convincing than if the same state is trying to deter the state ranked fifth.

Although this question seeks the overall score for cyber power, it may be deemed more appropriate to focus on scores for individual criteria as described in Appendix H.

Question:

- What are the relative positions of our state and the other party in the National Cyber Power Index (Voo et al., 2022)?

9.4.3 Attribution

This question addresses the appetite for one's action to be attributed by the other party (or for public attribution to be made by a third party). While attribution may be public or private, so either made widely known or recognised but not openly admitted by the deterree, the decision to make attribution public lies with the other party and so it is not appropriate to try to take this into account in a simple framework such as is proposed here. Hence the question is a simple one about the desirability of attribution against a very simple scale which recognises that attribution may be desirable in some circumstances but not in others.

Question:

- Do we wish our action to be attributed to us?
Definite wish not to be attributed / Preference not to be attributed /
Preference to be attributed / Definite wish to be attributed

9.4.4 External Perception

While the focus of this factor in the research was external stakeholders, particularly allies of the other state and neutral states, the focus for the framework is the other party, i.e. the potential deterree. Both the literature review (Heuer, 1999, p7) and the interview findings made clear that understanding the other's view is not trivial. As one interviewee commented, "getting in the mind of the other" and not seeing through one's own lens was vital but very difficult (interviewee 0F-07).

The other party's perception of one's capability and intent can be difficult to measure. What can be measured, however, is the ready availability of information to them, including published strategies and statements, media reporting of previous declarations, activities and exercises, and attribution of cyber activity to a state by other parties, whether one has acknowledged these or not. Tools such as the National Cyber Power Index (Voo et al., 2022) are also available to support the other party's perception, although this is not included here as it has already been included under credibility.

The coherence of these different types of information is important, too. Do they complement each other to form a consistent picture, or do they portray a difference between claims and evidence, for example claims to have undertaken offensive cyber operations could be undermined if there were no evidence of a trained cyber force, or if lacklustre performance in exercises had been reported. Rather than using closed questions and an objective score for perception, a more general but honest assessment is needed to understand what information may be available to the other party and how consistent this may be.

Questions:

- What strategies or statements have been published to indicate our capability for cyber operations?
- What has the media reported about our capabilities, including reporting of resources, declarations, previous activities and exercises? Have any comparable cyber activities been attributed to us by credible other parties

(regardless of whether these have been acknowledged by us, or whether we were actually involved)?

- Has our state been openly attributed for cyber activity (even where we have not acknowledged the attribution)?

9.4.5 Other party's services and economy

Questions about adherence to international law and the consistency of activities with strategic statements, such as the UK's desire to be seen as a responsible cyber power which operates in a legal, ethical and responsible way (Great Britain. National Cyber Force, 2023) will already be a part of planning, as was confirmed by some interviewees. These were therefore not covered in the framework, which was intended to supplement existing planning processes.

Instead, a simple question about the impact on citizens in the other state, or indeed more widely, was proposed. While this should also be covered under second- and third-order effects, it was included here for completeness to ensure it was properly covered. If subsequent review shows that it is not needed, then it could be removed.

Question:

- What services belonging to the other party or used by their citizens (or those of other states) would be impacted by our proposed activity? <list>

9.4.6 Cultural factors

Cultural factors cover a broad spectrum, as noted in the interview results, and some of these areas would already form the basis of intelligence (including open source) available to those planning. As with perception, it is important to try to see through the lens of the other party, so understanding their sacred values seemed a sensible start point.

Another area considered worthwhile to explore were the differences in cultural styles of communication, leadership and confrontation between the parties. Meyer's (2014) work on culture in business offered a potential starting point: although these are focused on business executives working with their colleagues

they will reflect wider cultural traits, and so may be valuable at the level of national political leadership. While national leaders may have greater exposure to leaders from other cultures, they (and their advisors) would seem likely to retain the cultural approach within which they have grown up. Although her book contains no evidence of academic rigour beyond her assertions, Meyer (2014) was considered to offer a simple and practical approach for those states listed, with the descriptions of different styles adapted slightly to address a national, rather than business, context. Even where the other party is not listed, the descriptions of the different styles may still be useful.

Questions:

- Do we know what the other party holds as important or non-negotiable? (These may include tangible or intangible assets, sometimes referred to as sacred values, for example, in the UK this might include our democracy.) <list>
- Thinking about who we are dealing with in the other party (its leadership or another group), is there a difference in communication, leadership or confrontational styles that we should take into consideration? Use the charts below to consider the relative positions of our state and the other party.

9.5 Format of the framework

While the format of the framework was less important than the content, it was still a serious subject for consideration. The eleven questions, when listed together, fitted on a single page, which was considered ideal for what was intended to be a simple framework. Two questions, however, referred to charts from Voo et al. (2022) and Meyer (2014) which needed to be made available to users, together with a further set of charts from Voo et al. (2022) which might be helpful. The charts for the two questions could either go in annexes, thus keeping the questions on a single page, or with the relevant questions, thus lengthening the questions but being more convenient for users. It was decided to take the latter approach so that everything was together and users did not have to flit between pages.

The complete framework, Appendix H, includes a short preamble, the eleven questions and the charts. The format choice did not affect the overall length of eight pages, and while this seemed very long for a “simple” framework, the decision to keep the charts with the relevant questions at least makes it user-friendly, and there is no need to go beyond p4 to the annex if one is not concerned with the breakdown of the National Cyber Power Index criteria. The framework was therefore shared for limited initial review in this form.

For convenience, the questions are listed below:

9.5.1 Escalation

1. How willing are we to escalate the situation on a scale of 0 (no appetite) to 5 (keen to escalate)?
2. If the answer to Q1 is ≥ 2 then do we have a clear exit strategy?
3. Does the other party's leadership need a face-saving exit strategy?

9.5.2 Credibility

4. What are the relative positions of our state and the other party in the cyber power overall ranking?

9.5.3 Attribution

5. Do we wish our action to be attributed to us?

9.5.4 External perception

6. What strategies or statements have been published to indicate our capability for cyber operations?
7. What has the media reported about our capabilities, including reporting of resources, declarations, previous activities and exercises? Have any comparable cyber activities been attributed to us by credible other parties (regardless of whether these have been acknowledged by us, or whether we were actually involved)?
8. Has our state been openly attributed for cyber activity (even where we have not acknowledged the attribution)?

9.5.5 Other party's services and economy

9. What services belonging to the other party or used by their citizens (or those of other states) would be impacted by our proposed activity?

9.5.6 Cultural factors

10. Do we know what the other party holds as important or non-negotiable?
11. Thinking about who we are dealing with in the other party (its leadership or another group), is there a difference in communication, leadership or confrontational styles that we should take into consideration?

9.6 Review of the framework

The framework was shared as an initial draft with three interviewees with particularly relevant expertise, who were invited to review it and comment on whether it would be suitable to fulfil its intended role as an aid to inform discussions and decisions. Two responded: 04-37, a planner with no cyber background, and 02-25, who was able to draw on their background of working with planners in the context of cyber activities. This was intended as an initial review, as a full review was outside the scope of this research, but a wider review and testing of the framework is planned as part of the next steps following the research, as noted in Chapter 10, Conclusions and Future Work.

9.6.1 Escalation

While both respondents made general comments, they addressed only questions 1-3 in detail, drawing out complementary points. 04-37 proposed focusing on the "effect we are wanting to achieve" and beginning each of the three questions with "With regard to the desired effect ..." They also note, however, that "Perhaps we don't know what effect we want to achieve yet and analysis will get us there, therefore we might have to revisit these questions."

02-25 found questions 1-3 "quite 'heavy' and load bearing", and they wondered whether these questions would be more appropriate at campaign level rather than for single operations. At campaign level, they observed, there would be other

activities outside cyberspace. These comments articulated the same tension that 04-37 had noted between the specific effect and not knowing it.

These points are valid. The escalation questions are intentionally deep and would work best at campaign level rather than for a specific effect. The framework is intended to spark and inform discussion, so while the situation will be known the detail of the intended effect (as opposed to its purpose) may not be and will be influenced by that discussion. Escalation is a strategic issue and should be determined generally, rather than about a specific effect, and the answers to questions 1-3 will have a bearing on the particular approach to be taken. At that tactical level, where the effect is already determined, then 04-37's proposal to revisit these questions might be appropriate, but this could be part of the discussion rather than a conscious return to the framework questions.

9.6.2 Other feedback

While some questions, such as questions 1-3, were clearly aimed at the strategic level, 02-25 observed that others were tactical, in particular questions 5, 9 and 11. Question 5 (attribution) is an important factor for cyber activity and should be considered when determining any particular action. The overall desirability of attribution will inform a strategic discussion, but perhaps the question could make the generic nature clearer by referring to any action taken in cyberspace. Question 9 (other party's services and economy) does depend on the tactical activity being determined, and this might not be an appropriate question, or could perhaps be modified in a similar way to that suggested for question 5. Question 11 (cultural factors) would surely still apply above the tactical as the campaign as a whole would have a specific focus. This may, however, need review after future research into the framework.

04-37 asked whether legal frameworks might be an additional factor to consider. These were specifically excluded, as noted above in the section on the development of the framework's structure. The introductory preamble to the framework also stated that there were other relevant factors which were also part of the planning process which were already well served, and specifically

referenced adherence to international law. This wording could, however, be clearer.

In terms of general question style, 04-37 suggested adding a short explanation for the questions and headers as to why they were important to answer. While they expressed concern that the answers to many of the questions were context-specific, in terms of whether or not the intended activity was part of a wider plan of activity with cyber being complementary, they noted that this might be more apparent in a real situation rather than from reviewing a standalone document. 04-37 also proposed using 'why?' and 'so what?' questions, and perhaps modifying some questions to do that in order to prevent the output being "just a list of facts with no analysis." While this seems on the face of it a good idea, it rather misses the point that the output is intended to be a set of statements to clarify thoughts and shape discussion, and the 'why?' and 'so what?' would be addressed in determining the answer to the questions as well as in the following discussion. That said, some prompts to make this explicit could be useful.

Turning to the framework's purpose, 04-37 thought that a framework was a useful planning tool and recognised that a key aim was to identify knowledge gaps, "to understand what we don't know. Identifying and answering these can assure the executive authority that sufficient analysis has been done before giving approval." This comment demonstrated that the framework was successful in its intent, although more in terms of articulating the unarticulated through asking about it than identifying actual knowledge gaps. It does, therefore, seem to be a worthwhile start point for further development.

Finally, both respondents commented on deterrence. As a non-SME in cyber, 04-37 struggled to understand the link between deterrence and escalation. 02-25 reflected that deterrence was not strongly considered as an option, partly because attribution is not wanted in covert activity (and so not available in messaging), and partly because, while the UK wishes to appear credible as a hard target, planners cannot do much to influence that. These points reflect the separation of deterrence from other activity and how it can be supported by that other activity. A future iteration of the framework could make it clearer that

escalation was included to inform consideration of how a wish to actively avoid it might impact on one's actions.

9.6.3 Summary

The framework received constructive criticism, as expected, but it appears to be a valid approach. While generalisations cannot be made from two responses, and it would be premature to act on the suggestions made, reflecting on the framework alongside the comments does suggest that focusing at the strategic or campaign level is appropriate, together with a minor change to question 5 to: Do we wish any action we might take in cyberspace to be attributed to us?

Whether question 9 should remain is a more interesting issue. The question reflects a key point from the research which would be important in any discussion about proportionality and legality. It is, however, concerned with the tactical level so does not fit well with the other questions. As proportionality and legality would always be considered in planning, there seems no reason to retain the question here. While this would remove one of the factors identified in the research, it would be in keeping with from the intent to supplement, rather than repeat, the existing planning process. An alternative question might address the state's dependence on cyberspace, using the "Growing National Cyber and Commercial Technology Competence" from the National Cyber Power Index (Voo et al., 2022, and provided on p7 of the framework), but this is already contributing to the overall position for credibility in question 4. What, if anything, to replace question 9 with would be a useful area to explore in further research and development of the framework.

Following this initial review, the framework needs to be circulated for wider review and tested by use in a practical context. Minor amendments as discussed above could take place at this stage, as reflection on the framework has highlighted some of the issues found by the reviewers, but it is anticipated that thorough review will lead to a more developed and useful framework.

9.7 Chapter summary

This chapter began by reviewing the models and frameworks identified during the literature review. All had limitations, although two had informed the initial creation of a list of candidate factors for use in this research. None had addressed culture, and only one considered the viewpoint of the other party, both of which were deemed, following the research, to be essential for planning for deterrence in cyberspace.

The purpose of the proposed framework was explored before its design was described. It was sent out for an initial review and the two responses received were discussed, together with potential amendments to address them. Overall, the framework seems to be a valid approach, although generalisations cannot be made against only two responses and further review and practical testing is required.

The conclusions from this chapter are taken forward to the Conclusions and Future Work chapter.

10 Conclusions and Future Work

10.1 Chapter overview

This chapter begins by reflecting on the research and how well the novel approach of addressing perception and the wider context has answered the research question. It draws together the different elements of the research, listing a number of conclusions that can be drawn and critically reflecting on the degree to which the research has been limited by its Western bias and theoretical nature, as well as reflecting on the critical realist research philosophy used. Overall, it finds that the research has made a striking and worthwhile contribution to knowledge and theory. Finally, the chapter, and thesis, ends by offering some recommendations for practice and several suggestions for future work to build on the results of the research.

10.2 Review of objective and Research Questions

The aim of the research was to understand the application of the wider context of deterrence in cyberspace with respect to the two parties involved, the deterrer and the deterree. This led to the research question: How can the wider context of the deterrer and deterree be addressed when planning deterrence in cyberspace?

This overarching research question was broken down into the following sub-questions:

- RQ1: What is meant by deterrence in cyberspace?
- RQ2: What are the main factors relevant to the interplay between the deterrer and deterree?
- RQ3: How can these factors be included in deterrence planning for deterrence in cyberspace?

RQ1 was principally answered by the literature review, supplemented by the interviews. The research adopted the UK MOD definition of cyberspace (Great Britain. Ministry of Defence, 2022, p7) and the terminology of ‘deterrence in cyberspace’ (rather than ‘cyber deterrence’) avoided the potential confusion in

much of the literature, which focused on deterring cyber with cyber while purporting to take a wider meaning. While some of the research (the scenario used in the questionnaire and in the group workshop) suggested a cyber-on-cyber situation, it was clear from the interviews that wider aspects of DIME would, in reality, always be considered and that deterrence in cyberspace formed part of a multi-domain approach using cyber activities.

Cyberspace is but one of the operational domains, and it needs to be addressed alongside all the levers of DIME, including other military operational domains, and not in isolation. Deterrence in cyberspace is rightly and sensibly no longer forced into the mould of nuclear deterrence, but has also lost much of the academic interest it held in the period before 2016 (Smeets, 2020). This could be ascribed to its being recognised as part of the wider operational picture and not as a special case, as nuclear was in the Cold War. As an operational domain, however, cyberspace is still an environment where effective deterrence can take place, as with the other domains of maritime, land, air and space.

Deterrence in cyberspace therefore includes both deterrence *of* and deterrence *using* cyber activity. As noted in the Discussion in Chapter 8, this ranges from physical effects on networks to loss of confidentiality or integrity of information, and also impact on the perceptions, interactions and behaviours of individuals. This recognises its relationship with other strategic levers, including DIME and other military operational domains, and aligns with the final definition of deterrence in cyberspace set out at the end of the Review of Literature chapter:

Deterrence in cyberspace seeks to prevent an action through fear of the consequences, using cyber activities as part of the full range of levers including conventional and DIME measures.

RQ2 built on Goodman's (2010) work by identifying candidate factors and using the research to determine those most relevant to the interplay between the parties, specifically focused on how the deterrer can influence the deterree. The initial candidate factors are listed in Chapter 3, the Conceptual Framework, at Figure 3-6, and the questionnaire narrowed this down to five factors, as discussed in Chapter 5. The interviews confirmed the initial assessment from the

questionnaire, exploring the rationale behind the factors, making minor adjustments to the focus of some, and adding an appreciation of the different cultures of the parties, which is recognised as an important issue in some of the literature but has not been taken forward in practical terms.

The final list of factors is therefore: escalation, credibility, attribution, deterree's perception, social/societal impact on the deterree's state and cultural factors, as illustrated at Figure 8-2 and further discussed in the Conclusions section below in this chapter. The research explored how these factors could be used in planning deterrence activities in cyberspace (RQ3), and the group workshop in particular indicated that, even after a lecture which might have prompted consideration of wider factors, planning was seen very much in the way it would have been for kinetic activity. This led to the creation of a framework, as outlined in Chapter 9, Developing a Framework, in order to highlight relevant points for the deterrer to consider and thus inform the planning process, not as a solution of itself but as a support for discussion.

The research thus answered the overall research question, and therefore the objective of the research, to determine the set of factors most relevant to the interplay of the two parties, and to demonstrate how these factors can be brought into the deterrer's planning process to enable them to better target their deterrence activity with the specific deterree and situation in mind. It did this by providing an approach, discussed in Chapter 8 and implemented in Chapter 9, for the deterrer to take into account both their own and the deterree's wider context in their planning activities. This offers a radically new angle to that already addressed in deterrence literature by addressing the interplay between the parties and the cultural context, as well as by creating a framework to inform discussion of options and subsequent decision making.

10.3 Conclusions drawn

10.3.1 The role of perception

Perception has long been recognised as a key issue, as noted in the literature, particularly in terms of avoiding misperception. Cyberspace brings fresh

challenges as it can offer a degree of anonymity and deniability, but these are unlikely to be useful for deterrence. Where deterrence is required it is particularly important to consider how other parties, particularly the deterree, will view actions to ensure that the deterrer sends the right messages so that the deterree receives them as intended. Recognition of the cyber security dilemma and clarity about intentions are needed to prevent espionage or relatively minor signalling activity from being misinterpreted as overly aggressive action. This is not easy, but it can support deterrence and avoid unwanted escalation. Ironically, as noted by one of the interviewees, it may be the case that focusing on cyberspace as an operational domain is not helpful because it reinforces standard military approaches which may not be appropriate in cyberspace. The difficulty of distinguishing between espionage and penetration to support offensive activity (Buchanan, 2016, p27), together with the need for robust network defence, require a broader viewpoint as they do not align well with approaches in the physical domains.

10.3.2 Factors relevant to deterrence in cyberspace

This research has identified the factors especially relevant to deterrence in cyberspace as:

- Escalation
- Credibility
- Attribution
- Deterree's perception
- Social/societal impact on the deterree's state.

Each is discussed below. Cultural differences will be addressed separately.

Escalation within cyberspace can be considered in terms of widening the scope of affected systems or users, and should be considered in planning. While some authors see cyber activity as potentially de-escalatory signalling, this can be risky in that it requires the other party (the deterree) to see it that way. Although there is no evidence of escalation from cyber activity to other domains, it has been successfully used for disruption, as noted by Fallon (2016) and Fleming (2018).

Credibility is recognised, both in the literature and by the research, as a key element in deterrence. Within cyberspace, credibility can be achieved through public statements and strategies backed up by claimed and attributed activity. This requires openness not only about plans and capabilities, but also about achievements, which goes against some of the early focus on covertness. Credibility is relative (credible against the other party) rather than absolute, but it depends upon the other party's viewpoint and so its communication must be clear and unambiguous while avoiding being seen as overly aggressive.

Attribution of one's own cyber activities is possibly undervalued by many. Some interviewees noted that attribution was often considered as undesirable, but attribution of successful activity can be positive for credibility. Like credibility, attribution is in the gift of other parties, particularly but not exclusively the deterree. Although attribution or its absence cannot therefore be guaranteed, the deterrer should consider their preference to be attributed or not when planning any activity in cyberspace, as promoted in the Framework. This applies to both private and public attribution. Depending on the circumstances, covertness or noisiness may be appropriate, including claiming responsibility. If attribution is likely, whether sought or claimed, this research shows that appropriate messaging needs to be in place to prevent or counter being portrayed as the aggressor in the situation.

How other states perceive a state's actions will depend on their relationship with that state, which will also be heavily influenced by their cultural values. For a state such as the UK, which is keen to appear as a responsible cyber power observing international law, its image and standing on the international stage are important, and it will judge others from that perspective. Others, however, may see the situation differently, and that needs to be recognised. For deterrence specifically, perception of credibility will be influenced by the available information about the state in question, and can be moulded to some extent by published strategy and media statements, which is why their use is proposed in the Framework developed in Chapter 9. Perception is, however, in the eye of the beholder, and while the deterrer can try to influence they cannot guarantee their message will

be received as intended, or that wider messages and actions, including inaction, will be seen and interpreted by others. States thus need their actions to be consistent with their stated strategy and the image they wish to portray.

Impact on the other state, like attribution, needs to be carefully considered to avoid being portrayed as the aggressor by the deterree. Any impact on civilians rightly presents an ethical dilemma for a state such as the UK which is keen to maintain its reputation as a responsible cyber power while also recognising the need for effective messaging through its actions. Other states, however, may not share such ethical scruples. While International Humanitarian Law forbids the targeting of civilians (a point emphasised by one interviewee and supported by others) activity in cyberspace is likely to cause disruption or discomfort rather than actual harm so is likely to be legal. Such impact may, however, give the deterree an opportunity to use it as a reason to respond (or escalate) and in many cases will be seen by their citizens as aggression rather than undermining their leadership, as with the lack of success of attempts to break the will of the German population by bombing in the Second World War (Quester, 1986, p154; Grayling, 2006, p86-7). That is not to say that disruption of the services or economy of the deterree may never be appropriate, but that the ethical implications need to be considered alongside its reception by the deterree.

10.3.3 Models

None of the models identified in the literature review addressed cultural issues, or even the context of a situation. Activity was seen in isolation and not in terms of developments over time - in other words not as a situation with a past and a future as well as a present. This made for clearly articulated and simple models, but not for a realistic and effective model of deterrence.

The reality is that deterrence cannot be easily modelled outside Snyder's (1961) simple and straightforward Cold War nuclear calculation. The existential threat presented by nuclear weapons lent itself to that simple approach in a way that cyberspace activity (and probably other operational domains) does not, because the wider context, including the historical and cultural relationships between the parties, are part of the equation and cannot be ignored. This adds a layer of

complexity which is hard to model. There are no silver bullets to determine whether deterrence will be effective. There is no simple 'if x then y' calculation, and there never can be without oversimplification which ignores the context – and which cannot, therefore, provide a full description.

This research sought to resolve this difficulty by introducing the wider context into planning through identifying relevant factors for consideration and implementing these through a framework. While this cannot definitively determine whether deterrence will be effective, it does offer the best opportunity for planning effective deterrence.

10.3.4 Cultural issues

The unifying element in all these factors is the culture of the deterree and how that affects their perception of the situation. This in turn is impacted by the deterrer's appreciation of the deterree's culture and viewpoint. The Review of Literature highlighted the importance of cultural factors, and this was reinforced by the interviews.

Yet there is no clear or practical approach to addressing cultural factors, and the work of Hofstede (2011) and the WVS (2022) do not lend themselves to application for deterrence. Understanding the different approaches to leadership, communication and confrontation, as described by Meyer (2014) and suggested in the proposed framework, should help in determining how the other party may receive the message.

What is most needed is empathy, implied by Davis (2015, p330-1) and Kennedy (1968), and noted in its absence by Owen and Ludlow (2017). Empathy does not mean "going native" or over-sympathising with an adversary, but simply trying to see the situation from their perspective so that one can tailor one's own activity to have the best possible chance of success. Writing the "other side" of the scenario to think through the original research plan was a valuable lesson which could be repeated in a real situation. It will not be easy but could best be supported by an intelligence team focused on that state using open source

material. While much open source material may appear to contain over-egged rhetoric it will include fundamental truth about the views of the other state.

Potentially harder, though, may be finding a senior person who is willing to acknowledge that it may contain the truth as the other state sees it. People tend, as noted in the literature review, to favour information that supports, rather than contradicts, their initial view, so taking on board a contrary viewpoint is not easy. While this does not apply only to seniors, getting them to acknowledge the value of empathy would allow its broader use. If it could be done, however, it would present a real opportunity to tune one's own messaging and action to get the best outcome.

10.3.5 Framework

Seeking an empathetic understanding of the deterree is probably too difficult for many, so the framework was developed as a tool to highlight relevant points for the deterrer to consider. It was not intended to provide a simple answer but to provoke meaningful discussion.

From the limited review of the Framework thus far, it appears a reasonable approach, although some change seems likely to keep it focused at a strategic level. Further review is needed, followed by an opportunity to test it as a practical tool, and the Framework in Chapter 9 indicates some areas to consider for amendment. The underlying approach of seeking to gather some general points to aid discussion of options appears sound, as do the use of tools such as the National Cyber Power Index (Voo et al., 2022) and charts taken from Meyer (2014), although whether these offer the best articulation or need further support needs to be reviewed. Although both have limitations (particularly the lack of articulated rigour in Meyer's work) they fulfil the framework's requirement for a focused approach which can be understood and used with minimal explanation. This focus is the main strength of the framework and should be maintained in any changes to specific questions.

10.3.6 Summary of conclusions

In summary, the main conclusions drawn from this research are:

- As an operational domain, cyberspace should be addressed not in isolation, but alongside all elements of DIME, including other military operational domains.
- It is vital for the deterrer to consider the perception of the deterree when planning their deterrence declaration so it can be correctly received and understood. It may also be prudent to take the perceptions of other parties (allies and neutral states) into account.
- Credibility depends upon the deterree's viewpoint, and can be supported by openness about strategy, capabilities and achievements, including self-attribution (claims of action) and public attribution by others.
- Planning needs to take into account the potential for escalation, which might result from the deterree's perception of the deterrence declaration, and public attribution.
- Actions must be consistent with the deterrer's stated strategy and the image they wish to portray on the world stage, including ethical implications.
- Existing models fail to address the wider context of the situation or the cultural factors relating to the parties, but deterrence does not exist in a vacuum and context and culture are important for planning successful deterrence.
- Empathy is vital, but difficult, so the framework was developed as a way to help planners consider the factors and the deterree's culture.

10.4 Critical reflection and limitations of the work

10.4.1 Research question

The research question and its sub-questions have been reviewed earlier in this chapter, but it is sensible to reflect on whether these were the right research questions. The literature review identified the candidate factors, which were narrowed down to a set of key factors by the first stage of the research (the questionnaire) and then explored in greater detail in the interviews. Yet all this was done from the deterrer's viewpoint, although the selection of candidate factors and the analysis were specific about where the deterrer could influence

the deterree. Asking a deterree whether they had taken the factor into account, and whether they believed the deterrer cared about that factor, may have given a different answer. To do this, though, would have been far from straightforward, and likely to be unproductive because, even if senior leaders and decision makers had been willing to discuss examples they might not acknowledge or, indeed, realise that deterrence had taken place, as noted in the Research Methodology in Chapter 4.

The deterree must interpret the deterrer's deterrence declaration, in whatever form it takes, to determine its credibility and their own level of fear and reassurance, putting these together in their own cost-benefit calculation. The material for them to use in this calculation is provided by the deterrer, in their declaration in terms of the interest together with their denial and penalty measures, and supplemented with external context available to the deterree, such as intelligence about the deterrer's capability and previous track record. Much of this context may comprise of open source intelligence influenced by the deterrer, such as their strategy publications and claims of activity. Thus focusing on the deterrer's viewpoint offers valid and useful insight.

The research identified relevant factors and has led to initial thoughts on a framework to enable decision makers to explore these. The research questions and the approach from the deterrer's viewpoint were, therefore, valid, and have provided a practical focus for deterrence planning.

10.4.2 UK bias

As noted in the Research Methodology chapter, this research has been conducted from a Western, and specifically UK, viewpoint. It reflects the definition of cyberspace used by the UK Ministry of Defence, which is in line with that of other Western states but is very different to those of some non-Western states such as Russia and China. This Western bias is also reflected in English-language deterrence literature, most of which originates from the UK or US.

While this UK bias is a limitation, it is largely inevitable in view of the literature and the potential access to questionnaire responses and interviewees. It does

not, however, negate the value of the research, as it offers an approach which could be applied to other cultures (both Western and non-Western) to determine whether it has wider applicability. The important point to note here is that the bias is recognised and accepted as a potential limitation.

10.4.3 Theoretical nature of the research

The theoretical nature of the research might also be considered a limitation, in that it sought the views of participants rather than looking at actual historical instances of deterrence to determine common elements present in or missing from them. To do this usefully would have been difficult, if not impossible, as noted in the Research Methodology in Chapter 4. Real situations may not have been recognised or recorded as deterrence by the participants, and the reasons for apparent deterrence 'success' might not be related to the deterrer's actions. Further, such real examples would be likely to be highly classified and not available for research in a useful timeframe (important because of the relatively novelty of cyberspace as an operational domain). The theoretical approach was, therefore, the only practical way to determine relevant factors.

10.4.4 Empathy

The importance of empathy became clear during the research, as did the difficulty of achieving it. For a researcher it presents an additional problem of participant authenticity. As noted above, not everyone can be empathetic where it involves understanding a viewpoint alien to one's own, and it is difficult for the researcher to know whether this is an accurate representation of the other party's view. Playing out a scenario with participants allocated to different sides was considered, but without participants from another culture representative of potential deterrees this would be likely to encourage the deterree being represented either as similar to the deterrer or as a play-acted version of how the participant thought the deterree might react. Either would be flawed: the former would fail to recognise the perception of cultural difference, as it would not be needed, while the latter would lack participant authenticity and be devalued accordingly. Indeed, such an approach was considered but was discounted as not able to deliver the value of the explorative research conducted.

Studying empathy, therefore, is difficult, and is likely to be unproductive in a study such as this. While it might be possible to explore in retrospect, through asking the deterrer how they thought the deterree would react and then later asking the deterree how they did react, or observing their reactions, this is difficult because deterrence is not always perceived as deterrence by the deterree and there is no absolute causal link between the deterrer's deterrence declaration and the deterree's action. This chimes with the findings of the literature review, which identified instances of empathy occurring or, more commonly, being absent and leading to misperception. Further, to attempt to force empathy in the primary research would potentially have impacted adversely on the quality of the research by straining the willingness and openness of the interviewees.

10.4.5 Critical realism

The final point for reflection is the research philosophy, namely critical realism. The three layers of reality it recognises align well with the different viewpoints of the parties involved in deterrence, as the empirical view will vary between them in terms of how they perceive the actual and the real. It thus offered an appropriate way to explore the factors relevant to deterrence in cyberspace. The three layers align with the deterree's view of the actions intended to deter (the empirical), the actions themselves as carried out by the deterrer (the actual) and the factors relevant to determining the actions, whether consciously considered or not (the real).

This articulation using the layers of critical realism allows not only the actions carried out by the parties but also the different viewpoints of the two actors to be explored. The factors can be considered as unchanging mechanisms which the actors use to plan and implement their actions. While in many circumstances the different views at the empirical layer do not matter greatly, when the two parties are facing each other in a potential conflict the difference between their views can be very significant. This highlights the importance for the deterrer to consider how the deterree will perceive their actions, and whether or not their perception will lead to the outcome desired by the deterrer. The practical nature of the framework

to help inform the deterrer's planning is entirely in line with the focus of critical realism.

10.5 Contribution to knowledge and theory

The novelty of this research has been in exploring the factors relevant to deterrence in cyberspace, and introducing culture as an underpinning factor in deterrence at a practical level. While previous work has recognised the importance of culture, none has addressed how it can be brought into deterrence planning. While this research has focused specifically on deterrence in cyberspace, it may well be that its findings have wider application to deterrence in other operational domains.

In addition to the comprehensive Review of Literature in Chapter 2, which draws together relevant themes and critically reviews a variety of models relevant to deterrence, the research has made four main contributions to knowledge:

- It has recognised the interplay between the parties.
- It has identified the factors considered most relevant to deterrence in cyberspace and offered an up-to-date conceptualisation of it.
- It has promoted the value of empathy.
- It has developed an initial simple and practical framework to support planning.

While the interplay between the parties in deterrence is implicit in the literature, it is not formally or fully articulated beyond references to bargaining theory. Deterrence is an interplay, and while bargaining theory recognises the to and fro of offer and counter-offer, this does not fully reflect the place-changing between victim (deterrer) and aggressor (deterree) as a situation progresses, and the deterree perceives the deterrer's deterrence declaration as aggression. Recognising this interplay is vital to understanding the deterree's perspective and delivering a deterrence message which is understood and avoids unwanted escalation.

The research identified and discussed the factors considered most important to deterrence in cyberspace, based largely on a series of expert interviews with

those with relevant expertise. In doing this it built on Goodman's (2010) elements of deterrence, adding the wider context and recognising that the deterrer cannot control all of Goodman's elements. The deterree's cost-benefit calculation is under the deterree's determination, and their view of the deterrer's credibility, together with their own fear and reassurance, cannot be directed by the deterrer. To influence the deterree's viewpoint the deterrer must recognise the importance of the difference between their, and the deterree's, cultures. While all these points are variously made in the existing literature, they have not been previously drawn together in a cohesive and practical manner.

Beyond simply acknowledging cultural difference, however, this research recognises and promotes the value of empathy with the deterree's viewpoint. Where empathy is present, as with President Kennedy in the Cuban Missile Crisis (Kennedy, 1968), it presents a powerful tool to help resolve a situation, but where it is not present it can exacerbate the situation, as recognised by Owen and Ludlow (2017). Empathy can allow the deterrer to tailor their approach to best effect, but it can be misunderstood by some as sympathy with the adversary's cause. It is difficult and may be impossible for some, so while promoting empathy this thesis acknowledges that it may not offer a universally acceptable solution.

Finally, and with the limitations of empathy in mind, the thesis proposes an initial version of a simple, practical framework, outlined at Chapter 9 and shown in Appendix H, based on the factors identified in the research, together with culture. This draws together the output of the research to create a useful start point for decision makers to inform their discussions and deliberations. While it needs further work to test and revise, its review thus far has not undermined the concept, and regardless of its success it offers a novel approach that others can learn from and develop.

10.6 Recommendations for policy and practice

Deterrence is a practical issue, so as well as contributing to knowledge this research was intended to have a practical impact. The creation of the framework to inform planning is the most obvious practical feature, but the way deterrence is visualised also has real-world application.

The framework, as noted in Chapter 9, was created as a way to encourage decision makers to consider relevant factors in their deliberations. It moves deterrence from being focused in a simple cost-benefit calculation to a more nuanced exploration of relevant factors, so that these can be recognised and used to inform planning from deterrence in cyberspace. It is therefore recommended that, following further testing and development, the framework is implemented at the start of the deterrence planning process.

Deterrence is a dialogue between the parties, where the deterrer makes their deterrence declaration and the deterree interprets this according to their perception of the situation and of the deterrer. Making the interplay between the two parties explicit, as was shown in the final development of the conceptual framework (at Figure 8-3 in Chapter 8, Discussion of Findings), will enable planners and decision makers to better understand the influences on deterrence. Goodman's (2010) eight elements of cyber deterrence were used as the basis for the definition of deterrence in this research, but by themselves they cannot fully explain deterrence unless they are organised according to which party determines each element. It is therefore recommended that deterrence is explained and visualised in terms of who determines the elements, as well as including relevant factors as shown in Figure 8-3.

While the framework will make a tangible difference to how planners take the relevant factors into account, the articulation of deterrence in terms of the parties' determination of its component elements demonstrates a step change in how deterrence is understood. Not only is this a major contribution to knowledge but it is also a major contribution to policy through broadening deterrence to recognise the role of perception and the influences upon others' perceptions.

10.7 Future work

Several areas for further work have been identified during the research. These address extending the focus of this research into other environments, the articulation of cultural factors and further work on the framework.

As has been noted, this research was conducted from a Western, specifically UK, perspective. Repeating it outside the UK, both in other Western states and beyond the West, would determine whether its results were parochial within a UK context, applied within the West more generally or were indeed valid outside the West. Where appropriate, this could start from the different definitions of cyberspace used within non-Western states, as noted in the Review of Literature in Chapter 2, and how these affect the views of cyber and planning experts.

A second area for future work would explore the articulation of cultural factors. The research has identified the importance of cultural factors and the need for deterrers to take the deterree's culture into account in planning deterrence activities. How this should be done, however, is not clear, and this difficulty may explain why cultural values have not been included in existing models and research. Yet the importance of cultural factors is such that a way is needed to try to assess them, including determining the deterree's sacred values, and to take this assessment into account in planning. The framework proposed the adoption of Meyer's (2014) scales for communication, leadership and confrontational styles as a start point, but while these offer a potential way forward they cannot be rigorously defended academically, and may well not be the best articulation for this purpose. Future work could take a wider view of cultural models, not studied in this research, with a view to identifying the most appropriate model.

The framework, as noted above, appears to offer a sound approach as a concept but needs further development and thorough testing to turn it into a defensible and usable tool which could help to incorporate greater awareness of cyber and its nuances into planning. The review of the framework thus far has been limited, but wider review and further development should turn this into a worthwhile tool for planners and decision makers.

In addition to these three areas identified from the research, the questionnaire respondents identified two proposals which were outside the scope of this research but were worthy of future consideration. The first concerned "The extent to which the cyberspace activities expected to deter are integrated with a full-

spectrum campaign plan, including that cross-domain risk is being managed” (respondent 07-35). Studying cyber activity as part of a cross-domain solution and exploring the optimum approach would be of value.

The other interesting proposal was the “Potential for multiple simultaneous escalations (i.e. polycrisis)” (respondent 18-36). This reflects the real-world environment, where cyber activity and deterrence are unlikely to occur in a vacuum, but will be part of an ongoing hostile relationship of some type which may manifest as a series of events occurring simultaneously. It may also be that more than one threat actor is involved, and deterrence must be more general against a range of threats and threat actors. This creates a dynamic environment very different to any considered in the models reviewed in the Literature Review, adding a layer of complexity recognised in the current research but not specifically addressed by it. While this would be extremely difficult to model because of the number of potential variables and the possible relationships between them, it could explore historic data about cyber attacks to offer insights into escalation and deterrence well beyond those recognised to date.

All these five areas are worthy of future work. Not only would they push the boundaries of previous theory and research, but they would also build upon the insights derived from the research described in this thesis and support practical, as well as academic, application of theory.

10.8 Final thoughts

This research began with an exploration of the meaning of cyber deterrence and the factors that were relevant to it. It quickly became apparent that deterrence depended upon the relationship and perceptions of the two parties, the deterrer and the deterree, and the cultural factors which influenced this relationship and their perceptions of the situation. These, together with the wider activity which has occurred before the immediate situation, provide the context for the situation, and the research has sought to keep this context in mind throughout. This is not easy, as is evidenced by the absence of it from the models reviewed in the literature review, but it does reflect reality, where deterrence is not simply the response to a specific threat but is part of a bigger story with a past and a future.

These may not be easy to identify, even in retrospect and particularly not at the point where the deterrence occurs, but successful deterrence must recognise the bigger story, making use of the past and attempting to influence the future.

Fundamentally, deterrence needs the deterrer's communication to be accurately received by the deterree. This encompasses all the different elements of that communication, including the credibility of the deterrence measures and addressing the other elements put forward by Goodman (2010). What matters, though, is that it is received by the deterree in the way intended by the deterrer. For this, the deterrer must consider it from the point of view of the deterree and try to anticipate the deterree's perceptions.

References

- Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S. and Upton, D. (2018) 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*, vol 4 no 1, pp1-15.
- Bar, S. (2011) 'Gods, nations, and deterrence: the impact of religion on deterrence', *Comparative Strategy*, vol 30 no 5, pp428-452.
- Barnard-Wills, D. and Ashenden, D. (2012) 'Securing virtual space: cyber war, cyber terror, and risk', *Space and Culture*, vol 15 no 2, pp1-14.
- Bayles, W. (2001) 'The ethics of computer network attack', *Parameters*, Vol 31 No 1 pp44-58.
- Beckerman, C. (2022) 'Is there a cyber security dilemma?', *Journal of Cybersecurity*, vol 8 no 1.
- Berman, J. (2013) 'Utility of a conceptual framework within doctoral study: a researcher's reflections', *Issues in Educational Research*, vol 23 no 1, pp1-18.
- Betz, D. and Stevens, T. (2011) *Cyberspace and the state: toward a strategy for cyber-power*. Abingdon: The International Institute for Strategic Studies.
- Bhaskar, R. (2008, orig 1978) *A realist theory of science*. London: Verso.
- Blaikie, N. (2007) *Approaches to social enquiry, 2nd edition*. Cambridge: Polity Press.
- Bloomfield, A. (2012) 'Time to move on: reconceptualizing the strategic culture debate', *Contemporary Security Policy*, vol 33 pp 437-61.
- Booth, K. and Wheeler, N. (2008) *The security dilemma: fear, cooperation and trust in world politics*. Basingstoke: Palgrave Macmillan.
- Borghard, E. and Lonergan, S. (2023) 'Deterrence by denial in cyberspace', *Journal of Strategic Studies*, vol 46 no 4, pp534-569.

Brodie B. (1959) *Strategy in the missile age*. Princeton NJ: Princeton University Press.

Buchanan, B. (2016) *The cybersecurity dilemma*. London: Hurst & Co.

Bunn, M.Elaine (2007) 'Can deterrence be tailored?', *Strategic Forum* 255. Washington DC: National Defense University Press.

Burton, J. (2018) *Cyber deterrence: a comprehensive approach*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. [online] Available at www.ccdcoe.org Accessed 25 April 2018.

Butterfield, H. (1951) *History and Human Relations*. London: Collins.

Campbell, P. and Donahoo, M. (2024) 'Harnessing the power of cyber defence', *Survival*, vol 66 no 2, pp127-142.

Clausewitz, C. von (2007) *On war*. Translated by Michael Howard and Peter Paret; Abridged with an Introduction and Notes by Beatrice Heuser. Oxford: Oxford University Press.

Cui, J., Rosoff, H. and John, R. (2017) 'Deterrence of cyber attackers in a three-player behavioral game', in Rass, S., An, B., Kiekintveld, C., Fang, F. and Schauer, S. (eds) *Decision and game theory for security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017*. Cham: Springer.

Davis, P. (2015) 'Deterrence, influence, cyber attack, and cyberwar', *International Law and Politics*, vol 47, pp327–355.

Day, J. and Bobeva, M. (2005) 'A generic toolkit for the successful management of Delphi studies', *Electronic Journal of Business Research Methods*, vol 2 no 2, pp103-116.

Denning, D. (2015) 'Rethinking the cyber domain and deterrence', *Joint Force Quarterly*, vol 77, pp8-15.

Dodd L (2019) 'Choice-making and choose-ables: making decision agents more human and choosy', *European Journal on Decision Processes*, vol 7, issue 1–2, pp101–115.

Dorff, R. and Cerami, J. (2000) 'Deterrence and competitive strategies: a new look at an old concept', *Small Wars & Insurgencies*, vol 11 no 2, pp109-123.

Easterby-Smith, M., Thorpe, R. and Jackson, P. (2015) *Management and business research, 5th ed.* London: Sage Publications Ltd.

Edgar, T. and Manz, D. (2017) *Research methods for cyber security*. Cambridge, MA: Elsevier.

Edwards, B., Furnas, A., Forrest, S. and Axelrod, R. (2017) 'Strategic aspects of cyberattack, attribution, and blame', *Proceedings of the National Academy of Sciences of the United States of America*, March 14, vol 114 no 11, pp2825-2830. [online] Available at www.pnas.org. Accessed 10 April 2018.

Elliott, D. (2011) 'Deterring strategic cyberattack', *IEEE Security and Privacy*, Sept/Oct 2011.

Fallon, M. (2016) *Defence Secretary's speech at the second RUSI Cyber Symposium*. Delivered 20 October 2016.

Fischerkeller, M. (2017) 'Incorporating offensive cyber operations into conventional deterrence strategies', *Survival*, vol 59 no 1, pp103-134.

Five Eyes (2019) *Five Eyes Panel on global cyber issues*, at CyberUK, Glasgow, 24 April 2019.

Fleming, J. (2018) *Director GCHQ's speech at CyberUK18*. Delivered 12 April 2018.

Fletcher, A. (2017) 'Applying critical realism in qualitative research: methodology meets method', *International Journal of Social Research Methodology*, vol 20 no 2 pp181-194.

France. Ministère des Armées (2019) *Éléments publics de doctrine militaire de lutte informatique offensive*.

François, D. (2020) *Cyber operations and international law*. Cambridge: Cambridge University Press.

Freedman, L. (2004) *Deterrence*. Cambridge: Polity Press.

Gartzke, E. and Lindsay, J. (2015) 'Weaving tangled webs: offense, defense, and deception in cyberspace', *Security Studies*, vol 24 no 2, pp316-348.

Geers, K. (2010) 'The challenge of cyber attack deterrence', *Computer Law & Security Review*, vol 26, pp 298-303.

Geers, K. (2011) *Strategic cyber security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Giles, K. (2012) 'Russia's public stance on cyberspace issues', in Czosseck, C., Ottis, R. and Ziolkowski, K. (eds) *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

Giles, K. and Hagestad, W. (2013) 'Divided by a common language: cyber definitions in Chinese, Russian and English', in Podins, K., Stinissen, J. and Maybaum, M. (eds) *5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.

Goodman, W. (2010) 'Cyber deterrence: tougher in theory than in practice?', *Strategic Studies Quarterly*, Fall 2010, pp102-135.

Gray, C. (2003) *Maintaining effective deterrence*. Carlisle, PA: Strategic Studies Institute, US Army War College.

Gray, C. (2013) *Making strategic sense of cyber power: why the sky is not falling*. Carlisle, PA: Strategic Studies Institute, US Army War College.

Gray, C. (2023) 'The nature and utility of strategic culture scholarship', in Kartchner, K., Bowen, B. and Johnson, J. (eds) *Routledge Handbook of Strategic Culture*. Oxford: Routledge.

Grayling, A.C. (2006) *Among the dead cities*. London: Bloomsbury.

Great Britain. HM Government (2010) *Securing Britain in an age of uncertainty: the strategic defence and security review*. London: The Stationery Office. Cm 7948.

Great Britain. HM Government (2015) *National security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom*. London: HMSO. Cm 9161.

Great Britain. HM Government (2016) *National cyber security strategy 2016-2021*. London: HMSO.

Great Britain. HM Government (2021) *National cyber strategy 2022: pioneering a cyber future with the whole of the UK*. London: HM Government.

Great Britain. House of Commons Defence Committee (2014) *Deterrence in the twenty-first century: Eleventh Report of Session 2013-14. Volume II Written evidence*. London: The Stationery Office.

Great Britain. House of Lords (2015) *The EU and Russia: before and beyond the crisis in Ukraine - European Union Committee*. [Online] Available at <https://publications.parliament.uk/pa/ld201415/ldselect/lddeucom/115/11510.htm> Accessed 25 September 2024.

Great Britain. Ministry of Defence (2016) *Cyber primer (second edition)*. Development, Concepts and Doctrine Centre.

Great Britain. Ministry of Defence (2018) *Defence in numbers: October 2018*. London: Ministry of Defence.

Great Britain. Ministry of Defence (2019) *Deterrence: the Defence contribution (Joint Doctrine Note 1/19)*. Development, Concepts and Doctrine Centre.

Great Britain. Ministry of Defence (2022) *Cyber primer (3rd edition)*. Development, Concepts and Doctrine Centre.

Great Britain. National Cyber Force (2023) *The National Cyber Force: Responsible cyber power in practice*. [Online] Available at

www.gov.uk/government/organisations/national-cyber-force Accessed 5 April 2023.

Great Britain. National Protective Security Authority (2024) *Critical National Infrastructure*. [Online] Available at <https://www.npsa.gov.uk/critical-national-infrastructure-0> Accessed 1 November 2024.

Guest, G., Bunce, A. and Johnson, L. (2006) 'How many interviews are enough? An experiment with data saturation and variability', *Field Methods*, vol 18, no 1, pp59-62.

Halas, M. (2019) 'Proving a negative: why deterrence does not work in the Baltics', *European Security*, vol 28 no 4, pp431-448.

Harvey, P. (ed) (1937) *The Oxford companion to classical literature*. London: Oxford University Press.

Healey, J. and Jenkins, N. (2019) 'Rough-and-ready: a policy framework to determine if cyber deterrence is working or failing', in Minárik, T., Alatalu, S., Biondi, S., Signoretti, M., Tolga, I. and Visky, G. (eds) *2019 11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications.

Hennessey, S. (2017) 'Deterring cyberattacks: how to reduce vulnerability', *Foreign Affairs*, vol 96 no 6, p39-46.

Herz, J. (1950) *International politics in the atomic age*. New York: Columbia University Press.

Heuer, R. (1999) *Psychology of intelligence analysis*. Washington DC: Central Intelligence Agency. [Online] Available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf>. Accessed 21 June 2020.

Heuser, B. (2010) *The evolution of strategy: thinking war from antiquity to the present*. Cambridge: Cambridge University Press.

Heuser, B. (2023) 'The conceptual heritage of strategic culture and collective mentality', in Kartchner, K., Bowen, B. and Johnson, J. (eds) *Routledge Handbook of Strategic Culture*. Oxford: Routledge.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture, Unit 2*. [online] Available at <http://scholarworks.gvsu.edu/orpc/vol2/iss1/8>. Accessed 9 May 2021."

Howell, K. (2013) *An introduction to the philosophy of methodology*. London: Sage Publications Ltd.

Hughes, J. (1989) 'The origins of World War II in Europe: British deterrence failure and German expansionism', in Rotberg, R. and Rabb, T. (eds) *The origin and prevention of major wars*. Cambridge: Cambridge University Press.

Iasiello, E. (2013) 'Is cyber deterrence an illusory course of action?', *Journal of Strategic Security*, vol 7 no 1, pp 54-67.

Jensen, E. (2012) 'Cyber deterrence', *Emory International Law Review*, vol 26, pp 773-824.

Jervis, J. (1978) 'Cooperation under the security dilemma', *World Politics*, vol 30 no 2, pp167-214.

Jervis, R. (2017) *Perception and misperception in international politics*. Princeton, NJ: Princeton University Press.

Kania, E. (2016) 'Cyber deterrence in times of cyber anarchy - evaluating the divergences in US and Chinese strategic thinking', *CyCon US, International Conference on Cyber Conflict, 21-23 Oct 2016*; Washington DC.

Kant, I. (1983) *Perpetual peace and other essays*. Translated by Ted Humphrey. Indianapolis: Hackett Publishing Co.

Kari, M. and Pynnöniemi, K. (2023) 'Theory of strategic culture: an analytical framework for Russian cyber threat perception'. *Journal of Strategic Studies*, vol 46 no 1, p56-84.

Kartchner, K. (2023) 'Defining and scoping strategic culture: promises, challenges, and conundrums', in Kartchner, K., Bowen, B. and Johnson, J. (eds) *Routledge Handbook of Strategic Culture*. Oxford: Routledge.

Kello, L. (2013) 'The meaning of the cyber revolution: perils to theory and statecraft', *International Security*, vol 38 no 2, pp 7-40.

Kennedy, R. (1968) *13 Days: The Cuban missile crisis October 1962*. London: Macmillan.

Kosseff, J. (2024) 'The international legal framework for Hunt Forward and the case for collective countermeasures', in Kwan, C., Lindström, L., Giovannelli, D., Podiņš, K. and Štrucl, D. (eds) *16th International Conference on Cyber Conflict, CyCon 2024: Over the Horizon*. Tallinn: NATO CCDCOE Publications.

Kugler, R. (2011) 'Deterrence of cyber attacks', in Kramer, F., Starr, S. and Wentz, L. (eds) *Cyberpower and national security*. Washington: National Defense University Press.

Kvale, S. and Brinkmann, S. (2009) *InterViews: learning the craft of qualitative research interviewing*. Los Angeles: Sage.

Lebow, RN and Stein, J. (1989) 'Rational Deterrence Theory: I think, therefore I deter', *World Politics*, vol 41 no 2.

Lebow, RN and Stein, J. (1990) 'Deterrence: the elusive dependent variable', *World Politics*, vol 42 no 3, pp336-369.

Leshem, S. and Trafford, V. (2007) 'Overlooking the conceptual framework', *Innovations in Education and Teaching International*, vol 44 no 1, pp93-105.

Lewis, J. (2022) 'A strategic outlook for cyberspace operations', in Pernik, P. (ed) *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis*. Tallinn: NATO CCD COE Publications.

Libicki, M. (2009) *Cyberdeterrence and cyberwar*. Washington DC: Rand.

Libicki, M. (2012) 'Cyberspace is not a warfighting domain', *I/S: A Journal of Law and Policy for the Information Society*, vol 8 no 2, pp321-336.

Liff, A. (2012) 'Cyberwar: a new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war', *Journal of Strategic Studies*, vol 35 no 3, pp 401-428.

Limnell, J (2013) 'Offensive cyber capabilities are needed because of deterrence' in Rantapelkonen, J and Salminen, M (eds) *The Fog of Cyber Defence*. Helsinki: National Defence University.

Lindsay, J. (2015) 'Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, vol 1 no 1, pp53-67.

Lindsay, J. and Gartzke, E. (2022) 'Politics by many other means: the comparative strategic advantages of operational domains', *Journal of Strategic Studies*, vol 45 no 5, pp743-776.

Lin-Greenberg, E., Pauly, R. and Schneider, J. (2022) 'Wargaming for international relations research', *European Journal of International Relations*, vol 28 no 1 pp 83-109.

Linstone, H. and Turoff, M. (eds) (1975) *The Delphi Method: Techniques and Applications*. [Online] Available at www.researchgate.net. Accessed 16 November 2019.

Lonsdale, D. (2018) 'Warfighting for cyber deterrence: a strategic and moral imperative', *Philosophy & Technology*, vol 31 issue 3, pp409-429.

Lynn-Jones, S. (1995) 'Offense-defense theory and its critics', *Security Studies*, vol 4 no 4, pp660-691.

Maslow, A. (2000) *The Maslow business reader*, ed D. Stephens. New York: John Wiley and Sons, Inc.

Maxwell, S. (1968) *Rationality in deterrence: Adelphi Papers No 50*. London: Institute for Strategic Studies.

Mazanec, B. and Thayer, B. (2015) *Deterring cyber warfare: bolstering strategic stability in cyberspace*. Basingstoke: Palgrave Macmillan.

McDermott, R. (2004) 'The feeling of rationality: the meaning of neuroscientific advances for political science', *Perspectives on Politics*, vol 2 no 4, pp691-706.

McDermott, R. (2019) 'Some emotional considerations in cyber conflict', *Journal of Cyber Policy*, vol 4 no 3, pp309-325.

Meyer, E. (2014) *The culture map*. New York: Public Affairs.

Morgan, P. (2003) *Deterrence now*. Cambridge: Cambridge University Press.

Nakasone, P. (2019) 'A cyber force for persistent operations', *Joint Forces Quarterly*, vol 92, pp10-14.

NATO (2023) *Collective Defence and Article 5*. [online] Available at <https://www.nato.int/cps/en/natohq/topics.htm> Accessed 8 August 2024.

Nye, J. (2011) 'Nuclear lessons for cyber security?', *Strategic Studies Quarterly*, Winter 2011, pp18-38.

Nye, J. (2017) 'Deterrence and dissuasion in cyberspace', *International Security*, vol 41 no 3, pp44-71.

Owen, D. and Ludlow, D. (2017) *British foreign policy after Brexit*. London: Biteback Publishing Ltd.

Oxford English Dictionary (2015) *Oxford Dictionary of English*, 3rd ed. Oxford: Oxford University Press [Online]. Available at www.oxfordreference.com. (Accessed 25 Sep 2018)

Payne, K. (2010) 'The fallacies of Cold War deterrence and a new direction', *Comparative Strategy*, vol 22 no 5, pp411-428.

Payne, K. (2011) 'Understanding deterrence', *Comparative Strategy*, vol 30 no 5, pp393-427.

Powell, R. (2002) 'Bargaining theory and international conflict', *Annual Review of Political Science*, vol 5, pp1-30.

Quester, G. (1986) *Deterrence before Hiroshima*. New Brunswick, NJ: Transaction.

- Rattray, G. (2001) *Strategic warfare in cyberspace*. Cambridge, MA: MIT Press.
- Raud, M. (2016) *China and cyber: attitudes, strategies, organisation*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. [online] Available at www.ccdcoe.org Accessed 18 March 2019.
- Rid, T. (2012) 'Cyber war will not take place', *Journal of Strategic Studies*, vol 35, no 1, pp5–32.
- Robson, C. and McCartan, K. (2016) *Real world research, Fourth edition*. Chichester: John Wiley & Sons Ltd.
- Russian Federation. Ministry of Defence (2011) *Russian Federation Armed Forces' information space activities concept*. [Online] Available at <http://eng.mil.ru>. Accessed 4 October 2018.
- Ryan, N. (2017) 'Five kinds of cyber deterrence', *Philosophy & Technology*, vol 31 no 3, pp331-338.
- Sackman, H. (1974) *Delphi assessment: expert opinion, forecasting, and group process*. Santa Monica, CA: RAND.
- Sample, S. (2000) 'Military buildups: arming and war', in Vasquez, J. (ed) *What do we know about war?* Lanham, Maryland: Rowman & Littlefield.
- Saunders, M., Lewis, P. and Thornhill, A. (2019) *Research methods for business students, Eighth edition*. Harlow: Pearson Education Limited.
- Scheber, T. (2011) 'Evolutionary psychology, cognitive function, and deterrence', *Comparative Strategy*, vol 30 no 5, pp453-480.
- Schechter, B., Schneider, J. and Shaffer, R. (2021) 'Wargaming as a methodology: the international crisis wargame and experimental wargaming', *Simul Gam*, vol 52 pp 513-26.
- Schelling, T. (1960) *The strategy of conflict*. Cambridge, MA: Harvard University Press.
- Schelling, T. (1966) *Arms and influence*. New Haven, CT: Yale University Press.

Sharp, T. (2017) 'Theorizing cyber coercion: the 2014 North Korean operation against Sony', *Journal of Strategic Studies*, vol 40 no 7, pp898-926.

Singer, P. and Friedman, A. (2014) *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: OUP.

Smeets, M. (2020) *Cyber deterrence Is dead. Long live cyber deterrence!* Council on Foreign Relations. [online] Available at www.cfr.org Accessed 24 June 2023.

Snyder, G. (1961) *Deterrence and defense: toward a theory of national security*. Princeton NJ: Princeton University Press.

Snyder, J. (1977) *The Soviet strategic culture: implications for limited nuclear operations*. RAND Research Paper R-2154-AF. Santa Monica, Ca: RAND Corporation.

Solomon, J. (2011) 'Cyberdeterrence between nation-states: plausible strategy or a pipe dream?', *Strategic Studies Quarterly*, Spring 2011, pp1-25.

Stein, J. (2013) 'Psychological explanations of international decision making and collective behaviour', in Carlsnaes, W., Risse, T. and Simmons, B. (eds) *Handbook of International Relations*. London: SAGE Publications Ltd.

Straub, J. (2019) 'Mutual assured destruction in information, influence and cyber warfare: comparing, contrasting and combining relevant scenarios', *Technology in Society*, vol 59.

Tetlock, P. (2005) *Expert political judgement: how good is it? How can we know?* Princeton: Princeton University Press.

Thucydides (1910) *The history of the Peloponnesian War*. Translated by Richard Crawley. London: Dent Dutton.

Tibbs, H. (2013) *The global cyber game: achieving strategic resilience in the global knowledge society*. Shrivenham: Defence Academy of the United Kingdom.

Tikk, E., Kaska, K. and Vihul, L. (2010) *International cyber incidents: legal considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE).

United States. Joint Chiefs of Staff (2018) *Joint Publication 3-12: Cyberspace operations*.

Valeriano, B. and Maness. A. (2015) *Cyber war versus cyber realities: cyber conflict in the international system*. Oxford: Oxford University Press.

Van Evera, S. (1999) *Causes of war: power and the roots of conflict*. New York: Cornell University Press.

Voo, J., Hemani, I. and Cassidy, D. (2022) *National Cyber Power Index 2022*. Cambridge, MA: Belfer Center for Science and International Affairs.

Williams, H. and Blum, I (2018) *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica, CA: RAND.

Williams, L. (2019) *Cyber Command looks to expand* (article dated 12 Feb 2019). [Online] Available at www.fcw.com. Accessed 27 March 2019.

Wilner, A. (2017) 'Cyber deterrence and critical-infrastructure protection: expectation, application, and limitation', *Comparative Strategy*, vol 36 no 4, pp309-318.

WVS (2022) *World Values Survey - Findings and Insights*. [online] Available at www.worldvaluessurvey.org. Accessed 9 October 2023.

WVS wave 7 (2017-2022) Haerpfer, C., Inglehart, R., Moreno, A., Welzel, C., Kizilova, K., Diez-Medrano J., M. Lagos, P. Norris, E. Ponarin & B. Puranen (eds.). 2024. *World Values Survey: Round Seven – Country-Pooled Datafile Version 6.0.0*. Madrid, Spain & Vienna, Austria: JD Systems Institute & WWSA Secretariat. [doi:10.14281/18241.24](https://doi.org/10.14281/18241.24).

Yorke, C. (2023) 'Is empathy a strategic imperative? A review essay', *Journal of Strategic Studies*, vol 46, no 5, pp1082–1102.

Zilincik, S. (2022) 'Technology is awesome, but so what? Exploring the relevance of technologically inspired awe to the construction of military theories', *Journal of Strategic Studies*, vol 45 no 1, pp5-32.

Copyright Permissions

Figure 2-1 by permission from UK Great Britain. Ministry of Defence, contains public sector information licensed under the Open Government Licence v3.0.

Figure 2-3 and figure in Appendix B by permission from World Values Survey Association Secretariat, Vienna, Austria, www.worldvaluessurvey.org.

Figure 2-4 and figures in Appendix H by permission from Erin Meyer (The Culture Map).

Figure 2-5 is reprinted from *Technology in Society*, vol 59, Straub, J. 'Mutual assured destruction in information, influence and cyber warfare: comparing, contrasting and combining relevant scenarios', Article 101177, 2019, with permission from Elsevier.

Figure 2-6 and figures in Appendix H by permission from Belfer Center for Science & International Affairs, Harvard Kennedy School.

Table 2-1 is taken from Halas, M. (2019) 'Proving a negative: why deterrence does not work in the Baltics', *European Security*, vol 28 no 4, pp431-448. © copyright 2019, reprinted by permission of Informa UK Limited, trading as Taylor & Francis Group, <https://www.tandfonline.com>.

Table 2-2 is taken from McDermott, R. (2019) 'Some emotional considerations in cyber conflict', *Journal of Cyber Policy*, vol 4 no 3, pp309-325. © copyright 2019, reprinted by permission of Informa UK Limited, trading as Taylor & Francis Group, <https://www.tandfonline.com>.

Appendix A Questionnaire

Factors in Deterrence

Please read this Consent information before completing the questionnaire

Study title: Addressing the deterree's context when planning deterrence in cyberspace

I am Sharon Wiltshire, employed by MOD and a PhD research student at Cranfield University Defence and Security. I am researching how the deterree's context can be addressed when planning deterrence in cyberspace.

I am inviting those with experience in relevant areas to complete this questionnaire, and up to 2 more similar ones approx. 6 weeks apart, and possibly (if willing) be interviewed. The findings will be anonymised, summarised and analysed for my PhD thesis, which may also include anonymous quotations which will identify participants only by a reference code and their area of expertise. The thesis will be shared with MOD.

All raw and analysed data will be stored on MOD's or Cranfield's secure network, and will only be accessed by myself as Chief Investigator and my Research Supervisors. Personal data is limited to contact details only, and will be collected, stored and processed in accordance with UK Data Protection Legislation.

The questionnaire should take no more than 30 minutes to complete.

You may withdraw from the research at any time without giving a reason, by informing me within two months of any questionnaire or interview. If you do choose to withdraw, you may request that all your input up to that point is destroyed and not used in the analysis and results.

If you have any questions, or would like a fuller version of this information, please contact me at s.wiltshire@cranfield.ac.uk

If you have any complaints, please contact my supervisor, Dr Ken McNaught, at k.r.mcnaught@cranfield.ac.uk

1. **Please confirm that you have read and understand this information, and consent to taking part in this study ***

☐ Yes

2. Your area(s) of experience or study (completed or in progress) *

- ☐ Cyber - technical
- ☐ Cyber - leadership/management (including Cranfield Cyber Masters courses)
- ☐ Military planning
- ☐ Intelligence analysis
- ☐ Understanding different cultures
- ☐ Other

3. Your email address *

4. Your phone number (optional)

5. Please indicate whether you would be willing to be interviewed

- ☐ Yes - face-to-face
- ☐ Yes - MS Teams
- ☐ Yes - by phone

The situation - fictitious example

The states described and the situation are fictitious, but may help you think about the factors in following questions

Your state – deterrer

Liberal democracy, accepting of freedom of speech and media criticism. Strong dependency on internet and other technology in industry, business and society. Critical national infrastructure mainly in private sector, with involvement of international companies. Active player in world affairs, seeking to promote freedom, human rights and peace. Strong and active military capability, with frequent support to coalitions and links with allies. Offensive cyber capability held within military and openly admitted.

Other state – deterree/potential attacker

Authoritarian government in control of elections and intolerant of serious opposition. Some dependency on internet but use is controlled and censored. Even where industries are officially independent of government some level of control is maintained. Has status as a major player in world affairs, with strong military capability concerned with maintaining its status and influence. Offensive cyber capability within military and through proxy organisations; widely suspected of (but denies) interference with other states.

Situation: intelligence suggests an impending potential cyber attack on a CNI asset within your state by the other state (no specific threat has been received, but relations between the two states are not cordial).

Your state is considering activity in cyberspace to deter the other state.

Your role is as an adviser to the leadership of your state, considering the likely effectiveness of this deterrence activity.

6. Did you find the situation presented helpful to focus your thoughts? *

- ☐ Yes
- ☐ No

7. Any comments about the situation or its usefulness?

Relevance of factors to deterrence

Review of the literature on deterrence suggests the following factors may be relevant to deterrence in cyberspace. If you think there are additional factors please add in the text boxes at the end. Then please label which you consider to be the top 5 factors (which may include those you have added) where 1 indicates the most relevant, 2 the second most etc.

8. Review of the literature on deterrence suggests the following factors may be relevant to deterrence in cyberspace. Please indicate up to 5 factors which you consider to be the most relevant. *

Please select at most 5 options.

- ☐ A. Potential use by the other state of any deterrence threat to distract from internal unrest or other political issues
- ☐ B. Other state's willingness to attribute your state for any actions your state may take in cyberspace
- ☐ C. Reassurance to other state that if they do not attack your CN asset then you will not take further action
- ☐ D. Disruption to the daily life activities of the other state
- ☐ E. Worry/anxiety of the leadership and citizens of the other state
- ☐ F. Self-confidence of the leadership of the other state
- ☐ G. Perception of technology by citizens or businesses in the other state
- ☐ H. Impact on the services or economy of the other state
- ☐ I. How external stakeholders (their allies or neutral states) perceive the other state
- ☐ K. Internal morale of the citizens of the other state
- ☐ L. Your state's political reputation as viewed by the other state
- ☐ M. The credibility of your state's proposed action to the other state
- ☐ N. Potential for escalation of the situation

9. Are there any factors not included above that you would include in your top 5?

If so, please list these below and label each (up to 3) as P, Q and R respectively.

10. Using the label letters in question 8, and any you have added at question 9, please indicate which of the factors you have chosen are the 2 most important.

*Example: if you think B, Other state's willingness to attribute and L, Your state's political reputation are the most important, enter B L in the box below. **

11. Any further comments about your choices and their ratings?

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.



Appendix B Interview Script

B.1 Interview consent form

Consent form
Study title: Addressing the deterree's context when planning deterrence in cyberspace
Invitation to take part: Prospective participants are being selected from those with experience in relevant areas such as cyber operations, military doctrine, deterrence and study of other cultures.
What is the purpose of the research? It is intended to determine how the deterree's context can be addressed when planning deterrence in cyberspace.
Who is doing this research? It is being conducted by Sharon Wiltshire as part of my PhD research. Anonymised and summarised findings will be shared with the Ministry of Defence.
Why have I been invited to take part? You have been selected as you have knowledge or experience in relevant areas.
Do I have to take part? No, participation is entirely voluntary.
What will I be asked to do? Take part in an interview. The research will explore the factors relevant to the deterree's context, including societal and political factors, from the point of view of the deterrer. The interview should take 60-90 minutes.
Are there any direct benefits to me of taking part? None, although I would be happy to supply information on the analysis.
What are the possible disadvantages (or risks) of taking part? None.
Can I withdraw from the research and what happens if I withdraw? You may withdraw at any time without giving a reason, by informing me within two months of the interview. If you do choose to withdraw, you may request that all your input up to that point is destroyed and not used in the analysis and results.
Will I receive any expenses or payments? No.
Who do I contact if I have any questions? Sharon Wiltshire, Cranfield University Defence and Security, Shrivenham. Tel [REDACTED] email s.wiltshire@cranfield.ac.uk
Who do I contact if I have a complaint? Dr Ken McNaught, Cranfield University Defence and Security, Shrivenham. Tel 01793 785278 email k.r.mcnaught@cranfield.ac.uk
What happens if I suffer any harm? If you suffer any harm as a direct result of taking part in this study, you can apply for compensation under the MOD's No-Fault Compensation Scheme.
Will my records be kept confidential? All raw and analysed data will be stored on MOD's secure network, and will only be accessed by myself as Chief Investigator and my Research Supervisors. All personal data

will be collected, stored and processed in accordance with UK Data Protection Legislation, which comprises the Data Protection Act 2018, the retained EU General Data Protection Regulations (2016/679), and all other applicable law relating to the processing and protection of personal data.

The findings will be written up in a thesis, which will be submitted towards my PhD. Anonymous quotations may be used together with result summaries in the analysis and published in my thesis. Participants will be identified only by a reference code and their area of expertise.

I confirm that I have read the participant information sheet and consent to taking part in this study: Yes / No

Contact details:

Signature:

Name:

Researcher:

Thank you

B.2 Interview Script

Introduction

- Consent form
- *Much of the literature on deterrence, including that relating to cyberspace, sees it in terms of a relatively straightforward cost-benefit calculation. Other authors recognise the potential importance of other factors (as I listed in the questionnaire) but give no indication of how these can be measured or formally addressed. I am trying to get past simple cost-benefit calculations to how wider considerations can be addressed by planners.*

Opening question

- How would you define deterrence in cyberspace?

The initial questionnaire you and others completed drew out 5 factors which most respondents rated as the most relevant. I would like to look at each of these in turn.

Potential for escalation of the situation

- In the questionnaire, you identified the potential for escalation of the situation as one of the most relevant factors. Why?
OR
In the questionnaire, you identified the potential for escalation of the situation as not being one of the most relevant factors. Why?
- Under what circumstances would you want to risk escalating? Why?
- Is escalation positive or negative to your state?
- How can you measure this?
- What information might help you?
- How can you take that into account in planning?

The credibility of your state's proposed action to the other state

- In the questionnaire, you identified the credibility of your state's proposed action to the other state as one of the most relevant factors. Why?
OR
In the questionnaire, you identified the credibility of your state's proposed action to the other state as not being one of the most relevant factors. Why?
- How can you measure how credible the other state will consider the action?
- What information might help you?
- How can you take that into account in planning?

Other state's willingness to attribute your state for any actions your state may take in cyberspace

- In the questionnaire, you identified the other state's willingness to attribute as one of the most relevant factors. Why?
OR
In the questionnaire, you identified the other state's willingness to attribute as not being one of the most relevant factors. Why?
- How far does their attribution matter, both public attribution and simply them knowing the source of your action? Why?
- Is attribution positive or negative to your state?
- How can you measure this?
- What information might help you?
- How can you take that into account in planning?

How external stakeholders (their allies or neutral states) perceive the other state

- In the questionnaire, you identified how external stakeholders perceive the other state as one of the most relevant factors. Why?
OR
In the questionnaire, you identified how external stakeholders perceive the other state as not being one of the most relevant factors. Why?
- How would you want to influence external stakeholders' perceptions? Why?
- Are the perceptions of external stakeholders likely to be a positive or negative to your state?
- How can you measure this?
- What information might help you?
- How can you take that into account in planning?

Impact on the services or economy of the other state

- In the questionnaire, you identified the impact on the services or economy of the other state as one of the most relevant factors. Why?
OR
In the questionnaire, you identified the impact on the services or economy of the other state as not being one of the most relevant factors. Why?
- Would you want to have an impact on the services or economy of the other state? Why?
- Is any such impact likely to be a positive or negative to your state?
- How can you measure this?
- What information might help you?
- How can you take that into account in planning?

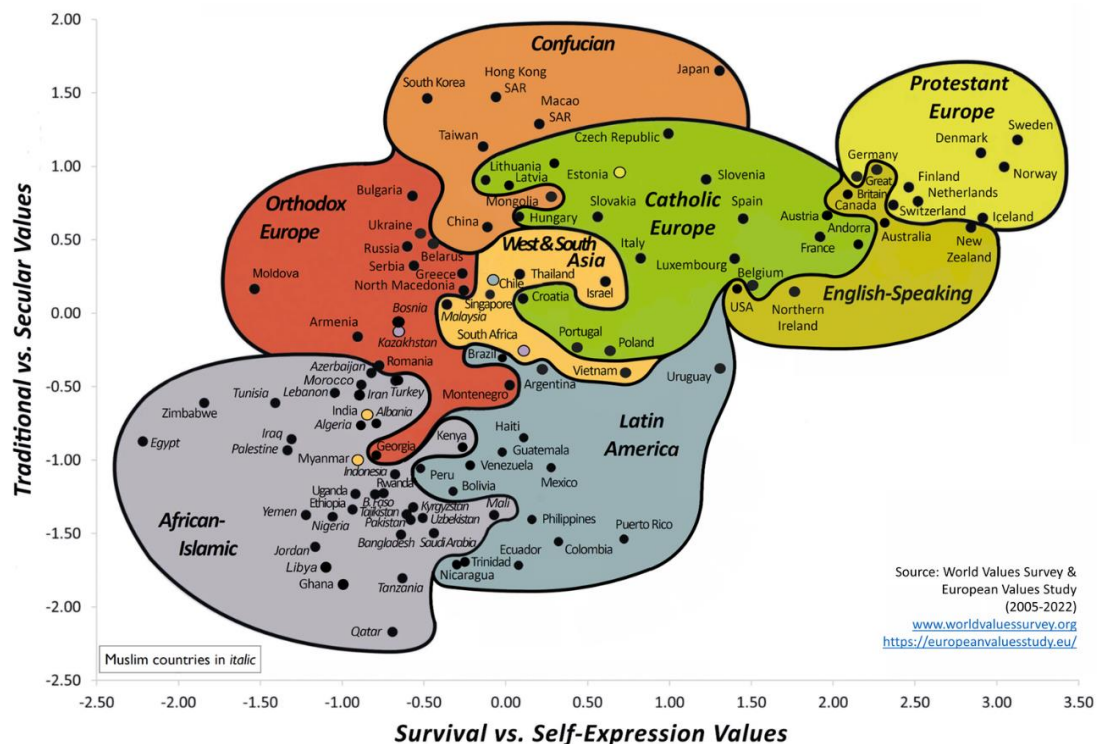
Where at major variance review one other factor as necessary

- In the questionnaire, you identified X as one of the most relevant factors. Why?
- Would you want to have that impact? Why?
- Is this factor likely to have a positive or a negative impact on your state?
- How can you measure this?
- What information might help you?
- How can you take that into account in planning?

General questions

Cultural difference:

- Thinking about the two states involved, yours and the other, regardless of who the two states actually are - is there anything here about the culture of the two states that might be relevant in planning and understanding the context of these factors?
- *Use the example situation if that helps.*
- The World Values Survey (WVS) addresses general societal issues by sampling individuals in countries across the globe about issues as diverse as religion, respect for authority, political interest, trust in others, happiness and attitudes to homosexuality. The WVS data suggests two major dimensions of cross-cultural variation: Traditional vs Secular-rational values and Survival vs Self-expression values. This figure shows the latest update.
- Does the WVS map make it easier to think about your own and the other state?



Intelligence reports:

- Are there any generic intelligence report titles that might help you?

Any other questions specific to their questionnaire responses

Appendix C Workshop Materials

The workshop handouts consist of:

- Workshop consent form
- Workshop handout 1 - scenario
- Workshop handout 2 – group activity
- Workshop handout 3 – individual activity

C.1 Workshop consent form

Consent information – workshop

Study title: Addressing the deterree's context when planning deterrence in cyberspace

I am Sharon Wiltshire, employed by MOD and a PhD research student at Cranfield University Defence and Security. I am researching how the deterree's context can be addressed when planning deterrence in cyberspace.

I am inviting a group of Cranfield Cyber Masters students to take part in a workshop to explore potential impacts of actions in cyberspace. The findings will be anonymised, summarised and analysed for my PhD thesis, which may also include anonymous quotations which will identify participants only by a reference code. The thesis will be shared with MOD.

All raw and analysed data will be stored on MOD's or Cranfield's secure network, and will only be accessed by myself as Chief Investigator and my Research Supervisors. Personal data is limited to contact details only, and will be collected, stored and processed in accordance with UK Data Protection Legislation.

You may withdraw from the research at any time without giving a reason, by informing me within two months of this workshop. If you do choose to withdraw, you may request that all your input up to that point is destroyed and not used in the analysis and results.

If you have any questions, please contact me at s.wiltshire@cranfield.ac.uk

If you have any complaints, please contact my supervisor, Dr Ken McNaught, at k.r.mcnaught@cranfield.ac.uk

Consent information – workshop

Study title: Addressing the deterree's context when planning deterrence in cyberspace

I confirm that I have read the participant information sheet and consent to taking part in this study: Yes / No

Contact details:

Signature:

Name:

Thank you

C.2 Workshop handout 1 – scenario

Deterrence in cyberspace workshop – Scenario

The states described and the situation are fictitious.

Your state – deterrer

Liberal democracy, accepting of freedom of speech and media criticism. Strong dependency on internet and other technology in industry, business and society. Critical national infrastructure mainly in private sector, with involvement of international companies. Active player in world affairs, seeking to promote freedom, human rights and peace. Strong and active military capability, with frequent support to coalitions and links with allies. Offensive cyber capability held within military and openly admitted.

Other state – deterree/potential attacker

Authoritarian government in control of elections and intolerant of serious opposition. Some dependency on internet but use is controlled and censored. Even where industries are officially independent of government some level of control is maintained. Has status as a major player in world affairs, with strong military capability concerned with maintaining its status and influence. Offensive cyber capability within military and through proxy organisations; widely suspected of (but denies) interference with other states.

Situation: intelligence suggests an impending potential cyber attack on a CNI asset within your state by the other state (no specific threat has been received, but relations between the two states are not cordial).

Your state is considering activity in cyberspace to deter the other state.

Your role is as an adviser to the leadership of your state, advising on and considering the likely effectiveness of this deterrence activity.

C.3 Workshop handout 2 – group activity

Deterrence in cyberspace workshop – Group activity

Courses of action

What COAs have you considered, and what is your selected COA?

What possible impacts have you considered? How would you assess those impacts?

Impact

Assessment of impact

What intelligence reports would you find useful to help you determine these impacts or decide on your COA?

C.4 Workshop handout 3 – individual activity

Deterrence in cyberspace workshop – Individual activity

Did you agree with your group's proposed COA?

Yes / No

Why?

If no, what was your preferred COA, and why?

What possible impacts did you personally consider? How would you assess those impacts?

Impact

Assessment of impact

Was there anything in my lecture that made you consider something that you might not otherwise have done?

Appendix D Participant Background Representation using Binary and Hexadecimal encoding

The Research Methodology chapter indicated how hexadecimal values were used to indicate the background experience of the participants. This approach was selected because it allowed an easy identifier to be applied which could address multiple background areas rather than purely a single background.

While a single background could be indicated by the use of a simple label, such as a meaningful expression (e.g. CyberTech or CyberLeader), or a representative indicator such as a colour or a single letter (e.g. Blue or Green, T or L), this would not have allowed multiple background experiences to be described. For the sample used for this research multiple backgrounds were necessary as many would have Cyber Technical or Cyber Leadership experience (or indeed both), as well as experience of military planning or intelligence analysis. As noted in Chapter 5, Questionnaire: Data Collection, Review and Results, the expertise areas claimed by the respondents were considered accurate in view of what was known by the researcher about specific individuals and the military training that many participants would have received.

Hexadecimal (base 16) uses a system where each digit can be a value between 0 and 15, with the values from 10-15 represented by alphabetic characters (A=10, B=11 ... F=15). Two digits can therefore support a range of values between 0 and 63. Each hexadecimal digit can be described in terms of four binary (base 2) digits (called bits) where each bit is either 0 or 1. For one hexadecimal digit the binary values are shown in Table D-1.

Table D-1: Representation of a single hexadecimal digit using four binary digits

Hexadecimal	Binary	Denary	Hexadecimal	Binary	Denary
0	0000	0	8	1000	8
1	0001	1	9	1001	9
2	0010	2	A	1010	10
3	0011	3	B	1011	11
4	0100	4	C	1100	12
5	0101	5	D	1101	13
6	0110	6	E	1110	14
7	0111	7	F	1111	15

The first part of the numeric identifier for questionnaire and interview participants consisted of a two-digit hexadecimal coding where each background was described using a single bit, as shown in Table D-2. Note that the leftmost bit (the highest value in the 8-bit representation of the two hexadecimal digits) is referred to as the most significant bit (msb), and the rightmost as the least significant bit (lsb).

Table D-2: Meaning assigned to individual bits forming two hexadecimal digits

Bits	Meaning
0000 0001	Cyber technical
0000 0010	Cyber leadership/management
0000 0100	Military planning
0000 1000	Intelligence analysis
0001 0000	Understanding different cultures
0010 0000	Other (not used in practice)

Combining each of these bits as appropriate gives a hexadecimal value indicating one or more backgrounds. Table D-3 shows examples of how different backgrounds are allocated descriptors. Since the hexadecimal value can easily

be translated back to its binary form, so hexadecimal 16 can be read as 0001 0110, this means it is simple to identify the individual’s multiple backgrounds from the coded descriptor. This would not be possible with decimal, so a far more cumbersome system would have to be devised.

Table D-3: Examples of descriptor coding

Background experience	Binary	Hexadecimal
Military planning	0000 0100	04
Intelligence analysis and Cyber technical	0000 1001	09
Understanding different cultures, Military planning and Cyber leadership	0001 0110	16

Appendix E Questionnaire Responses and Comments

E.1 Comments on the scenario

respondent ref	comments on scenario
07-05	Does the deterrer state have an appetite to use its OC capability against the potential attacker, and does its political appetite extend to a willingness to be attributed?
0F-07	It feels like there is a need to deter the adversary's Cyber Attack (deterrence of Cyber) but constrains the consideration to using Cyber Means (Deterrence Through Cyber). I would expect wider levers of deterrence to be considered also.
1E-08	This is an area we obviously need to consider. We often look at these situations for a western perspective. It is difficult to put yourself into another culture and take another view point. We also need to remember that there are no right or wrong answers here. Some of this is new ground.
09-09	Already starting to ask, what do we mean by deter? Usually this means making the aggressor pause, ideally indefinitely, in their intended actions and 'think again' about their determination to continue in the course of action. For nuclear deterrent, it is the principle of MAD that is the primary driver for deterring the aggressor. For cyber, MAD does not apply. If anything, any 'action in cyberspace' is more likely to increase the level/seriousness of attacks, in a tit-for-tat situation.
07-12	It set the outline and gets me thinking about this from a Cyber Tactical mission. It is very useful from the above point of view but then on the other hand be causing an individuals unconscious bias to come into play.
07-13	The situation is, I would suppose, necessarily vague - though this is often the case with cyber domain events. It would be difficult to present a credible threat brief to senior leadership based on this kind of threat, and I would almost frame it as BAU.
02-14	Not enough detail about the economic dependencies between the countries and depends upon what you mean by deterrence.
14-16	It's useful to shape the conceptualisation of how the states are likely to behave and their approaches to both international engagement and understanding of the public/private distinction of critical assets. What isn't there - and may be deliberately excluded, to be fair! - is wider contextual information which would help evaluate the effectiveness of and approach to any planned deterrence, including: on the direct relationship between the states and any framing of whether they engage/trade/conflict, directly or indirectly; whether actions may be considered or taken by a proxy; evaluation of any relevant previous interaction in a deterrence/hybrid space, be that active or passive deterrence or other activities, including sanctions etc, which might positively or negatively shape the effectiveness of this planned deterrence, etc.
04-19	The case study scenario implies that a one-off cyber operation would have deterrence effect, which does not take into account contemporary (and prevailing) theories of integrated deterrence and cyber persistence.
02-20	More detail on the types of attacks of the other state

0E-22	Situation is somewhat useful, but lacks the detail needed to make cyber-specific recommendations. Other components of national power (Diplomatic, Military, Economic, S&T) aren't really included in the scenario. Very limited information included on your own and the adversaries intelligence capability (likelihood of detection/attribution and accuracy of these). Otherwise a broadly realistic representation of the dilemmas faced in reality.
06-23	Both summaries of the two states are useful. In the Other State's description I would use a different word to "strong" as arguably that is subjective. And strong in what sense? The Situation succinctly described the Other State's intent but I think it is missing a couple of key bits of information. The first is what CNI. Knowing this would steer who else across Government should be involved in the briefing. And secondly, I think an assessment of the effect the Other State is seeking to achieve would be necessary in order to scale a response, and the direction and guidance that requires. Also, if possible, and related to the Other State Effect would be an indication, available, of the attack vector they are likely to use.
02-25	I think this situation has assumed that the over-riding dynamic in cyberspace is similar to the lens of warfare. In conventional kinetic terms the dynamic tends to be a pendulum swinging between offense dominance or defence dominance (as in the time between innovations and their countermeasure). In the nuclear paradigm, the dynamic tended towards how to coerce change in the behaviour of an opponent. What if the cyber environment has a different dynamic?
14-26	The scenario adds context but, in planning deterrence activities, as much information as possible about the immediate context but also the longer-term history of the adversary and the relationship between our nations would be useful; e.g. what are the adversary's long-term aims and objectives? What does it see as its global role and position? Does it have specific grievances against our nation and / or our allies? Has something occurred or taken place that the adversary vies (from their perspective) as a justifiable reason (they may see it as a trigger) to conduct a cyber attack? Is it just a show of force / demonstration of capability or are they seeking to impose costs / damage on us? And so on
00-27	I thought the situation was articulated very well, although the devil will be in the detail on how best to approach the potential cyber attack on CNI assets.
0B-29	I like how this sets out each nations situation and position. I like how you have called out CNI as the target as that gives policy makers a clear knowledge of the risks being held. My only criticism would be the the line "intelligence suggests an impending potential cyber attack". I think intelligence language would be better to used for this example. an example "Recent Intelligence indicates it is Highly likely a cyber attack will be made against our CNI"
08-31	May help to understand what other capabilities the state has to escalate (e.g. is it nuclear armed?), and the possible motivations for the CNI attack
1C-33	Is the cyber activity the only part of the intended deterrent action, or are there other elements?

16-34	If I'm honest I found the descriptions too simplistic. Liberal democratic values for instance are not universally held in regard around the world. Likewise, government influence and a level of authoritarian behaviour may be viewed by some as acceptable. Part of the the appeal of both the Russian and Chinese narrative is that it has some basis in truth, ro certainly perceived truth.
07-35	Situation only provides very high-level contextual information. One can perhaps infer potential vulnerabilities in the deteree e.g. 'control of their domestic information environment' and aversion to status damaging counter-measures. But this is unlikely to be inadequate for deterrence planning, particularly given lack context around the motivations for the cyber attack on the CNI asset. On the assumption that it is the CNI cyber attack specifically that we wish to deter, it would be helpful to understand the motivations for the attack, who is directing, commanding and conducting the activity and any relevant factors that might form the basis for us planning activities (to deny benefits or impose costs) that would affect their sense-making - causing them to adjust their behavior as a result of being deterred. The description of the situation also doesn't provide a clear basis that our activity in cyberspace (as opposed to other domains) is capable of being effective in deterring the CNI attack.
18-36	The situation is partially relevant, as I can draw some early conclusions about how the other state system works and targets which might be more or less impactful. Really, I'd be much more interesting in the most up to date information on political trends, economics, elite bargains, military posture, etc on which to base decisions and advice.

E.2 Top five relevant factors

respondent ref	A. Distract	B. Attribute	C. Reassure	D. Disrupt	E. Anxiety	F. Self-conf	G. Tech	H. Svcs/econ	J. external	K. morale	L. reput'n	M. credibility	N. escalation
07-05		1			1				1			1	1
03-06		1				1		1				1	1
0F-07	1					1			1			1	1
1E-08			1				1	1	1		1		
09-09			1		1	1		1		1			
10-10			1	1				1		1			1
06-11		1		1				1					1
07-12		1	1	1		1			1				
07-13		1				1		1	1			1	
02-14		1			1				1			1	1
06-15	1								1			1	1
14-16	1							1	1			1	1
02-17		1	1	1								1	1
06-18				1				1	1			1	1
04-19									1			1	1
02-20	1	1								1	1		1
06-21				1				1	1			1	1
0E-22				1	1	1		1				1	
06-23				1		1			1	1		1	
0A-24								1					1
02-25		1									1		1
14-26		1		1				1					
00-27		1	1									1	
12-28	1		1					1				1	1
08-29	1	1						1		1			1
00-30					1			1	1			1	1
08-31			1			1		1				1	1
16-32		1		1							1	1	1
1C-33			1			1		1					1
16-34								1	1			1	
07-35		1		1				1				1	1
18-36					1				1		1		1

E.3 Additional factors

respondent ref	additional factors
07-05	P. Clarity and consistency of signalling of your state
03-06	P. Confidence in own state's resilience and ability to withstand cyber activity against it
06-11	P. The willingness of the deterring state to publicly announce Govt policy describing their position on the threshold for a cyber attack to constitute an attack serious enough to warrant a conventional kinetic or other military response.
02-14	P. Their ability to attribute your actions. Q. Likelihood of avowal. R. Why other options are no valid, mitigating vulnerabilities.
04-19	P. Other state's leadership/military confidence in the effectiveness of their own defence/resilience Q. Communication of the deterrence threat to the intended deteree.
0E-22	P. Whether the leadership of the other state are rational actors (within their own frame of reference).
06-23	P. Overt disruption to the "elite" surrounding the Other State's autocratic leader
02-25	P. Demonstrating willingness to use (even quite low level but noisy attacks) on other states.
14-26	P. Ability to impose costs / harass an actor at very low cost. Q. Ability to impose costs / harm an actor with less risk of attribution (and subsequent response) than other means.
00-27	P. Adherence to established rules, norms and principles (legally binding, political statements, etc) and ensuring legitimacy Q. Ability/capability to verify and attribute attacks and/or actions of others in order to call them out. (similar to B I guess) R. Societal support both as a deteree and within the state being deterred.
0B-29	P. Cost, you can deter a Nation State by making it to costly for them to do cyber operations in your country. Aka if UK Gov were to enforce secure networks, technical measures such as MFA etc. This would then force the attacker to spend money to make bespoke tools and novel ideas which costs money. This will deter them doing operations in that country and move to on to other targets.
00-30	Many of the factors you list are about the other state. Are there more home state factors? Home state public support/trust/ethical-concerns?
1C-33	O. Potential impact on military capability of other state
16-34	P. Perceived willingness of my country to escalate the crisis and conduct credible offensive operations. This includes attribution. Q. Effective messaging that an attack will be met by force that puts at credible risk the opponent's objectives for conducting the attack.

07-35	P - Whether there is a credible 'theory of change' linking our planned cyberspace activity to the necessary change in adversary thinking such that they become 'deterred'. Q - The extent to which the cyberspace activities expected to deter are integrated with a full-spectrum campaign plan, including that cross-domain risk is being managed.
18-36	(O) Potential for multiple simultaneous escalations (i.e. polycrisis).

E.4 Top two relevant factors

Note that these were discounted from the research due to inconsistent user input.

respon dent ref	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R
07-05												1		1		
03-06												1		1		
0F-07	1			1									1			
1E-08								1			1					
09-09			1		1											
10-10			1	1												
06-11		1		1				1					1	1		
07-12		1							1							
07-13		1				1		1	1			1				
02-14	1			1									1			
06-15	1								1			1				
14-16												1	1			
02-17	1		1	1									1			
06-18									1			1				
04-19												1			1	
02-20											1		1			
06-21								1					1			
0E-22					1							1				
06-23									1					1		
0A-24								1								
02-25											1		1			
14-26	1		1	1	1	1	1	1			1	1	1	1		1
00-27														1	1	
12-28								1				1				
0B-29													1	1		
00-30												1	1			
08-31	1	1	1	1	1			1			1	1	1			1
16-32		1										1				
1C-33													1			
16-34												1		1		
07-35													1	1		
18-36	1			1	1								1			

E.5 Further comments

respondent ref	other comments
07-05	
03-06	Deterrence needs to be effective through the path to potential conflict, depending whether sub-threshold, transition to conflict, in conflict or crisis will likely influence which aspects are most important.
0F-07	The authoritarian state will invariably control/dominate their internal narrative/information that is the nations main lever, but the fact they need to control the information is their main vulnerability. Any action and subsequent deterrence action will be tactical considerations in a strategic landscape. Consequently the strategic view must also be considered (by both sides) in any deterrence calculus.
1E-08	This ranking above will be state dependant. We can draw some insight from the Russian behaviour over Georgia in 2008, Ukraine in 2014 and Ukraine following the Feb 2022 second invasion and the spectrum of responses for the EU and NATO and the rest of the world.
09-09	Thought about it from both a Russian and Chinese perspective, as there's a key difference between the 2 for the level to which the leadership is concerned about domestic unrest. Russia, not bothered, China a lot more concerned. So China would potentially be more likely to be deterred by actions taken that could lead to domestic unrest. For both though, the articulation of red-lines does have some effect, even if they eventually seek to test our resolve against those red lines, and will happily carry out attacks beneath that threshold. Finally, deterrence is mostly about changing the aggressors intent, so key factors will relate to the authoritative leadership of the other state. Self-confidence is a tricky one, because over-confidence leads to bullishness and disregard for red lines, but also too little confidence can often result in lashing out, like a wounded animal. In terms of worry/anxiety, I think this is more about anxiety about how they look, as an individual leader and as a country, both to their domestic audiences but also externally. Cyber attacks are a great way to retaliate to perceived disrespect, to try and impose control over other states, to help them look powerful and effective. It's because the western world failed to deter cyber attacks the moment they started being possible that has given aggressor states a green light to attack their 'enemies', where previously they could only do a show of force or conduct information operations.
07-12	An attack in 'Cyberspace' can never truly be attributable as there are many reasons why - the concept of 'Innocent until proven guilty' is the response any state could use. How could anyone ever prove another state is guilty unless there was access to the other states networks and services ... ?
07-13	I think deterrence comes from a combination of a target state being perceived as capable of defence (or retaliation) allied to the political will to attribute blame and act accordingly.

02-14	The whole point of cyber deterrence is that it does not cause an escalation and thus lack of attribution is key. If they know it's you then you are not good at Cyber Ops. Deterrence requires avowal and that would be unlikely for your to highlight your capabilities
14-16	This was difficult to select in a state/context-agnostic way, as these variables naturally will shift as soon as real-world contexts are applied.
06-21	I have looked at this from the point of view of how action taken by my state could beneficially or adversely contribute to / impact upon our cause, as well as ensuring clear understanding of the risks to the public and public services of the other state. Any action would need to be proportionate and these risks understood to the highest degree in order to mitigate the risk of unintended consequences or unlawful and unethical implications. I would also ensure that my state's leadership was made aware of the limitations and particular role the deterrence activity could/will play as part of any wider planned non-cyber related deterrence activities.
0E-22	It is nuanced as the factors I have selected are not specific to deterrence in cyberspace, but apply to deterrence more broadly. There is also a question of whether the domain of deterrence activity (cyber in this case) and deterrence effect (unclear if this is cyber in the scenario or deterring land/air/maritime/space attack) needs to be coherent for success to be achieved or whether cross-domain deterrence is effective from cyberspace.
02-25	I have chosen these as the factors I have seen most often at play in policy making when it comes to cyber operations. But I think this is because largely these operations are seen through a lens of attempting to coerce opponents - deny them something, or possibly message in some way. We have not seen in the West (possibly because we are not revanchist powers where it is possible to argue this has been state strategy) a cyber strategy that seeks advantage or to deny opponent advantage through continual action for advantage in a series of cumulative impacting operations (e.g. espionage, investment laws, control of social media).
00-27	In order to know what you are deterring, you need to have an agreed baseline understanding of the perception of threat from both parties.
08-31	I am slightly confused about the question being asked here in terms of who is being deterred. Is it whether the above factors contribute to 'our state' deterring the 'other state'? If so I do not understand the relevance of factor (B) which is more about what the other state may do in retaliation to our deterrent threat.

16-32	Found this quite difficult as a mix of behaviours and actions from 'our side' and also the other side.
1C-33	I feel this question is a bit too complex - could it broken down a little further? I'm not quite sure whether I'm judging the potential impact of factors on the hostile state's thinking, or how I would rate the various criteria if I were on the receiveing end of the attack. Sorry!
16-34	It is difficult to rule out Q as these 3 elements form the deterrence triangle. All 3 elements would be key to deterring an attack. It should be noted that retaliation would not be limited to cyberspace unless in the view of the defending nation that such a limitation would still offer a credible deterrence. Given the liberal nature of the nation and its reliance on technology it is an assumed that any comparable cyber attack would have a detrimentally larger impact than on the authoritarian nation. J (external stakeholders) would also play a role but only if they could undermine the attacker's objectives. We see this now with the reluctance of Russia to breach a perceived threshold for the use of tactical nuclear weapons.
07-35	P is in some ways very similar to Q. Both are important given that deterrence is a means to an end, not an end in itself. The important thing is that the CNI attack doesn't happen. If that can be achieved via a deterrence strategy (i.e. denying benefits/imposing costs such that the net-benefit of a CNI attack is reduced such that the adversary no longer pursues it) then great. But if a deception strategy, or preclusion strategy also results in the the CNI attack not happening then this is equally good. Proper full-spectrum planning is important to determine that (a) deterrence is a sensible strategy and (b) that cyber activities have a role to play in the deterrence strategy. N is important given that conducting activities powerful enough to actually deter are unlikely to be delivered without consequence. There is a tensions between having an explicit deterrence conversation with an adversary (which may require a degree of clear messaging so that the adversary is clear about what we want to deter, signaling what is likely to happen if they continue, etc) and the tendency to be covert and deniable.

Appendix F Two States used in Scenario from their Own Viewpoints

F.1 Introduction

The following scripts were designed to be used in a two-sided scenario to explore the deterrer actions and the response of the deterree, working through a two- or three-stage interaction. They attempt to demonstrate how each of the two states views each other coming from their own perspective of what is right. Although they were not used in the final research, they do indicate how the viewpoints of each may differ.

F.2 Situation description for player A (deterrer)

F.2.1 State A – deterrer (you)

Liberal democracy, accepting of freedom of speech and media criticism. Strong dependency on internet and other technology in industry, business and society. Critical national infrastructure mainly in private sector, with involvement of international companies. Active player in world affairs, seeking to promote freedom, human rights and peace. Strong and active military capability, with frequent support to coalitions and links with allies. Offensive cyber capability held within military and openly admitted.

F.2.2 State P – deterree/potential attacker (other party)

Authoritarian government in control of elections and intolerant of serious opposition. Some dependency on internet but use is controlled and censored. Even where industries are officially independent of government some level of control is maintained. Has status as a major player in world affairs, with strong military capability concerned with maintaining its status and influence. Offensive cyber capability within military and through proxy organisations; widely suspected of (but denies) interference with other states.

F.3 Situation description for player P (deterree)

F.3.1 State P – deterree/potential attacker (you)

Strong government and leadership, a major player in world affairs, with strong military capability concerned with maintaining its status and influence. Offensive cyber capability within military and through proxy organisations. The government is concerned that other international players (including A and its allies) are seeking to undermine its political ideology, authority and influence. Leadership is keen to maintain the status quo, including influence over neighbouring states which have traditionally been allies but are being wooed by A and its allies. Denies accusations by other states of interference in their affairs, including elections.

Some dependency on internet but concerned that open access may have a destabilising effect, allowing information operations by other states to confuse its citizens, and therefore controls and censors internet use. Similarly, some level of control is maintained even where industries are officially independent of government.

There is unrest in some local areas and in allied states, including calls for reform, greater democracy and action against corruption.

F.3.2 State A – deterrer (other party)

Active player in world affairs, claiming to promote freedom, human rights and peace, but suspected of using this as a cover to weaken P's influence. Active military capability, with frequent support to coalitions and links with allies. Offensive cyber capability held within military and openly admitted.

Strong dependency on internet and other technology in industry, business and society. CNI mainly in private sector, with involvement of international companies. Views internet as an opportunity to promote its view of democracy and freedom of speech, without regard to the destabilising effect that can have on other states.

Appendix G Workshop Outputs

G.1 Agreement with group course of action

Group/ ref	Did you agree with your group's proposed COA?	Why?	If no, what was your preferred COA, and why?
1a	Y	A cyber defence exercise centred around CNI, with appropriate media releases and associated defence/commercial seminars enable overt messaging to populace and intended target state. It enables posturing without escalatory action, and indicates this cyberspace is hostile to external actors.	
1b	Y	Highest chance of success of all the proposed options Proportionate, non-escalatory Benefits to us in improving skills, as well as deterrent effect	
1c	Y	I thought it was the best way to avoid escalation but also to send a message. The corresponding response may provide a better metric of impact.	
1d	Y	It seemed like the most appropriate way to signal to the other state that the possible threat was understood, and this seemed likely to achieve deterrence.	
1e	Y	Reasonable balance between action and avoid escalation.	
1f	N	I wanted to prevent the attack without doubt. We selected a more passive COA in my opinion.	COA 1 -> attack adversary OC infrastructure and use as leverage or destroy. This would demonstrate our capability whilst preventing attack on CNI. Whilst it risks escalation, I think it prevents (hopefully) future attacks by demonstrating capability and increases reputation with local population and we thwart an attack on CNI.
2g	Somewhat	I think the ideal COA was either do nothing (our chosen COA) or COA 3 DCO, but without more information on enemy capability and the vulnerability of our CNI, it is hard to make a meaningful decision. At any rate, I concur with the group that OCO would be a wasteful use of resources.	Just to expand on the above, we all agreed as a group that if we were to decide that this threat was credible/dangerous enough to warrant the investment of resource, we would be better off investing that in general-purpose hardening of our CNI, which provides value against all threat actors than going after one specific actor via exquisite OCO capability.
2h	Y	COAs were assessed and scored against an agreed metric, based on principles of warfare and applied to cyber operations. A consensus was reached on each scored attribute, and respective scores for each COA.	
2j	Y	Assessed against a criteria and scored each COA. Appropriate to the scenario. Suitable given the current information on the situation -> "intelligence suggest" and "potential".	
2k	Y	Looked at it in a methodical and practical way, looking at case in which they can be bolted on to current cyber capabilities.	
2l	N	Scoring criteria was flawed. Purpose-built criteria would need to be designed and applied.	Defensive Cyber Ops (DCO). Amplified with human intelligence and cyber awareness to minimise social engineering of such attacks.

G.2 Impacts considered

<i>What possible impacts did you personally consider? How would you assess those impacts?</i>		
<i>Group/ ref</i>	<i>Impact</i>	<i>Assessment of impact</i>
1a	Hostile actor continues with successful attack	Loss of credibility
	Cyber defence exercise observed closely by hostile nations	Potentially reveals tradecraft and/or exposes vulnerability
	Hostile nation does not see media releases	Continues with successful attack
1b	Adversary does not assess our capability as credible	Deterrent effect diminished
	Adversary becomes aware of reason for activity as deterrence declaration	Deterrent effect could be diminished, but likely by a smaller amount
	Declaration is misinterpreted by adversary as escalatory activity	Deterrent effect fails
1c	Strong message	Expect a response from the other side
	Made aware we were expecting an attack	This would potentially slow any timelines or lead to cancellation
	It would heighten the awareness to the public that an attack was coming	Provide resilience to the system
	A chance to engage with Allies and build a better relationship	May provide access to better capabilities from Allies
1d	Greater public awareness of threat supporting a "casus belli"	People discussing it in news/other outlets
	Compromise of intelligence assets possibly making subsequent attacks more successful. Especially noting that this attack was against a CNI asset and not all CNI -> may not be worth a major response now	Difficult to assess
	Signals to allies -> builds narrative	Discussions with allies and their messaging
1e	The impact on the other state (COA 1)	
	Escalation	Worsening relations
	Targeted messaging	Sows doubt
1f	Defeat attack	Maximum risk of escalation Longer term deterrence
2g	Resource investment	Must be balanced against other national aims. Do nothing not to be under-estimated.
	Credibility of threat	?? Not enough context to determine.
	Reusability/utility of response	DCO more widely useful as an investment against a variety of threat actors. Better VFM.
2h	Availability	Availability of COA.
	Simplicity	Simplicity of implementation.
	Surprise	Element of surprise to adversary.
	Cost/Resource	Cost in monetary and resource terms.
	Time	Time required to achieve effect/COA.
	(Scored 0-5) Taken from Lands Ops Warfare Doctrine and applied to the sphere of cyber operations.	
2j	Availability / Simplicity / Surprise / Cost / Time	0 -> 5 (5 being the greatest)
	Relevant as part of an adviser role when considering effectiveness of deterrence activity.	Can be measured (potentially not surprise).
2k	Personally considered time/effect and what/how it would add on to existing practices/methods already being used by the states.	
2l	Economic	Cost/benefit analysis of consideration to country economy.
	Time	Continuous.
	Cost	Steady, but heavy related to 'economic'.
	Availability	Ongoing / routine.
	Infrastructure	Cost/capability analysis of damage to CNI infra.

G.3 Topics considered from prior lecture

Group/ ref	<i>Was there anything in my lecture that made you consider something that you might not otherwise have done?</i>
1a	Taking simplest COA is often the best solution.
1b	That fear is a significant driving factor in adversary decision making That cultural differences create a large potential area for misunderstanding and escalation
1c	Yes. That communication is key to deterrence however the other side has to be listening and understand you.
1d	I found the 8 criteria for deterrence useful to think about while assessing COAs/
1e	The 8 things of Goodman were useful as a framework.
1f	Not that springs to mind.
2g	Your point around defence being a sufficient deterrence in of itself if messaged correctly definitely challenged my view of deterrence being primarily an OCO-focussed tool
2h	Doing nothing can be valid and positive action. Deterrence actions from one viewpoint may be viewed as aggressive/escalatory actions and this may trigger an escalatory spiral.
2j	It is unclear how effective deterrence is until it has failed. Sometimes 'doing nothing' can be the most suitable COA in deterrence.
2k	
2l	Consideration of geo-political impact drawing in other allied state actors.

Appendix H Initial Proposed Framework

Framework for planning cyber activities

This framework is intended to help those planning a potential cyber activity to understand their own situation and that of the potential target, as an aid to inform discussions and decisions. It consists of a series of questions and is based upon the findings of research into understanding the wider context of the deterrer and deterree when planning deterrence activities in cyberspace. Even where the aim of the activity is not specifically to deter, the framework may still be helpful in clarifying the wider context.

The framework consists of a series of 11 questions that can be answered quickly and simply. They should not need detailed input from intelligence or other sources: while these are important for the overall planning process this framework focuses on key areas identified in research. These factors are: escalation, credibility, attribution, external perception, the other party's services and economy), and cultural factors.

Note that while the responses to these questions may help to inform discussion, areas such as attribution may not fall out in practice as intended. Whether we want an activity attributed or not, however, we cannot guarantee that this will be so, and the decision to make attribution public lies with the other party.

There are many other factors that are not addressed here which are relevant to planning. These questions are not intended to replace these or to repeat areas which are well-served by them, such as adherence to international law.

The 11 questions are listed on pages 2-4 (including charts to answer two of the questions). The Annex on pages 5-8 contains additional material which may be useful for question 4 as an alternative or supplement to the main chart shown on page 2.

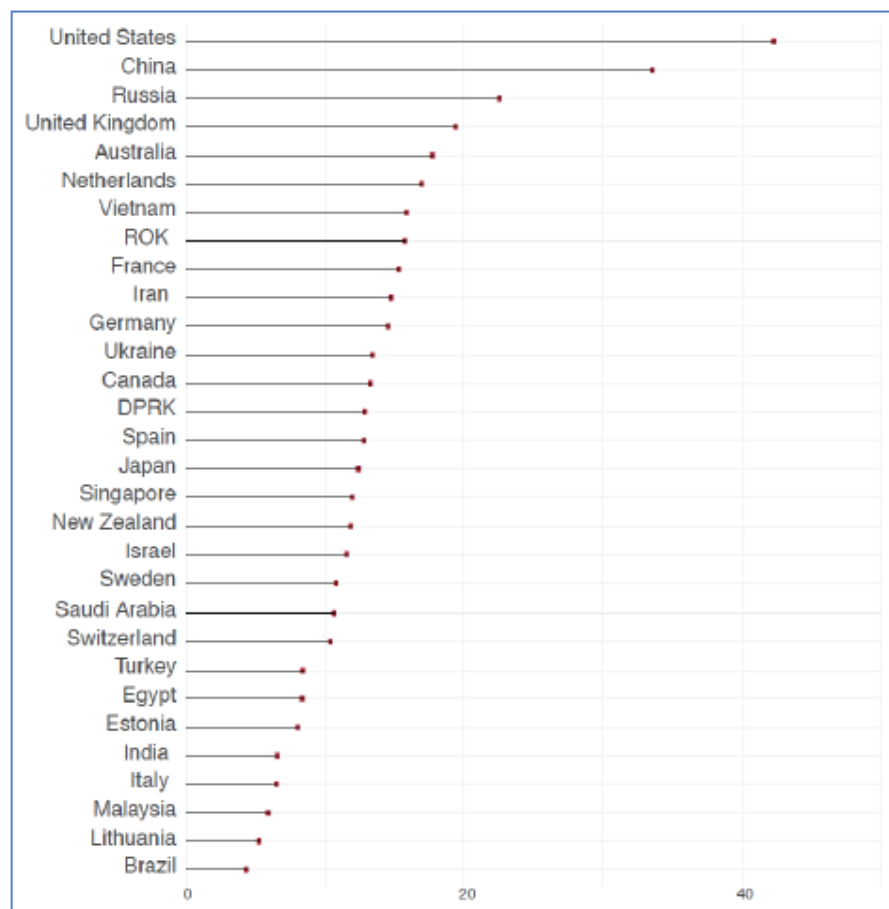
Escalation

1. How willing are we to escalate the situation on a scale of 0 (no appetite) to 5 (keen to escalate)?
2. If the answer to Q1 is ≥ 2 then do we have a clear exit strategy? Yes / No / N/A
3. Does the other party's leadership need a face-saving exit strategy? Yes / No

Credibility

4. What are the relative positions of our state and the other party in the cyber power overall ranking below?

Note: it may be more appropriate to consider individual criteria within the National Cyber Power Index shown in Annex A.



Taken from:

Voo, J., Hemani, I. and Cassidy, D. (2022) *National Cyber Power Index 2022*. Cambridge, MA: Belfer Center for Science and International Affairs. (p10)

Attribution

5. Do we wish our action to be attributed to us? Select one option:

- Definite wish not to be attributed
- Preference not to be attributed /
- Preference to be attributed
- Definite wish to be attributed

External perception

6. What strategies or statements have been published to indicate our capability for cyber operations?
7. What has the media reported about our capabilities, including reporting of resources, declarations, previous activities and exercises? Have any comparable cyber activities been attributed to us by credible other parties (regardless of whether these have been acknowledged by us, or whether we were actually involved)?
8. Has our state been openly attributed for cyber activity (even where we have not acknowledged the attribution)?

Other party's services and economy

9. What services belonging to the other party or used by their citizens (or those of other states) would be impacted by our proposed activity?

Cultural factors

10. Do we know what the other party holds as important or non-negotiable? (These may include tangible or intangible assets, sometimes referred to as sacred values, for example, in the UK this might include our democracy.) <list>
11. Thinking about who we are dealing with in the other party (its leadership or another group), is there a difference in communication, leadership or confrontational styles that we should take into consideration? Use the charts below to consider the relative positions of our state and the other party.

Note: where the other party is not shown in the charts, the descriptions of the different styles may still be useful.

US Australia Canada	Netherlands Germany	Finland Denmark UK	Poland	Spain Brazil Argentina	Mexico France Peru	Italy Singapore Russia	Iran India Saudi Arabia	China Kenya Indonesia	Japan Korea
Low-context							High-context		
Low-context		Good communication is precise, simple, and clear. Messages are expressed and understood at face value. Repetition is appreciated if it helps clarify the communication.							
High-context		Good communication is sophisticated, nuanced, and layered. Messages are both spoken and read between the lines. Messages are often implied but not plainly expressed.							

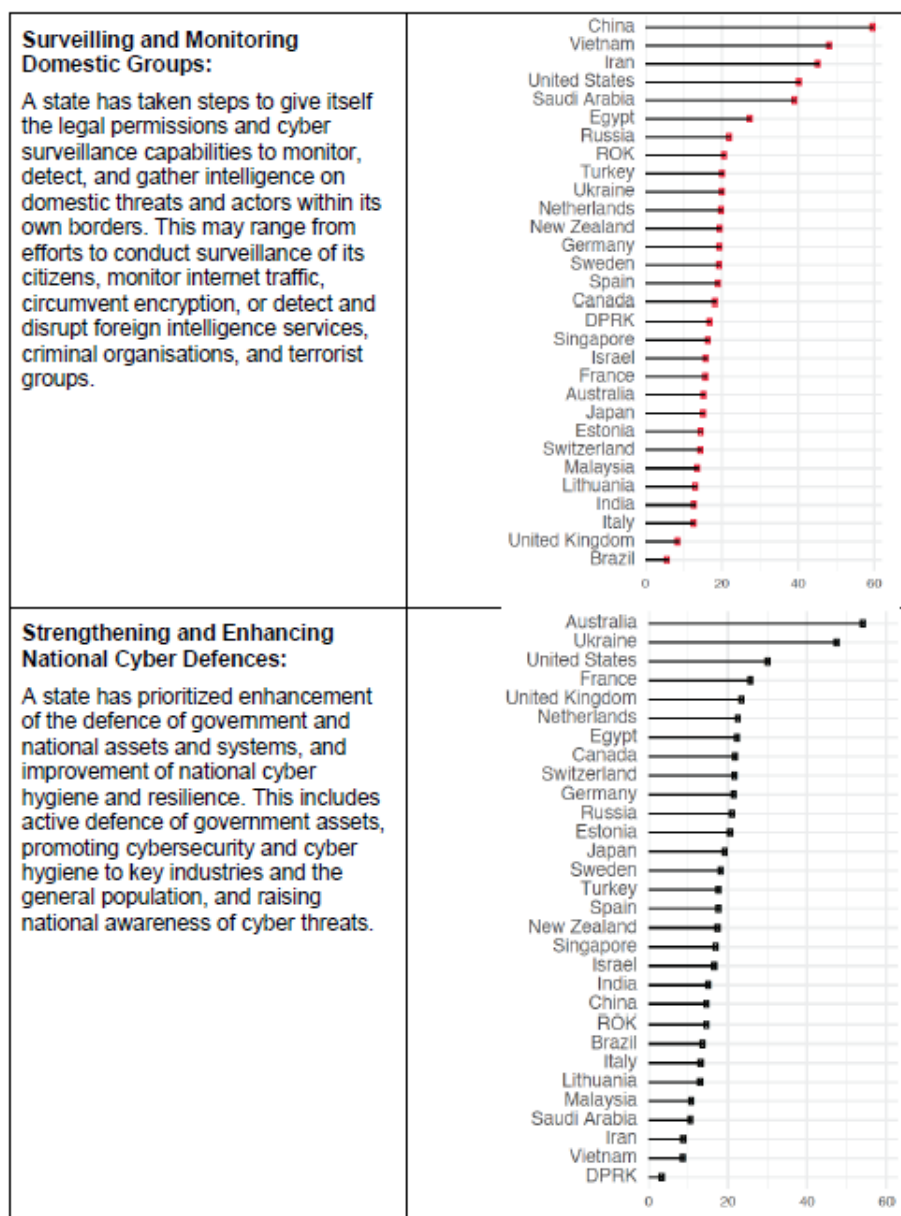
Denmark Netherlands Sweden	Israel Australia	Canada Finland	US UK	Germany Brazil	France Italy Spain	Poland Mexico	Saudi Arabia Russia Peru	India China	Japan Korea Nigeria
Egalitarian					Hierarchical				
Egalitarian					Organisational structures are flat. Communication often skips hierarchical lines.				
Hierarchical					Status is important. Organisational structures are multilayered and fixed. Communication follows set hierarchical lines.				

Israel France Netherlands	Germany Russia	Denmark Spain	Australia Italy	US UK	Sweden Brazil Singapore	India Mexico Peru	China Ghana Saudi Arabia	Indonesia Japan Thailand
Confrontational					Avoids confrontation			
Confrontational					Disagreement and debate are positive for the organisation. Open confrontation will not negatively impact the relationship.			
Avoids confrontation					Disagreement and debate are negative for the organisation. Open confrontation is inappropriate and will negatively impact the relationship.			

Charts (with adapted definitions) taken from
Meyer, E. (2014) *The culture map*. New York: Public Affairs.

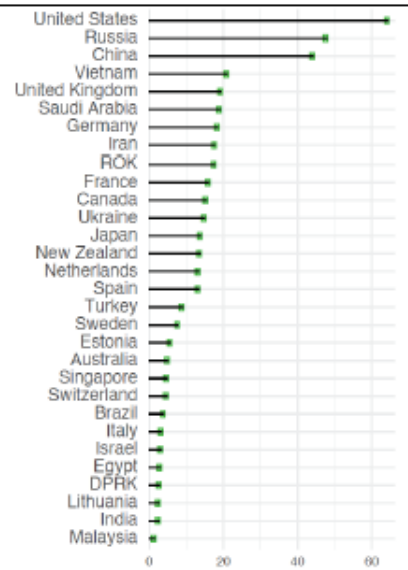
Annex A. National Cyber Power Index 2022 – breakdown by component criteria

Taken from: Voo, J., Hemani, I. and Cassidy, D. (2022) *National Cyber Power Index 2022*. Cambridge, MA: Belfer Center for Science and International Affairs. (pp5-6; 11-12)



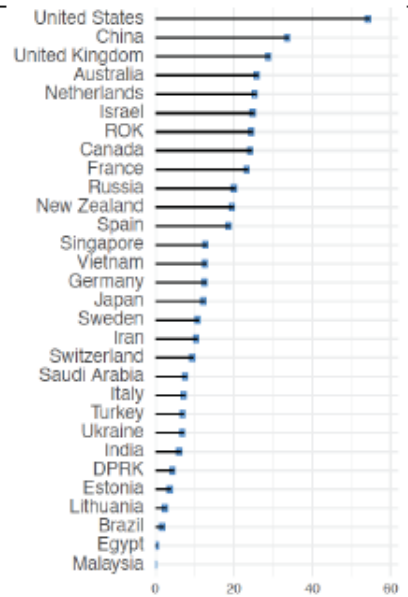
Controlling and Manipulating the Information Environment:

Reflecting the duality of information controls, a state has utilized using electronic means to control information and change narratives at home and abroad. The form includes spreading domestic propaganda, creating and amplifying disinformation overseas, and using cyber capabilities to target and disrupt groups otherwise outside of its jurisdiction. The latter includes taking down extremist material from social media and refuting foreign propaganda.



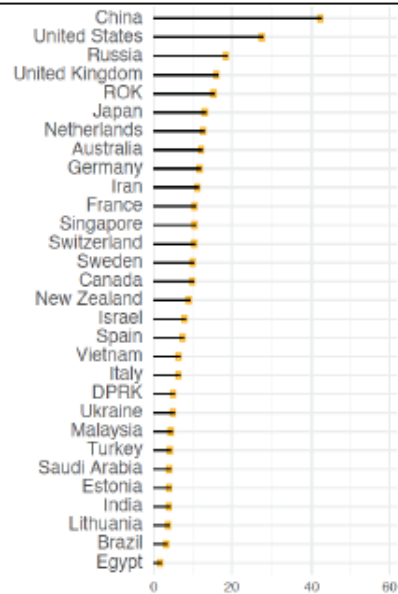
Foreign Intelligence Collection for National Security:

A state has extracted national secrets from a foreign adversary via cyber means. This objective is specifically focused on the collection of information that is not commercially sensitive, but instead the collection of information that informs diplomatic activities, military planning, treaty monitoring, and other situations in which states seek to improve their situational awareness and understanding of a foreign state. This includes hacks and breaches of classified material, such as military plans, but it also includes stealing personnel records, and accessing the communications of senior government figures.



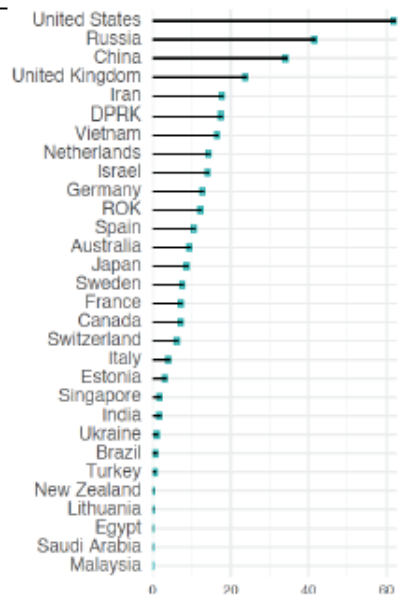
Growing National Cyber and Commercial Technology Competence:

A state has attempted to either grow its domestic technology industry or used cyber means to develop other industries domestically. This could be through legal and illegal means. Illegal means include conducting industrial espionage against foreign companies and states to facilitate technology transfer. Legal means include investment in cybersecurity research and development and prioritizing cybersecurity workforce development



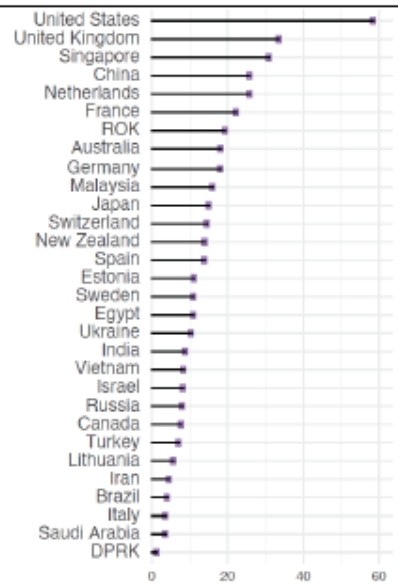
Destroying or Disabling an Adversary's Infrastructure and Capabilities:

A state has used destructive cyber techniques, tactics, and procedures to deter, erode, or degrade the ability for an adversary to fight in cyber or conventional domains. This includes cyberattacks on critical infrastructure, and Distributed Denial-of-Service attacks on government communications networks. It also includes cyberattacks to demonstrate intent and capability to deter an adversary from acting



Defining International Cyber Norms and Technical Standards:

A state has actively participated in international legal, policy, and technical debates around cyber norms. This might include signing cyber treaties, participating in technical working groups, and joining cyber partnerships and alliances to combat cybercrime and share technical expertise and capabilities.



Amassing Wealth and/or Extracting Cryptocurrency:

A state has conducted cyber operations to amass wealth. This includes theft by cyber means including ransomware, blackmail using information obtained via data breaches and attacking the digital infrastructure of financial institutions, and blackmail based on information obtained via data breaches.

