

# Exploring the Role of Service Personnels' Key Relationships in Military Cyber Resilience

**Francesca Kooner-Evans**

A thesis submitted in partial fulfilment of the requirements of  
Bournemouth University for the degree of Doctor of Philosophy.

April 2024

# Abstract

When creating an organisation with a strong Cybersecurity Culture, a consideration of individuals' awareness, attitudes and values are key to building a workforce that is resilient to cyber-attacks. Military organisations and the extended military community share characteristics with civilian populations but have additional unique attributes that influence individual attitudes and values. Whilst research into Cybersecurity Culture in military settings has focused on employee behaviours, there is limited existing literature that considers the role of the extended community, including military personnel's close friends and relatives. This research aims to investigate the extent military personnel's Key Relations contribute to military cyber resilience through their online behaviours. The thesis explores the perspective of military personnel, military friends and relatives, and subject matter experts in military cyber education and cyber incident reporting, to identify online behaviours Key Relations exhibit that could be a target for a military adversary. The thesis contributes to the literature on cyber security culture by applying theories of accountability and responsibility to understand these online behaviours. Building on this understanding, recommendations are put forward for how military organisations should engage with military key relations to encourage a positive cyber security culture, using cyber security training, education and awareness materials.

The research applied a mixed methods approach and consisted of three separate, but inter-related studies. Phase 1 explored the perspective of military personnel across the front-line commands in an online mixed methods survey, that was analysed using frequency analysis and qualitative content analysis. Phase 2 also investigated the perspective of military personnel, alongside the perspective of Subject Matter Experts in cyber incident reporting and monitoring, and cyber education and awareness in Defence. The data collection for Phase 2 consisted of semi-structured interviews, which were analysed with a thematic analysis. Phase 3 differed slightly as it studied the perspective of military personnel's close friends and relatives with an online mixed-methods survey. Similarly to Phase 1, the Phase 3 survey was analysed using frequency analysis and qualitative content analysis.

Findings from across these three studies found that to reduce the cyber risk profile for military organisations, further engagement is needed with the extended military community about their cyber security behaviours and understanding. The results suggest that close relationships for military personnel are vast and include extended family and friends alongside immediate family, defined within the thesis as Key Relations. The research identifies online behaviours exhibited by these key relations, such as oversharing on social media can present a risk to military organisations, which heightens during certain military operations such as deployment or re-location. The thesis summarises by providing suggestions for how military organisations should engage with the extended military community to encourage awareness and application of secure online behaviours that protect Military Key Relations, military personnel and consequently military organisations.

## Contents

<b>Abstract</b> .....	<b>2</b>
<b>List of Figures and Tables</b> .....	<b>8</b>
<b>Acknowledgements</b> .....	<b>10</b>
<b>Declaration</b> .....	<b>11</b>
<b>Chapter 1 - Introduction</b> .....	<b>12</b>
<b>1.1. Rationale</b> .....	<b>12</b>
<b>1.2. Thesis Structure</b> .....	<b>14</b>
<b>Chapter 2 – Literature Review</b> .....	<b>15</b>
<b>2.1. Chapter Introduction</b> .....	<b>15</b>
<b>2.2. Scope of the literature review</b> .....	<b>15</b>
2.2.1. Literature search.....	15
<b>2.3. Organisational Culture</b> .....	<b>16</b>
<b>2.4. Information Security Culture</b> .....	<b>17</b>
2.4.1. Cybersecurity Culture .....	18
2.4.2. Cybersecurity resilience .....	21
<b>2.4. Accountability</b> .....	<b>23</b>
<b>2.5. Responsibility</b> .....	<b>24</b>
<b>2.6. The Theory of Planned Behaviour</b> .....	<b>25</b>
<b>2.7. Cognitive biases</b> .....	<b>25</b>
2.7.1. Optimism Bias.....	27
<b>2.8. The COM-B system</b> .....	<b>28</b>
<b>2.9. Military families</b> .....	<b>30</b>
2.9.1. Defining Friends and Relatives .....	30
2.9.2. Characteristics of military friends and relatives .....	31
2.9.3. The influence of Key Relations experiences on cyber resilience .....	32
2.9.4. Barriers to behaving safely online in a military context.....	35
<b>2.10. Existing ways of addressing threats</b> .....	<b>36</b>
2.10.1. Cybersecurity training, education and awareness .....	36
<b>2.11. Literature review summary</b> .....	<b>37</b>

<b>2.12. Research problem and objectives .....</b>	<b>37</b>
2.12.1. Research problem.....	39
2.12.2. Objectives.....	39
 <b>Chapter 3 - Methodology .....</b>	<b>42</b>
<b>3.1. Chapter Introduction.....</b>	<b>42</b>
<b>3.2 Using a mixed-methods approach.....</b>	<b>42</b>
<b>3.2. Reflection on challenges of data collection within the military .....</b>	<b>42</b>
<b>3.3. Phase 1: Online Survey with military personnel.....</b>	<b>44</b>
3.3.1. Data Collection: Online survey .....	44
3.3.2. Data Analysis: Frequency Analysis and Qualitative Content Analysis.....	45
<b>3.4. Phase 2: Online semi-structured interviews with military personnel and Subject Matter Experts (SMEs) .....</b>	<b>46</b>
3.4.1. Data Collection: Online semi-structured interviews .....	46
3.4.2. Data Analysis: Thematic analysis .....	48
<b>3.5. Phase 3: Online survey with Military Key Relations.....</b>	<b>49</b>
3.5.1. Data Collection: Online survey .....	49
3.5.2. Data Analysis: Frequency Analysis .....	49
<b>3.6. Phase 4: Intended Methodology and Future Plans .....</b>	<b>49</b>
<b>3.7: Chapter Summary .....</b>	<b>50</b>
 <b>Chapter 4 - Phase 1: Exploring the Perspective of Military Personnel in an Online Survey .....</b>	<b>51</b>
<b>4.1. Phase 1 Pilot Study .....</b>	<b>52</b>
4.1.1. Phase 1 Pilot Study: Method .....	52
4.1.2 Phase 1 Pilot Study: Results and Discussion.....	54
<b>4.2. Phase 1 Main Study: Method.....</b>	<b>59</b>
4.2.1. Participants.....	59
4.2.2. Materials .....	61
4.2.3. Procedure .....	64
4.2.4. Ethical Considerations .....	64
4.2.5. Data Analysis .....	65
<b>4.3. Phase 1 Main Study: Results.....</b>	<b>66</b>
4.3.1. Defining Key Relationships: Relationship frequency and strength results .....	66
4.3.2. Communication platform choices and considerations.....	75
4.3.3. Topics discussed when communicating .....	81
<b>4.4. Phase 1 Main Study: Discussion and implications for Phases 2 &amp; 3 .....</b>	<b>83</b>
Aim 1: For military personnel to define who is a key relation by identifying who is considered a close friend or relative. ....	83
Aim 2: To explore how military personnel communicate with their key friends and relations and whether they use different communication platforms with different relations. ....	88
Aim 3: Identify what topics military employees discuss with their friends and relatives over online platforms. ....	91

<b>4.5. Limitations and Considerations for Future Research.....</b>	<b>93</b>
<b>4.6. Takeaways from Phase 1.....</b>	<b>94</b>
<b>4.7. Chapter Summary .....</b>	<b>95</b>

**Chapter 5 - Phase 2: Exploring the perspective of Military Representatives and Subject Matter Experts (SMEs) in Online Semi-Structured Interviews ..... 96**

<b>5.1. Phase 2: Pilot Study.....</b>	<b>97</b>
5.1.1. Method.....	97
5.1.2 Results and Discussion.....	98
5.1.3. Alterations and decisions made following results and feedback.....	101
<b>5.2. Phase 2 Main Study: Method.....</b>	<b>103</b>
5.2.1. Participants.....	103
5.2.2. Materials .....	103
5.2.3. Procedure .....	104
5.2.4. Ethical Considerations .....	105
5.2.5. Data Analysis .....	105
<b>5.3. Phase 2 Main study: Analysis .....</b>	<b>109</b>
5.3.1. Main theme 1: Definition diversity .....	109
5.3.2. Main theme 2: Online risk behaviours .....	111
5.3.3. Main theme 3: Understanding online risk .....	114
5.3.4. Main theme 4: Individual differences .....	120
5.3.5. Main theme 5: Existing approaches .....	123
5.3.6. Main theme 6: Training and education recommendations .....	127
5.3.7. Main theme 7: Military Culture .....	132
5.3.8. Main theme 8: Positive Cybersecurity Culture .....	136
5.3.9. Main theme 9: Responsibility .....	138
<b>5.4. Results summary and implications for Phases 3 &amp; 4 .....</b>	<b>141</b>
<b>5.5. Limitations and considerations for future research.....</b>	<b>145</b>
<b>6.5. Key takeaway points from Phase 2.....</b>	<b>145</b>

**Chapter 6 - Phase 3: Exploring the Perspective of Military Key Relations in an Online Survey ..... 147**

<b>6.1. Phase 3 Pilot Study.....</b>	<b>149</b>
6.1.1. Phase 3 Pilot Study: Method.....	149
6.1.2. Phase 3 Pilot Study: Results and Discussion.....	152
6.1.3. Phase 3 Pilot Study: Alterations made following feedback and results .....	154
<b>6.2. Phase 3 Main Study: Method.....</b>	<b>156</b>
6.2.1. Participants.....	156
6.2.2. Materials .....	156
6.2.3. Procedure .....	160
6.2.4. Ethical Considerations .....	160
6.2.5. Data Analysis .....	161

<b>6.3: Phase 3 Main Study - Results .....</b>	<b>161</b>
6.3.1. Relationships with military personnel: Types, strength and communication regularity .....	162
6.3.2. Communication platform preferences and safety considerations .....	165
6.3.3. Communication via group messaging .....	170
6.3.4. Understanding risk behaviours .....	172
6.3.5. Online behaviours in the context of military organisations .....	175
6.3.6. Training, Education and Awareness .....	176
<b>6.4. Phase 3 - Discussion .....</b>	<b>177</b>
Aim 1: Explore how Key Relations report communicating with their military counterparts, including platform usage and frequency. ....	177
Aim 2: Gather perspectives on what Key Relations believe their online vulnerabilities to be for military organisations. ....	181
Aim 3: Explore current experiences and opinions of cybersecurity training, education, and awareness materials for Key Relations provided by military organisations. ....	185
<b>6.5. Key takeaway points from Phase 3.....</b>	<b>186</b>
<b>Chapter 7: Discussion .....</b>	<b>188</b>
<b>7.1. Chapter Introduction.....</b>	<b>188</b>
<b>7.2. Main research findings .....</b>	<b>191</b>
7.2.1. The definition of Military Key Relations .....	191
7.2.2. Potential behaviours influencing military cyber resilience .....	192
7.2.3. Current approaches to Cybersecurity training, education and awareness for Military Key Relations. ....	193
7.2.4. Accountability and Responsibility for Military Key Relations' online behaviours .....	194
<b>7.3. Evaluation of the Research .....</b>	<b>195</b>
<b>7.4. Impact of the Research.....</b>	<b>197</b>
7.4.1. Recommendations for future Cybersecurity initiatives with Military Key Relations .....	198
7.4.2. Application of Findings Outside of Military Key Relations .....	199
<b>7.5. Directions for Future Research.....</b>	<b>200</b>
<b>7.6. Conclusion.....</b>	<b>201</b>
<b>References .....</b>	<b>203</b>
<b>Appendix A: Phase 1 Online Survey Questions .....</b>	<b>221</b>
<b>Appendix B: Phase 2 Semi-Structured Interview Questions .....</b>	<b>259</b>
<b>Appendix C: Phase 3 Online Survey Questions .....</b>	<b>263</b>
<b>Appendix D: Phase 1 Advert .....</b>	<b>279</b>
<b>Appendix E: Phase 3 Advert .....</b>	<b>280</b>
<b>Appendix F: MODREC Letter of Favourable Opinion for Phases 1 &amp; 2 .....</b>	<b>281</b>
<b>Appendix G: Bournemouth University letter of Ethical Approval for Phases 1 &amp; 2 .....</b>	<b>282</b>

<b>Appendix H: Theme table for themes from Thematic Analysis of the Phase 2 pilot study .....</b>	<b>283</b>
<b>Appendix I: Theme table for themes from Thematic Analysis of the Phase 2 main study .....</b>	<b>290</b>
<b>Appendix J: MODREC Letter of Favourable Opinion for Phases 3 &amp; 4 .....</b>	<b>316</b>
<b>Appendix K: Bournemouth University Letter of Ethical Approval for Phases 3 &amp; 4 .....</b>	<b>317</b>

## List of Figures and Tables

Figure 2.1:	18
Figure 2.2:	29
Figure 2.3:	32
Figure 2.4:	34
Figure 4.1:	56
Figure 4.2:	57
Figure 4.3:	58
Figure 4.4:	59
Figure 4.5:	61
Figure 4.6:	62
Figure 4.7:	64
Figure 4.8:	75
Figure 4.9:	76
Figure 4.10:	77
Figure 4.11:	78
Figure 4.12:	79
Figure 4.13:	79
Figure 4.14:	79
Figure 4.15:	79
Figure 4.16:	81
Figure 4.17:	82
Figure 5.1:	99
Figure 5.2:	108
Figure 5.3:	109
Figure 5.4:	112
Figure 5.5:	115
Figure 5.6:	120
Figure 5.7:	124
Figure 5.8:	128
Figure 5.9:	133
Figure 5.10:	136
Figure 5.11:	139
Figure 6.1:	149
Figure 6.2:	151
Figure 6.3:	152
Figure 6.4:	155
Figure 6.5:	155
Figure 6.6:	155
Figure 6.7:	158
Figure 6.8:	163
Figure 6.9:	164
Figure 6.10:	165
Figure 6.11:	166
Figure 6.12:	167
Figure 6.13:	168



Figure 6.14: .....	169
Figure 6.15: .....	170
Figure 6.16: .....	171
Figure 6.17: .....	172
Figure 6.18: .....	173
Figure 6.19: .....	173
Figure 6.20: .....	174
Figure 6.21: .....	178

Table 1.1: .....	13
Table 4.1: .....	55
Table 4.2: .....	55
Table 4.3: .....	67
Table 4.4: .....	68
Table 4.5: .....	68
Table 4.6: .....	69
Table 4.7: .....	69
Table 4.8: .....	70
Table 4.9: .....	70
Table 4.10: .....	71
Table 4.11: .....	71
Table 4.12: .....	71
Table 4.13: .....	72
Table 4.14: .....	72
Table 4.15: .....	73
Table 4.16: .....	73
Table 4.17: .....	74
Table 4.18: .....	74
Table 4.19: .....	74
Table 5.1: .....	103
Table 6.1: .....	164
Table 7.1: .....	189
Table 7.2: .....	196

# Acknowledgements

First of all I would like to thank my supervisors, Professor John McAlaney, Dr Natalie Mestry and Dr Andrew M'manga for your guidance and support throughout the PhD process. Thank you for providing words of encouragement when I doubted my abilities and when the project seemed nothing more than a MODREC proposal, a literature review and hope.

Thank you to Dstl for match-funding the project and to those at Dstl who helped guide this PhD project. Thank to you Dr Heather Porter for your advice and support and providing clarity for all the acronyms. Thank you also to the Dstl Military Advisors who provided assistance with accessing the participant sample, and to Becky Fish for your help with working through themes and codes.

After studying for 7 years at Bournemouth University, I have to say thank you to all those who helped me get to this point, to my fellow PGRs who have provided comfort and validation during this journey, and those who will remain friends for life.

I couldn't have completed this PhD journey without my day ones, my grannies, thank you for bringing sunshine into my life on the dreary days, I am incredibly grateful to have you in my life. The gratitude also extends to my bestie for the laughter and light.

My biggest thank you goes to my family, for providing unwavering support, motivation and patience, and for being my biggest fans. Thank you for every cup of tea, every sweet treat and every minute spent laughing and dancing because it's better than crying. A special acknowledgement to my Nan for proving during this journey that if you want something done, ask a (retired) military spouse.

## Declaration

I hereby declare that the work presented in this thesis has been composed solely by myself, and it has not been and will not be, submitted in whole or in part to another University for the award of any other degree.

A handwritten signature in black ink, appearing to read 'Francesca Kooner-Evans', written in a cursive style.

Francesca Kooner-Evans

# Chapter 1 - Introduction

## 1.1. Rationale

The UK Armed Forces experience challenges similar to other organisations, in building an organisation resilient to cyber threats and attacks. Cyber resilience is an aspect of Information Security Culture, that focuses on ensuring organisations can predict, withstand and recover from cyber-attacks (Bodeau & Graubard, 2016). The UK's National Resilience Strategy identified multiple key themes of Cybersecurity Culture, including Accountability and Responsibility (Cabinet Office, 2021). The framework created as part of this strategy highlighted how coherent and coordinated responsibilities and accountability are important for strengthening resilience in the UK. Within Cybersecurity, accountability involves encouraging individuals to be answerable for their actions without supervision. It is intricately linked with responsibility, which focuses on encouraging accountability by ensuring all individuals are aware of their role within security (Nel & Drevin, 2019).

The research in this thesis focuses specifically on these themes of accountability and responsibility, which are also recurrent in the academic literature on organisational Cyber Resilience and Information Security Culture (Zimmerman et al. 2019; Uchendu et al. 2021). This thesis posits the importance of a holistic approach to information and cybersecurity. A holistic approach considers the role of people, as well as processes and technology, which interact to influence cyber resilience (Gill, 2021). This thesis mainly focuses on the people aspect. It applies psychological theories to explain behaviours and provide recommendations for how to encourage people to perform processes and securely interact with technology, to encourage cyber-resilient military organisations.

Soeters et al. (1997) argue that the military is often considered a 'Greedy Institution' due to the requirement of personnel to be highly dedicated in their role, being permanently on call during active duty and the potential to have leave cancelled and be deployed overseas at short notice. However personal relationships with friends and relatives can also be perceived as a 'Greedy Institution' as the survival of the relationship relies on reciprocal devotion between those in the relationships (Vuga & Juvan, 2013). This relationship with friends and relatives is often strained when military personnel are relocated or deployed overseas, having a negative impact on both personnel and their friends and relatives (O'Neal & Mancini, 2021; Ribeiro et al. 2023). The desire of military personnel to maintain these relationships during relocation and deployment necessitates the requirement to use online methods of communication, alongside more traditional communication methods, such as letter writing (Rea et al. 2015). When reviewing which relationships are considered pivotal for military personnel, military organisations and existing research in this area often only consider dependent or next-of-kin relationships (Clever & Segal, 2013). This includes spouses, children of a certain age and parents, but often does not consider short-term or LGBTQ relationships (Gribble et al. 2020), or individuals who have a close relationship with their friends.

Ensuring sensitive information is secure is key for military organisations as the consequence of information being used by a military adversary can impact operational effectiveness and potentially result in loss of life (Defense Science Board, 2013). Military friends and relatives often have access to sensitive information, particularly operational information such as location and timings. This results in a potential situation where military friends and relatives share this information either inadvertently or purposefully with individuals who present

a threat to military organisations. Therefore, it is important to identify potential risk behaviours that military friends and relatives engage in, that could create a cyber vulnerability for military organisations. Detecting these behaviours will be useful for directing future cybersecurity initiatives and campaigns. Successful cybersecurity campaigns can encourage Military Key Relations to engage in secure online behaviours, to keep their own and their military person’s information safe online and contribute positively to military cyber resilience.

This research is match-funded by the Defence Science and Technology Laboratory (Dstl), an agency of the Ministry of Defence (MOD). The requirement for this research has been identified by Dstl, to provide insight into how Military Key Relations influence cyber resilience in military organisations. Whilst the research focuses primarily on a population within the UK Armed Forces, this research has implications for other military organisations worldwide. Additionally, the results can be applied to any organisation dealing with sensitive information, including other government organisations, the financial and banking industry, health services and the legal sector. Table 1.1. below outlines a list of stakeholders and how they will use and apply outputs from the research.

**Table 1.1:**

*A list of key stakeholders for the research and how they will use the research outputs.*

<b>Stakeholder</b>	<b>Utilisation of research outputs</b>
The Defence Science and Technology Laboratory (Dstl).	<ul style="list-style-type: none"> <li>• Due to Dstl match-funding this research, they will be able to use the outputs to disseminate within Dstl and any requests for guidance in this area.</li> <li>• Findings from this research will also be used to provide context and justification to guide future work that could be undertaken in this area at Dstl.</li> </ul>
<p>A variety of personnel across the Front-Line Commands (Air, Land and Sea). Examples may include:</p> <ul style="list-style-type: none"> <li>• Those responsible for providing guidance to Units preparing for operational deployment.</li> <li>• Unit commanders to disseminate directly to personnel within their units.</li> <li>• Those working in Cyber roles within the military – this includes participants who took part in the Phase 2 interviews.</li> </ul>	<ul style="list-style-type: none"> <li>• During the data collection interviews participants requested outputs from the research once completed. Outputs would help guide creation of materials that can be used to provide guidance to military personnel and their Key Relations on how to ensure Key Relations are protecting military information online.</li> <li>• Specifically for those preparing for operational deployment, outputs from this research can provide direction for addressing potential online risk behaviours that military Key Relations might engage in that could impact the effectiveness and success of the operation.</li> </ul>
Those responsible for policy creation in the context of the extended military community.	<ul style="list-style-type: none"> <li>• Whilst there is no direct buy-in from policy creators. Research outputs once disseminated can provide a resource for policy creators to refer to when considering who to consider in the military community and when providing guidance for addressing online risk behaviours.</li> </ul>

## 1.2. Thesis Structure

Following this introduction chapter, the thesis begins with a review of the literature in Chapter 2. The review outlines key concepts in Information Security Culture, before discussing the culture of military organisations, the unique experiences of military friends and relatives, and an overview of the current approaches to existing online threats. Chapter 2 summarises the objectives of the research project to address the existing gaps in how military organisations involve the extended military community when considering cyber resilience. Chapter 3 provides an overview of the Methodology that will be applied to address these project objectives, including justifications for methodological decisions. Chapter 4 details Phase 1 of the project, an online survey conducted with serving military personnel, where an initial definition of 'Military Key Relations' is created. Chapter 5 discusses Phase 2, semi-structured interviews that explore the opinions of military personnel in more detail using a qualitative approach, and the perspectives of subject matter experts in defence. Phase 3 builds on the findings from Phase 1 and Phase 2, to understand the opinions and experiences of Military Key Relations towards military cyber resilience, detailed in Chapter 6. Chapter 7 discusses the findings from Phases 1, 2 and 3 of the project, addressing the research aims for each phase individually, and how these findings collectively address the overarching research question. This chapter concludes the thesis by outlining the research impact, limitations and suggestions for the direction of future work.

# Chapter 2 – Literature Review

## 2.1. Chapter Introduction

This chapter explores the current approaches to Information Security Culture and Cybersecurity Culture defining both of these terms and how they are intertwined, alongside addressing how aspects of culture influence how organisations approach cybersecurity. Information Security Culture encompasses all organisational systems and behaviour in an organisational context, including cyberspace, with Cybersecurity Culture as a subset of Information Security Culture (da Veiga et al. 2020). Due to Information Security Culture and Cybersecurity Culture terms often being used synonymously (Uchendu et al. 2021), theories and findings will be discussed in relation to Information Security Culture as a whole entity, considering specific cybersecurity examples, to not exclude any potential explanations for behaviour.

The chapter justifies focusing on two aspects of Information Security Culture: Accountability and Responsibility, before explaining the dissonance between military culture and Information Security Culture. The chapter explains the unique characteristics and challenges for military families and how this may influence how they contribute to cyber resilience, before summarising the current approaches to existing threats. Finally, this chapter outlines the objectives and aims of the research project, based on the existing literature.

## 2.2. Scope of the literature review

The literature review aimed to explore the existing research on Information Security Culture within military families and the impact on organisational cyber resilience. As military research is often confidential, this creates a challenge to identify a large range of literature and therefore the search was extended to include Cybersecurity Culture in all organisations, with a military focus where possible. When considering cyber risk, the potential cyber threats were considered within the scope when examining the literature. A risk assessment was not conducted at this stage, or at any point, of the research due to concerns that conducting a risk assessment in this area would be unable to be published in the public domain due to the identification of potential risks that could be exploited by a threat actor. Therefore, specific assets were also not identified, and potential threats to assets were considered generally within the military, such as any type of Platform (e.g. ship/boat/plane). It is recommended that any future application of findings in this research be accompanied by a risk assessment.

### 2.2.1. Literature search

The literature search was conducted on a variety of databases including Bournemouth University's Advanced Search, which searches a wide array of databases for relevant literature, Web of Science, and Google Scholar. The original search terms when exploring the literature were a combination of "*Cybersecurity OR Cyber Security*" and "*Organisational Resilience*". To explore the role of culture the terms "*Information Security Culture*" and "*Cybersecurity Culture OR Cybersecurity Culture*" were searched for. To reflect the narrow focus of exploring specific aspects of Cybersecurity Culture the terms "*Responsibility*" and "*Accountability*" were also key search terms. To provide additional insight into the topic, these search terms were searched by themselves, but also in combination with an additional search term "*Military OR Armed Forces*"

and “*Military Organisations*” to provide insight into how military organisations approach these considerations. When searching for research which focused on military family samples, the term “*Military Families OR Military Spouses*” was used, to encompass some of the research which only focused on spouses but was still relevant to include. To explore the relationship these individuals, have with social media, due to situations such as deployment, the term “*Social Media*” was also a search combination with the other search terms.

## 2.3. Organisational Culture

Literature on Information Security Culture has identified a connection between culture and cyber resilience (e.g. Gill, 2021). To understand organisational cyber resilience within the military, this thesis narrows in on a specific element of the extended military community, military personnel’s friends and relatives, to explore how they contribute to military cyber resilience. To understand cyber resilience within the military it is important to have an understanding of the organisational culture in the military. Van Den Berg and Wilderom (2004) define organisational culture as a shared belief of how an organisation works, or ‘organisational work practices’, which may be unique to that organisation. However, there is no distinct and shared definition within the literature for organisational culture (Denison et al. 2014). Other researchers suggest organisational culture focuses on shared attitudes, as well as practices (Tellis et al., 2009) or emotions (Barsade & O’Neil, 2014). Chatman and O’Reilly (2016) suggest this lack of consensus in defining organisational culture has occurred due to the applied development of culture within specific organisations, that may not be shared across other organisations, or within an academic understanding. The concept of organisational culture is complex, with many influential facets (Van Den Berg & Wilderom, 2004), which can explain the lack of a consistent definition.

When focusing on military organisational culture, the military relies on uniformity and conformity for operational success and encourages this through shared experiences, values and language (Redmond et al. 2015). Examples of key values within the military consist of obedience, discipline, trust, courage and teamwork (Howard, 2006). Military organisations are termed by some as ‘Greedy Institutions’ as personnel are required to be extremely dedicated in their role, being permanently on-call when actively serving, and have the potential to be deployed overseas at short notice (Soeters et al. 1997). Military organisations also have the unique aspect that jobs can potentially be dangerous and life-threatening. The uniqueness of military organisational culture can create dissonance when considering culture within civilian society. The current research on organisational culture outside of the military encourages the use of gender-inclusive language and moves away from the association of specific personality traits or work practices with genders (Ladwig, 2023). This is in direct contrast with military organisations where masculine and militarized language is used to enforce cohesion within personnel (Malmio, 2022). Military culture is steeped in historical tradition, with Kronsell (2012) explaining that the occupational culture within the military is loyal to these traditions. However, the strong masculine connotations of traditions within the military have previously been criticised (Alvinus & Holmber, 2019). The difference between a civilian society where diversity and inclusion are promoted, compared to military organisational culture where militarized language is used to encourage a cohesive team environment, can create dissonance for individuals within the military community (Malmio, 2022).

This can be the case for serving personnel but also friends and relatives in their personal network. Whilst friends and relatives are not necessarily active serving personnel themselves, there is a shared sacrifice between personnel and their friends and relatives, with friends and



relatives adopting military culture. This comes because of friends and relatives experiencing the impact of deployment, relocation, and concern about the safety of their serving person (Houston et al. 2009). Harrell (2001) also discusses how those relatives who are expected to represent their military person at military events are required to embody the values within the military culture. However, this can be dependent on the nature of the military role. Sewart (2022) explores the experiences of military personnel and their families throughout their military career and identifies that for some, their roles allowed them to have a stable and predictable life within a military setting, with little deployment and relocation. A lot of the research in this area focuses primarily on culture within the US military, with little existing research providing insight into the UK military (Sewart, 2022). Further in this chapter aspects of culture, such as differences in national culture, are explored and may be one suggestion as to why the culture in the US military may not be the same across military organisations in other countries, such as the UK.

Some literature in the area suggests that Cybersecurity Culture is a subset of organisational culture. Wiley et al. (2020) explored the relationship between organisational culture, security culture and information security awareness, and it was found that security culture mediates the relationship between organisational culture and information security awareness. Comparatively, other definitions of Information Security Culture suggest that organisational culture is a subset of wider information security. The rest of this chapter explores Information Security Culture, discussing findings and theories and how these can be applied when considering military culture. As an academic researcher working on research within the military community, it is important to highlight that simply having knowledge about organisational culture and experiences within the military is insufficient to claim cultural competency (Redmond et al. 2015). In this way, it is even more important to examine the literature on theories of culture within military organisations, but also in a non-military context to provide an understanding of the topic.

## 2.4. Information Security Culture

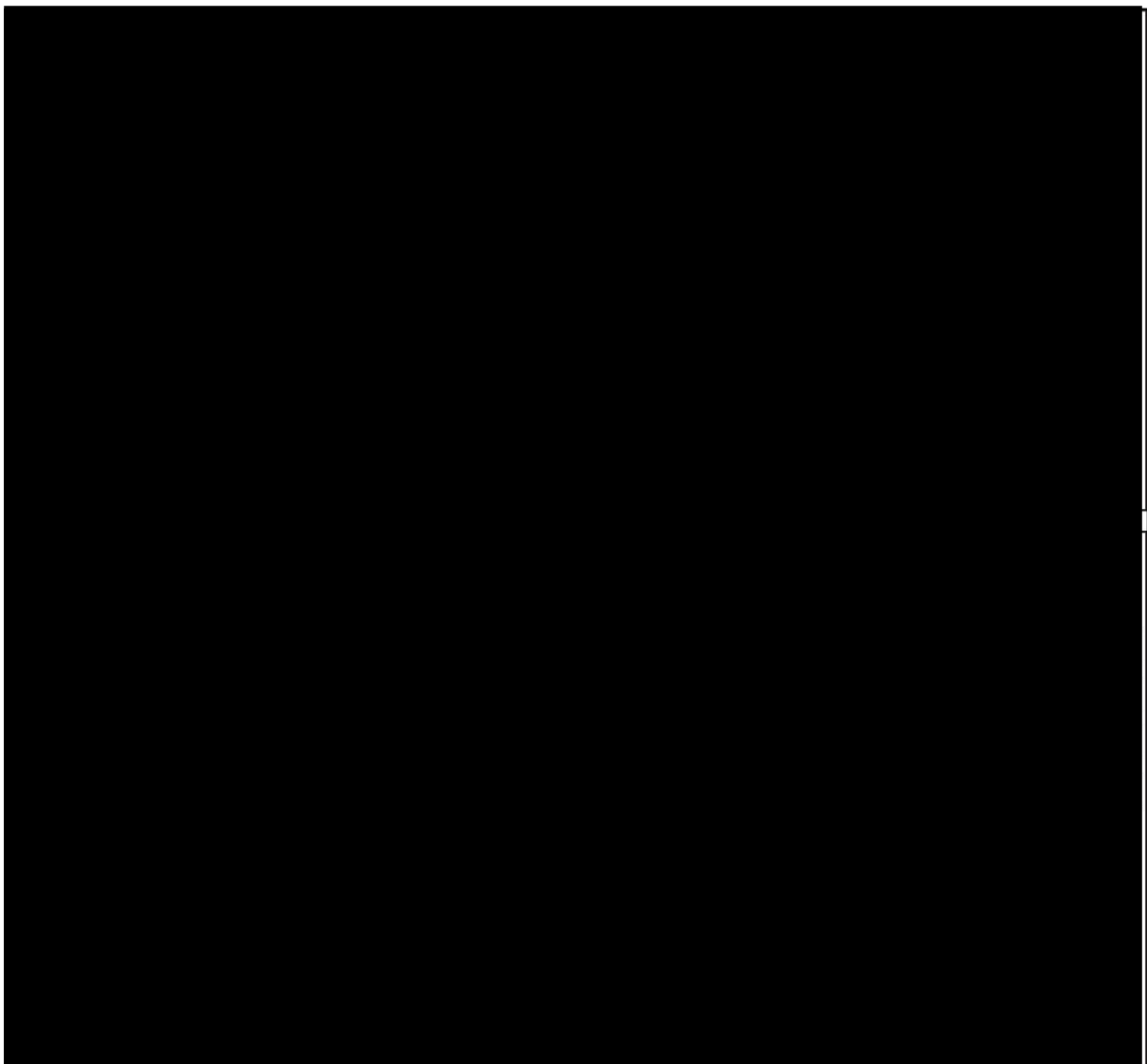
Challenges with addressing Information Security Culture can arise due to broad and inconsistent definitions of what Information Security Culture is, with ill-defined factors and an uncertainty of what the impact of addressing culture might look like. Some literature focuses on values and norms in their definition, whereas other definitions focus on managerial and policy compliance aspects of behaviour when defining Information Security Culture (Da Veiga et al. 2020). This inconsistency when defining Information Security Culture can also add to an already confusing definition of culture within the military as culture can vary depending on when you are considering the general military culture or how it interplays with more diverse unit and base culture (Drummet et al. 2003). There are reoccurring themes when definitions of Information Security Culture are created, such as the idea that Information Security Culture should provide a framework for how people should behave, specifically defining what is acceptable and unacceptable (Da Veiga et al. 2020). These common definitions have been guided by two definitions from papers conducted over 20 years ago; Dhillon (1997) and Martins and Eloff (2002), who both recognised the goal of Information Security Culture was to protect assets within an organisation and that this was achieved by considering human characteristics (Uchendu et al. 2021). Whilst both of these definitions consider the organisation a focal point in Information Security Culture, Da Veiga et al. (2020) highlighted that not all research on Information Security Culture refers to organisations when defining this concept. As the research in this thesis focuses

on organisational culture, within military organisations, the variation between whether organisations are mentioned within definitions of culture, or not, is something of interest.

Figure 2.1. visualises a model created by Da Veiga et al. (2020), which consists of all the potential factors that influence Information Security Culture, taken from the literature and based on the opinions of experts. This model demonstrates the vast plethora of concepts that can contribute to Information Security Culture, and how difficult it is to provide a concise definition that encompasses all these concepts. This thesis will provide an overview of some key concepts which are influential for the research topic of cyber resilience within military organisations.

**Figure 2.1:**

*Da Veiga et al. (2020) Organisational Information Security Culture Model (OISCM), visualises the concepts of information security culture, as discussed in the literature.*



### 2.4.1. Cybersecurity Culture

As mentioned earlier in this Chapter, Cybersecurity Culture is a subset of Information Security Culture (Da Veiga et al. 2020). Cybersecurity Culture relates to how individuals perceive

cybersecurity and how this impacts their behaviour in cyberspace to protect digital information, systems, and people (Da Veiga et al. 2020). Alshaikh (2020) suggests that organisations need to implement five key initiatives to change from an organisation that complies with cybersecurity policies, to one that fosters a Cybersecurity Culture, thus creating an organisation where employee behaviours are influenced by cybersecurity. One of the five initiatives from the Alshaikh (2020) definition of security culture is identifying key cybersecurity behaviours so that everyone is aware of how to behave to create a positive Cybersecurity Culture. However, there is inconsistency in defining the behaviours considered acceptable or unacceptable and which cybersecurity behaviours should be prioritised over others. For example, in a recent review of literature defining Cybersecurity Culture (Uchendu et al. 2021), when asked to consider the factors which are important in building and maintaining a Cybersecurity Culture, only 9 of the 58 papers reviewed identified accountability and responsibility (explored in detail later in the [Chapter](#)) as key factors. The least commonly reported factor was rewards and sanctions, with the most reported factor being management support or involvement, followed by security policy. This being said, Fennelly and Perry (2020) discuss how organisations can often claim to have policies in place to build a strong Cybersecurity Culture, without being able to define what this security culture looks like. Challenges can occur when building a strong security culture as prioritisation in adopting certain security culture factors can look different depending on the type of organisation. For example, the resource and expertise limitations of smaller organisations often mean that staff training and promoting a security culture can become less of a priority (Williams, 2009). Even if a priority, it can be difficult for management to find a balance between monitoring and responsibility due to communication being more direct (Williams, 2009).

Mediating factors from other aspects of culture, such as national culture, could also influence information security culture within organisations. Hofstede (2001) identified six dimensions of national culture. Hofstede's national culture dimensions are frequently considered alongside other models of culture, within the academic literature on Cybersecurity Culture. These dimensions include:

- **Power Distance:** Those in a high-power distance culture will comply with information security policy as they are following orders from authority figures in power, whereas those in a low-power-distance culture are less likely to comply with information security policy as power is distributed equally.
- **Uncertainty Avoidance:** Individuals from a culture with low uncertainty avoidance are more likely to engage with a phishing email due to relying on their knowledge to guide them rather than policy, whereas individuals from a culture with high uncertainty avoidance will not interact until they have guidance from an authority figure or expert.
- **Individualism versus Collectivism:** Those in an individualistic culture will engage with security requirements if there is a personal benefit, whereas those in a collectivist culture will engage with security requirements if there is a group benefit.
- **Masculinity versus Femininity:** An information security manager from a masculine culture prefers to control their employees' online behaviours, whereas an information security manager from a feminine culture will prioritise building a relationship with their employees to encourage safe behaviours.
- **Long-Term versus Short-Term Orientation:** An organisation with a long-term orientation culture will be more likely to invest in cybersecurity systems that prevent a cyber-attack from occurring, whereas a short-term orientation culture will be less likely to invest in a

cybersecurity system as the efficacy of the investment into the system is not demonstrated immediately.

- **Indulgence Versus Restraint:** Those in an indulgent culture are less likely to comply with security requirements if they involve controlling personal desires, whereas those in a Restraint culture will engage with requirements as less value is placed on personal desires.

Hofstede (2011) suggests that societal, national and gender culture is more ingrained in an individual than occupational and organisational cultures, with organisational culture being dependent on how people perceive their organisational environment. They also explain how distinguishing between levels of culture, such as national and organisational culture, is important when interpreting and applying findings from research to avoid inaccuracy. Considering the influence of national culture on military organisations is important as whilst a unique military culture exists that can transcend nationality, many military forces have their own organisational culture which stems from their national culture (Soeters, 1997). For example, when considering Hofstede's Masculinity versus Femininity dimension, it could be said that Military organisations would be closer to Masculinity on the continuum, due to using masculine language (Malmio, 2022).

When looking at Hofstede's dimension of Indulgence versus Restraint, Zhang and Yang (2018) identified that societies with an indulgence culture are less likely to comply with cybersecurity requirements if it involves restraining their behaviour. An indulgent society values happiness, well-being and freedom, and is common in Western societies, such as the UK. In this way, organisations and individuals within the UK may be less likely to engage in cybersecurity behaviours if they believe the secure behaviour is controlling or restrictive. This is relevant for the current thesis due to the research focussing on the UK's Armed Forces. However, as a Western society, the UK is also perceived as having an individualistic national culture. Individualist societies emphasise the desires of the individual whereas collectivistic cultures value in-group goals over individual goals (Hofstede 2001). Contradictory to Zhang et al. (2018), Connolly et al. (2019) suggest that countries with more of an individualistic national culture are more likely to adopt formalised information security policies than their collectivist counterparts (Connolly et al. 2019). This is potentially due to security policies providing individualists with information about online risk situations and potential adverse effects of engaging in risk behaviours that provide them with the context to decide their behaviour more effectively (Chen et al. 2008). Whilst Hofstede's dimensions provide potential explanations for how national culture may influence individual and organisational attitudes towards cybersecurity behaviours and compliance, there are criticisms of the dimensions that should be considered when taking a rounded view of the literature on Cybersecurity Culture. Minkov et al. (2018) discusses how there are very few replications of Hofstede's dimensions, and the replications that have occurred suggest that not all the dimensions are as empirically sound as first thought. For example, Minkov and Kaasa (2020) replicated the Uncertainty Avoidance and Masculinity versus Femininity dimensions and found they lacked internal consistency. Though replications of the Individualist versus Collectivist were robust in their replications (Minkov et al. 2017).

Despite these criticisms of some of Hofstede's dimensions, the role of national culture is important when considering how individual organisations' challenges with cybersecurity can be due to governmental-level issues. This includes a lack of resources devoted to cybersecurity research, and a lack of expertise due to the limited number of cybersecurity professionals (Zimmermann & Renaud, 2019). This may be heightened in public organisations which rely heavily on government funding, and where the government have a large input into how the

organisation is run, such as the military. Uchendu et al. (2021) suggest how a top-down approach where there is a culture supportive of cybersecurity at a national level can be beneficial for encouraging cybersecurity awareness within organisations. However, they also note that cultivating a national Cybersecurity Culture is much more challenging than addressing culture at an organisational level. National culture may also interact with other factors such as age and experience, with some research identifying that age may impact how cyberspace is viewed and impacts how securely people behave online. This difference in understanding and application of technology in daily life is often referred to as the digital divide and can be used to refer to differences in gender (Cooper, 2006), developing countries (Cullen, 2001) and age (Niehaves & Plattfaut, 2014). When looking at generational differences, Debb et al. (2020) found that Generation Y adults, born between 1980 and 1999 (often referred to as millennials) were more likely to engage in cybersecurity best practices, and explained that this may be due to growing up in a culture where risk of privacy violations and security threats online were becoming an everyday issue, and so behaving this way has become part of their conscious awareness. Debb et al. (2020) study consisted of participants from two American Universities, and whilst the participant sample was diverse including a large percentage of African American, Asian American, and Latin American students, this limits the applicability of the security threats discussed to Western Cultures. Due to this, it can be beneficial to explore specific aspects of culture, rather than security culture as an overall concept, and explore how these individual factors might influence organisations' cybersecurity.

#### 2.4.2. Cybersecurity resilience

The psychological definition of resilience focuses on the ability of individuals to maintain stable levels of psychological and physical functioning and positive emotions when exposed to a highly disruptive event (Bonanno, 2004). The American Psychological Association (2018) explains that psychological resilience is demonstrated when individuals adapt well when faced with adversity or stress. Richardson (2002) defines resilience as adjusting and reintegrating to a steady state of psychological function following adversity. However, resilience is an interdisciplinary concept, used in other aspects of psychology such as health psychology, as well as physics and ecology, which can make it difficult to define when considering computer science or cyberpsychology (Dupont et al. 2023). Hollnagel (2010, as cited in Pariès et al. 2010) discusses resilience engineering, which explores what makes a system resilient, how this can be done and how to maintain system resilience. Hollnagel's definition of resilience consists of four essential capabilities with the intention of making the definition more concrete. These four capabilities consist of: the actual, the critical, the potential and the factual. The 'actual' capability refers to the ability of a system to know how to respond to regular and irregular events, this can only be done once there is knowledge of what to look for, which is what the 'critical' capability discusses, and is the ability to monitor changes in the system. The definition highlights that there is a requirement for anticipation of future threats through potential disruptions to operating conditions, addressed by the 'potential' capability. The four capability 'factual' concerns how a resilient system is one that has the ability to use knowledge of an incident that has happened and take away the correct lessons from the incident.

When considering resilience in the context of cybersecurity, The National Institute of Standards and Technology (NIST) put forward that there are four cyber resilience goals organisations should apply to become cyber resilient, these are: Anticipate, Withstand, Recover and Adapt (The National Institute of Standards and Technology, 2019). These goals map similarly to Hollnagel's (2009) capabilities of resilience engineering and are aspects featured in the

definition of psychological resilience above. Bonanno (2004) focuses on maintaining stable levels of physical and psychological functioning, this relates to NIST's goal 'Withstand'. Therefore, demonstrating the interdisciplinary overlap between Psychology and Computer Science. Sepulveda Estay et al. (2020) provide an overview of existing cyber resilience frameworks and state that these frameworks can either be categorised as strategic or operational, however, most existing frameworks take an operational approach. This means frameworks are more considerate of the effects on disruption of operations and the legal and economic implications, as opposed to approaching resilience considering avoidance or response to disruptions (Sepulveda Estay et al. 2020). Therefore Sepulveda Estay et al. (2020) review of cyber resilience frameworks suggests that frameworks are only focusing on two of the cyber resilience goals outlined by NIST, Withstand and Recover rather than attempting to Anticipate or Adapt from a potential attack.

As outlined above resilience in Computing and Psychology has much overlap. Therefore, it is unsurprising that organisational cyber resilience can be achieved by addressing technological and process vulnerabilities, but also by ensuring that the people associated with the organisation are behaving securely online (Gill, 2021). A focus on building a Cybersecurity Culture where resilience is forefront when considering employee awareness, attitudes, and values, can be one way of increasing organisational resilience (Gill, 2021). Suggestions for creating a security culture that prioritises resilience range from recruitment and onboarding activities which focus on communication and consistency, through to post-mortems which shift from blaming individuals to learning from mistakes (Gill, 2021). Nonetheless, it should be considered whether organisational cyber resilience should be employer or employee focused. Within a military context, addressing the human component, as well as the technological is key to avoiding providing adversaries with sensitive information. Many of the existing frameworks on cyber resilience, which have a focus on application to military operations, concentrate on technological approaches rather than employees (Wagner et al. 2016; Barreto & Costa, 2019). Da Veiga et al. (2020) found that when individuals are asked about what their organisation should do to create a good information security culture, the most common responses included training and awareness, with much fewer mentioning anything to do with people. This may suggest that the reason very few cyber resilience frameworks with a human behaviour focus exist within a military context is due to a lack of apparent desire for one from employees. This is further supported by the finding that employee opinions on building a good Information Security Culture focused more on what the employer's actions should be to create and maintain policies, rather than what the employee behaviour should be to avoid risk (Da Veiga et al. 2020). This would suggest that even when there is a person-centred approach to organisational cybersecurity, employees would prefer this to be an employer focused approach to good security practices and organisational cyber resilience. Zimmermann and Renaud (2019) identified that even when prevention solutions do consider human behaviour as part of preventing adverse cyber events, people are considered the problem and policy aims to reduce problematic behaviours, rather than encouraging secure online behaviours. As a response to this, a "Cybersecurity, Differently" mindset was introduced which approaches the human element of culture as people being both part of the solution and part of the problem which needs to be addressed. The approach considers employees who present a security risk but also considers separately the employees who are well-intentioned and eager to perform secure behaviours (Zimmermann & Renaud, 2019).

Organisational resilience has been identified by the United Kingdom government as a critical area to develop so that the nation can be prepared in an evolving risk landscape (Cabinet

Office, 2021). As part of this resilience strategy, accountability and responsibility have been identified as two key areas of focus, which highlights that all those involved in resilience, being employee or employer, need a clear understanding of how and when to use resilience tools. The following sections will define and discuss the literature on accountability and responsibility, in relation to cybersecurity.

## 2.4. Accountability

Accountability within cybersecurity involves encouraging individuals to be answerable for their online actions, without constant supervision (Nel & Drevin, 2019). This means that individuals should consider whether they are complying with the cybersecurity requirements put forward by an organisation (Dornheim & Zarnekow, 2023). Whilst constant supervision is not required, accountability theory suggests that if individuals believe at some point, they will need to justify their behaviour and actions to someone else, this can impact the decision-making process (Vance et al. 2015). This decision-making process can be explained through systematic processing, where individuals will use deep-cognitive processing, involving considering an increased number of inputs in a slower manner, to reach what they believe is the optimal decision (Vance et al. 2015). Accountability theory is strongly linked to group norms and self-image as individuals may make decisions grounded on how they believe they are expected to think based on others around them (Dang-Pham et al. 2017). As well as this, there may be other factors which influence individual accountability for online behaviour, such as gender differences (Roberts & Burns, 2013).

In a report created by the House of Commons Defence Committee in 2013, it was highlighted that within defence good cyber practice ensures that accountability within distinct roles is clear as uncertainty would obstruct the effectiveness of the Ministry of Defence, including the Armed Forces (House of Commons, 2013). Dornheim and Zarnekow (2023) suggest one way of increasing accountability is through establishing consequence management, wherein there is an outcome for violating cybersecurity rules. The level of these consequences should be consistent with the levels of the violations. For example, clicking on a link in a simulated phishing attack would result in an individual being required to complete phishing awareness training, whereas using an unauthorised USB drive on a work device with sensitive information might result in an official warning. Deterrence theory can provide one suggested explanation for why the use of consequences or sanctions can be effective in encouraging compliant cybersecurity behaviour. Deterrence Theory explains sanctions are effective due to the consequence of violating a cybersecurity policy being so severe, that it outweighs any potential gain from subverting regulations (Straub, 1990). However, other research suggests that the use of sanctions may become a barrier to building a culture that values cybersecurity as employees become less trusting of security enforcers (Kirlappos et al. 2014) and delay compliance with cybersecurity behaviours, resulting in operational delays (Belanger et al., 2017). When considering the potential administration of sanctions because of Military friends' and relatives' online behaviours, there are multiple challenges. The first is the ability to sanction military friends and relatives who are not employees within the Ministry of Defence and therefore are under no obligation to engage with cybersecurity behaviours nor the sanctions associated with lack of compliance with these behaviours. There is the potential that accountability could be assigned to the military personnel on behalf of their friends and relatives' behaviour. However, as identified, this could have a cyclical detrimental effect on military friends and relatives engaging with cybersecurity behaviours to protect an organisation that they do not trust nor respect. In this

way it is important to create a “just culture” (Dekker, 2016) in an organisation that places importance on trust, learning and accountability rather than blame and sanctions.

One way of creating a “just culture” is by applying blameless post-mortems following a cyber incident. This is where individuals involved in a cyber incident share the details of their actions and consequences so that the organisation can learn from it, rather than sharing this information to attribute blame (Gill, 2021). Dekker (2018) highlights that an organisation without blame is not one without accountability. However, an organisation with a blame culture may be more likely to experience repeated cyber incidents due to the cycle of name/blame/shame. This cycle highlights how if an individual is blamed and consequently shamed because of their contribution to an incident, they will be less likely to share the day-to-day performance in their role with management. This results in management being unable to provide adequate provisions to address potential cyber risks and individuals become less educated on these risks, resulting in a higher likelihood of a cyber incident occurring. The retribution approach describes this as choosing whether to adopt a retributive process, wherein an appropriate punishment is imposed or a restorative process, focusing on repairing damaged trust and relationships (Dekker 2018). A retributive process may be detrimental if individuals perceive that the punishment is unjust for an accident, as this may lead to them growing to resent the company and creating an insider threat (Elifoglu et al. 2018). It is important to prevent this from occurring rather than attempt to deal with the aftermath due to the difficulty of being able to spot both malicious and non-malicious insider threats. Insider individuals have the authority and clearance to perform these actions in their roles, so it is difficult for technical tools to identify when these actions are being performed with malicious intent and to intervene, and when it is non-malicious and further training is required (Elifoglu et al. 2018). It is important to reduce insider threat as not only could this leak confidential data, which in a military situation can not only be detrimental to the day-to-day running of an operation but also life-threatening. There is also potential damage to reputation (Sanders et al. 2019), which may lead to a lack of trust in the Armed Forces.

## 2.5. Responsibility

Accountability and responsibility are intricately linked. Accountability is encouraged through responsibility by ensuring that individuals are aware of their role within security (Nel & Drevin, 2019). Through understanding their role in security, employees can behave responsibly by satisfying their obligation to complete a security related task (Uchendu et al. 2021). For this thesis that includes any stakeholders in the extended military community, including military personnel and their friends and relatives. Research suggests that organisations with a culture that is favourable towards cybersecurity should consider cybersecurity as a shared responsibility between all stakeholders in the organisation (Da Veiga & Eloff, 2010). However, this may not always be the case. Ramachandran et al. (2012) conducted research exploring the perception of responsibility for information security between different professions within one organisation. They found that whilst some individuals believe management is responsible for information security, or that information security is shared, the majority believe that cyber specialists should be responsible for security. The risk of the belief that it is only cyber specialists who are responsible for information security is that individuals may not fully understand the influence their behaviour has on the cybersecurity of the organisation, leaving the organisation vulnerable to cybersecurity threats.

Building this culture where responsibility is shared requires implementing a comprehensive cybersecurity framework. AlHogail (2015) put forward a framework for



Information Security Culture where four main dimensions of human behaviour impact Information Security Culture. The four dimensions of the framework consist of preparedness, management, society & regulations, and responsibility. Responsibility in this model reflects people's perceptions of security and their acceptance of responsibility and is a bi-directional component wherein people influence Information Security Culture and Information Security Culture influences the people. Tang et al. (2016) also highlight the importance of human behaviour in information security and that understanding how employees perceive responsibility for cybersecurity and information security within an organisation is important in developing an Information Security Culture. Marotta and Pearlson (2019) conducted research exploring a case study to understand how an Italian Bank has created a Cybersecurity Culture to help the bank protect itself from cyber threats. One of the core factors that formed the basis of the Cybersecurity Culture within the bank was a shared responsibility for cybersecurity, between four levels of employees. For shared responsibility to be effective in mitigating the risk of cyber threats, all employees were aware of their role in contributing to cybersecurity. Each employee had a clear understanding of their responsibility, which allowed them to make sure they were engaging with the appropriate security measures and keep the bank secure. Marotta and Pearlson also noted that identifying responsibility ensured employees were accountable for decisions they made about their security behaviours. This can be extrapolated and reworked to represent the hierarchy that exists within military culture, which can include the Key Relations, as part of the extended military community. For example, senior-level executives may be considered as unit commanders, security executives as personnel in higher ranks, general managers as those in lower ranks and general employees being Key Relations. However, Key Relations may also be groups that branch off from each of the levels, as friends and relatives often take on the rank of their military person (Drummet et al. 2003).

## 2.6. The Theory of Planned Behaviour

Accountability and responsibility may be influenced by social factors. The Theory of Planned Behaviour (Ajzen, 1991) can explain how group norms and self-image may lead individuals to make decisions when it comes to their online behaviour but also considers individuals' attitudes towards a behaviour and their perceived behavioural control (Somme stad, 2018). The theory suggests behaviour is influenced by intention and that intentions are influenced by attitude, subjective norms, and perceived behavioural control (Somme stad & Hallberg, 2013). A review of the studies that explore whether the Theory of Planned Behaviour can explain information security behaviours finds mixed results for the impact of each aspect of the theory. For example, Roberts and Burns (2013) identified that the Theory of Planned Behaviour can explain 81% of the variance in online safety behaviours, but that attitudes and normative beliefs only influenced the intention to perform online safety behaviours, whereas perceived behavioural control has a direct effect on these online behaviours. Evidence of the perceived behavioural control component of the Theory of Planned Behaviour within the extended military community may look like military friends and relatives believing that they cannot ensure they are protecting military information online if they are not informed what is acceptable and unacceptable operational information to share online.

However, the results of research into the Theory of Planned Behaviour and cybersecurity seem to vary depending on the safety behaviour being measured. Dang-Pham et al. (2017) measured security practices that involve relationships with others, such as sharing information security advice, and found an individual's positive attitude towards security behaviours can

increase information sharing but perceived norms and perceived behaviour control did not impact on security sharing behaviour. This could be due to a fear of social pressure or that the existing culture within the organisation discourages advice sharing (Dang-Pham et al. 2017). Within the extended military community, this social pressure may come from friends and relatives vicariously carrying the rank and being required to represent their service member (Drummet et al. 2003). In this way, military key relations may experience the social pressure to embody military culture, through association with their military person. This is an example of where the attitudes component of the Theory of Planned Behaviour might be evident within the audience being explored in this research. Safa and Solms (2016) suggest that organisational support influences the security behaviour of individuals as perceived support is viewed as a commitment to employees and therefore this is reciprocated back into the organisation. This could be a potential way for military organisations to encourage safe online behaviours within the extended military community. If military organisations engage with military friends and relatives about cybersecurity, this engagement could be perceived by Key Relations as supportive and could result in individuals engaging in online safety behaviours set out by military organisations, as a reciprocity behaviour. This may also increase the perceived behavioural control that Key Relations experience as they feel like they have an increased ability to engage in safe online behaviours due to being supported by military organisations.

One additional factor that may influence behaviour of those associated with an organisation, such as in the military community, when considering cybersecurity behaviours is the role of knowledge. An additional branch of the Theory of Planned Behaviour is the Knowledge-Attitude-Behavioural (KAB) model (Kruger and Kearney, 2006). The KAB model suggests that as an individual's knowledge of information security behaviours improves, their attitude towards these behaviours also improves, resulting in engaging with information security behaviours Parsons et al. (2014). The findings from this research present a justification for exploring the potential to increase military Key Relations' cybersecurity knowledge, as this may have a positive effect on attitude towards cybersecurity behaviours and consequent uptake of these behaviours, to protect military information. Further research by Zwilling et al. (2020) into the KAB model across four different countries; Israel, Poland, Turkey and Slovenia, identified that there may be cross-cultural differences that interplay with the KAB dimensions to influence information security awareness. They found Turkish participants perceived cybersecurity as risky and threatening and engaged in more protective cyber behaviours. Comparatively Israeli and Polish participants found cybersecurity less threatening, with Israeli participants having the lowest threat avoidance, however, both of these countries had low threat awareness. These findings present evidence to suggest cultural differences may influence behavioural intention and behavioural commitment, which is explored in the Theory of Planned Behaviour, and might need to be considered when exploring Key Relations online behaviours. However, the findings from Zwilling et al. (2020) could be debated when considering Hofstede's cultural dimensions, as these three countries score similarly across all dimensions, except for Power Distance, where Israel scores very low compared to Poland and Turkey (The Culture Factor Group, 2024). When looking at Hofstede's cultural dimension of Uncertainty Avoidance, all three of these countries are reported to have high Uncertainty Avoidance, suggesting they would all be cautious when considering online safety. This is inconsistent with Zwilling et al. (2020) findings which as explained above, indicate Israel has very low threat avoidance. Zwilling et al. (2020) highlight that differences in their results between countries could potentially be due to the design of their study, as Turkish participants completed a survey in their native language, whereas others took the survey in English. Additionally, other factors relating to the participants completing the study

could have influenced the results, as all the participants were students. Research into factors influencing information security awareness suggests that the level of education affects awareness of information security (Wiley et al. 2020; Hong et al. 2023). In Hong et al. (2023) research they proposed the KAB model be extended to include social education level, which is the average educational level of society, as an additional factor that influences information security awareness. This more recent research provides evidence to suggest that additional factors may need to be considered when applying the Theory of Planned behaviour to understand behavioural intention and engagement.

## 2.7. Cognitive biases

Another dimension that may influence an individual's attitude towards adopting cybersecurity behaviours to reduce cyber risk is the perception that the risk will happen to them. However, often these perspectives are biased and do not accurately evaluate the extent to which an individual may be put at risk by their online behaviour, which impacts their ability to make a safe and objective decision about their online behaviour (Pfleeger & Caputo, 2012).

### 2.7.1. Optimism Bias

Optimism bias, or social comparison bias, highlights how a cognitive error in judgement means individuals will perceive the risk to themselves as lower than others (Weinstein, 1980). In a cybersecurity context, this means that individuals experiencing optimism bias will believe that they are less vulnerable to a cyberattack compared to others. This reduced perception in vulnerability can make individuals less likely to engage in behaviours that might prevent a cyberattack or they might be more likely to engage in cyber risk behaviours as they don't believe they will be targeted by a threat actor (Alnifie & Kim, 2023). This can also extend to an organisational level, wherein a business believes that it will not become the victim of a cyber-attack despite other organisations experiencing cyber-attacks. In the context of military organisations this may display itself as an individual military unit believing they are less likely to experience an incident due to Key Relations sharing information online, despite another military unit experiencing an incident as a result of this vulnerability. Additionally, this may be heightened for those who work within the information security or cybersecurity domain, as some research suggests those who have more knowledge about cyber risk and threats are more optimistically biased and will not be the victim of a cyberattack (Rhee et al. 2005). Rhee et al. (2005) suggest that optimism bias occurs within an information security context due to defensive and functional optimism. Defensive optimism is a naïve optimism that an individual will not be the victim of a cyber-attack whereas others might, and functional optimism relates to personal ability and resources to control the situation. Therefore, those who work within information security and cybersecurity will perceive themselves as having the resources and ability to control the situation should a cyber event occur (Rhee et al. 2005). The theory of perceived control puts forward an explanation for why those individuals with an increased knowledge of cybersecurity may experience optimism bias in this area. Perceived control can be defined as an individual's perception that they are competent to produce desired and prevent undesired events (Wallston et al. 1987). The suggestion is that the higher perceived control individuals have about a situation the more likely they are to experience optimism bias (Rhee et al. 2005). Again, when considering the role of management in an organisation, Rhee et al. extended their research in 2012 by exploring the extent of this experience for individuals who are responsible for managing and directing information technology teams. They found that these individuals have a good understanding of the potential cyber risk to themselves, but they perceive themselves as having a higher level of ability to be able to control a potential situation where their organisation is

experiencing a cyber threat (Rhee et al. 2012). The theory of perceived control posits that this self-perception of having a higher level of ability to control a cyber threat situation would result in a cognitive error in the form of optimism bias that may consequently mean they are more vulnerable to an attack due to a reduced threat perception.

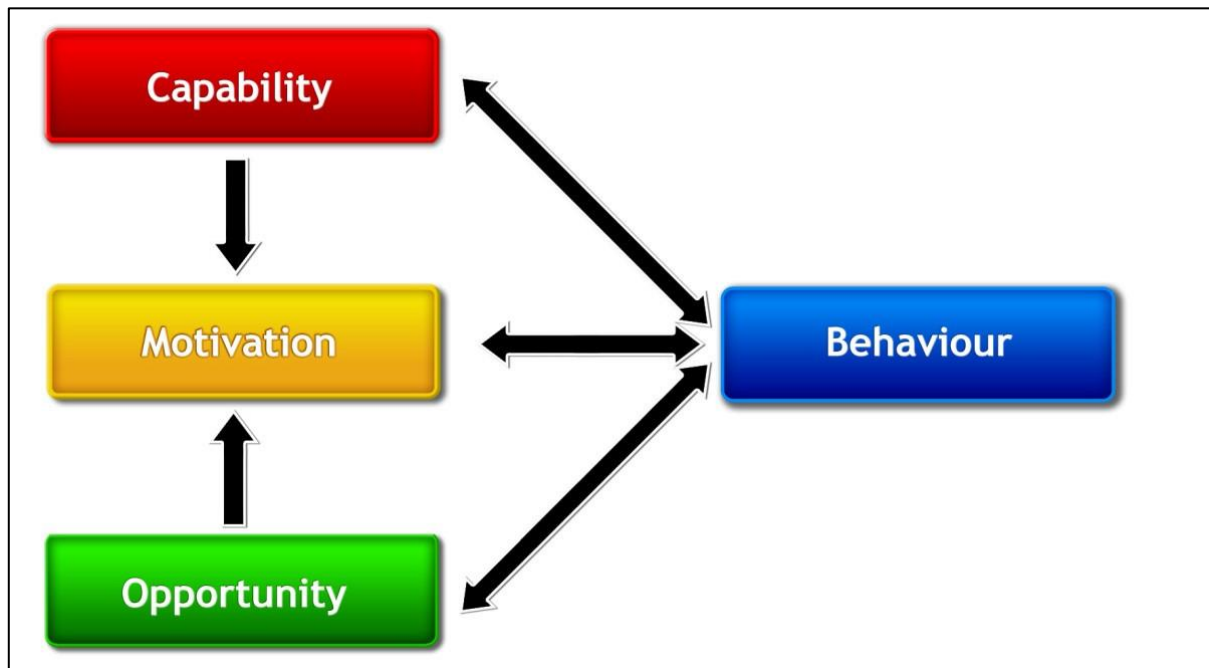
The privacy paradox is the term used when individuals are aware of the cyber risk yet still choose to act in an unsafe way online (Barth & De Jong, 2017). Such as in the situation where those who work within cybersecurity behave in a way that increases their vulnerability to a cyber threat. Barth et al. (2017) suggest that the privacy paradox occurs due to one of two rational processes. The first, risk-benefit calculation, explains that individuals choose to behave in an insecure way online even though they know the potential risk of their behaviour, due to the benefits that accompany behaving in this way. Cognitive biases, such as an optimism bias are considered within this first category of processing. The other type of process is that no or very little risk assessment takes place. This may be due to a lack of knowledge about the information, such as what is considered in the KAB model, which may be the situation in the case of military Key Relations as they might lack the knowledge of the extent their behaviour influences cyber resilience in the military. Alternatively, lack of risk assessment may occur because the desired outcome is more beneficial than the risk assessment, such as due to social conformity and peer pressure (Barth & De Jong, 2017). In the case of military Key Relations if there is peer pressure to post military information online, such as to receive validation or praise from peers, this may result in Key Relations choosing to act in an unsafe way online, despite them having the knowledge it is unsafe to do so.

## 2.8. The COM-B system

One theory often used within military research to explain behaviours and behaviour change is the Capability-Opportunity-Motivation-Behaviour (COM-B) system. This system explains how human behaviour is influenced by three components, Capability, Motivation and Opportunity that interact with each other and are in turn influenced by behaviour. Figure 2.2. demonstrates the directional relationship between these three concepts and behaviour. Capability is the ability to engage in a specific activity and Michie et al. (2011) explain there is a distinction between physical and psychological capability. Motivation is the brain processes that direct our behaviour and consists of reflective processes such as evaluative plans, and automatic processes that use our gut instincts and innate dispositions. Opportunity is the factors that prompt behaviours which are external to the individual, these can be either an environmental opportunity or a social opportunity, which is dependent on culture.

**Figure 2.2.**

*The COM-B model (Michie et al. 2011) demonstrates how individual Capability, Motivation and Opportunity influence human behaviour.*



The COM-B model has been used by previous research to explore behaviour change in cybersecurity training, education and awareness. Alshaikh et al. (2019) created a framework to map how a cybersecurity intervention based on the COM-B model may address the behaviour change required for individuals to engage in secure cyber behaviours. An example of how this was done considers the Capability concept of the COM-B model. One example of a physical capability behaviour they suggested is the lack of skill to identify phishing emails, whereas a psychological capability could be a lack of knowledge about the consequences of clicking on a phishing link (Alshaikh et al. 2019). As part of this framework suggestions for interventions were able to be identified. For the Capability behaviour examples provided, they recommended education and training interventions to encourage behaviour change and adoption of safer online behaviours. However, when considering the entire COM-B model, even the addressing gaps in Capability may not result in the desired behaviour if there is no Motivation or Opportunity (Michie et al. 2011). For example, cybersecurity education and training interventions may result in the adoption of safer online behaviours (Alshaikh et al. 2019) but only if there is the Opportunity for Key Relations to take part in these initiatives, which may not occur if there is a lack of resources available for military organisations to set up initiatives.

The military often uses the COM-B model to understand and implement behaviour change within the military process. Some examples of behaviours that have been explored within a military context when using the COM-B model were pro-environmental energy behaviours (Smaliukiene et al. 2020), healthcare access (Born & Frank, 2023) and physical activity amongst veterans (Walker et al. 2022). The use of the COM-B model to explore behaviour in the military is important when considering that military culture influences personnel's behaviour (Smaliukiene et al. 2020). Therefore, this model may be useful in exploring cybersecurity behaviours in the extended military community that adopts elements of military culture.

## 2.9. Military families

### 2.9.1. Defining Friends and Relatives

To explore online behaviours exhibited by the extended military community, a definition of who this consists of is required. Most people have five individuals whom they consider close relationships and who provide advice and comfort in times of trouble, are contacted once a week, and who would be considered the most intense relationships (Dunbar, 2010). Identifying who these individuals could be for military personnel can help determine who could potentially have access to information that could negatively influence military cyber resilience if it ends up in the hands of an actor who poses a risk to UK defence. Before exploring the role of military friends and relatives in contributing to military cyber resilience, these terms should be defined.

In terms of a military relative, the Ministry of Defence provides no clear definition and instead explains that when considering close relationships, such as partners and children, a diverse range of close relationships and situations should be considered (Ministry of Defence, 2023). The Families Strategy from the Ministry of Defence provides direction to policymakers for how to deliver interventions for Armed Forces families and states that relationships may include a variety of long-term relationship types, including marriages as well as civil partnerships, those with children or a role in raising children including stepfamilies, as well as parents and siblings (Ministry of Defence, 2023). However, the National Health Service (NHS) define Armed Forces families as dependents including spouses and children (NHS England, 2024). Broader definitions of a military relative can include relatives through blood, marriage, and adoption, as well as individuals whom service members who have an assumed responsibility to provide care for, such as an unmarried partner (National Academies of Sciences, Engineering and Medicine, 2019). However, some academics argue that the Ministry of Defence only considers those relationships in a 'nuclear' and heterosexual family (Sewart, 2022). Research involving the extended military community, including friends and relatives, still primarily focuses on traditional and heteronormative families, without considering dual-serving couples, LGBTQ personnel, unmarried relationships, and male partners (Gribble et al. 2020).

Friends as well as relatives, can be important in our lives. Rözer et al. (2016) suggest that primary contacts are people who take an active role in an individual's life. These people engage in activities together and are someone with whom individuals feel close and intimate. This relationship could come from either a relative or a non-relative and is defined by Rözer et al. (2016) as a 'personal network'. The fact that support can come from any individual relative or not is the same for military personnel. McCabe et al. (2020) suggest that support from friends can moderate depression symptoms for military personnel following trauma exposure. Support from friends can potentially be more beneficial in certain situations than support from relatives, as friendships tend to be stress-free whereas relationships with relatives are dynamic and can cause additional stress (Laffaye et al. 2008).

Research suggests we draw on diverse types of relationships depending on the type of support that we need, as family members may provide unconditional support whereas friends may share similar interests and introduce individuals to current ideas (Rözer et al., 2016). Additionally, the composition of our relationship networks and whether they consist of friends or relatives may differ due to additional factors such as personality and age (Buijs et al. 2023). The current thesis intends to provide more insight into which friends and relatives military personnel consider important in their lives by creating a definition of 'Military Key Relations.' As discussed

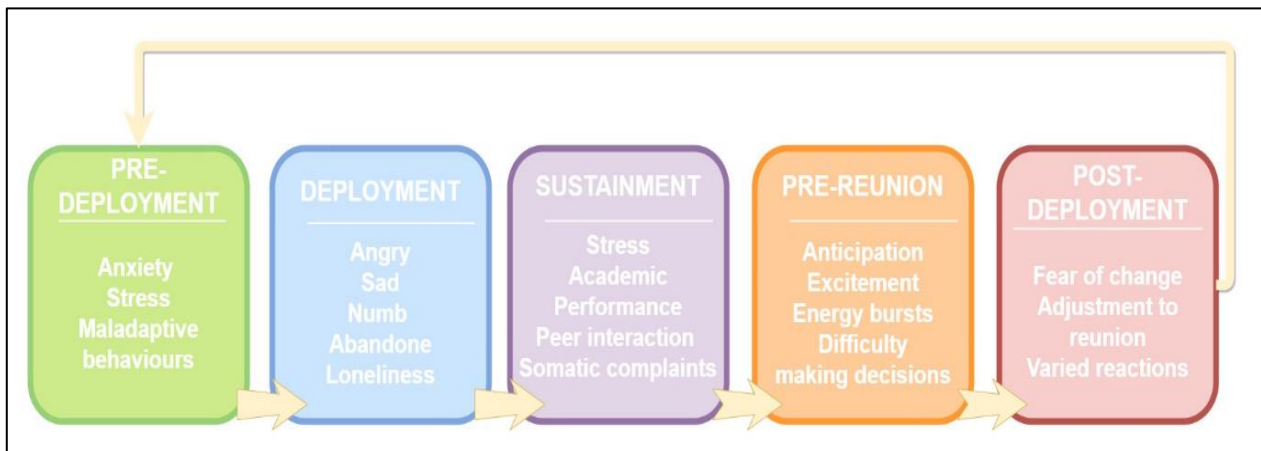
at the beginning of this section, Dunbar (2010) explains that everyone has five close relationships, that could consist of friends or relatives, who provide advice and comfort, and are contacted once a week. In this thesis the terms 'Key Relations' will be used to describe any friends and relatives military personnel would consider in their circle of five close relationships. This may not be the same for everyone, and so it is important to identify any potential friends or relatives that could be included in this intense relationship network and in the definition of 'Military Key Relations'. This can provide a clear direction for exploring the online behaviours of these individuals that may influence military cyber resilience, but also other behaviours influenced by being a military friend or relative, such as mental health consequences.

### 2.9.2. Characteristics of military friends and relatives

Whilst military families share characteristics common to all families, they also have unique characteristics which might make them more vulnerable online. One of the key differences for military families is repeated relocations or even separation of service members from their families, due to deployment (Drummet et al. 2003). For those who are active personnel, relocation might typically occur every 2 to 3 years, and this may be an accompanied relocation with family or unaccompanied. However, separation of families can occur during relocation due to other variables such as a partner's job, family members requiring care or a pivotal point in a child's schooling occur (National Academies of Sciences, Engineering, and Medicine, 2019). This can be an exciting time, providing an opportunity to travel or move to a more desirable location. However, the requirement for these families to frequently readjust and integrate into a new life can have adverse effects on individuals' psychosocial health (O'Neal & Mancini, 2021), particularly for spouses (Ribeiro et al. 2023) and adolescents (Wadsworth et al. 2022). Smith (2015) discusses how maintaining a work-life balance where both career success and family happiness and well-being are prioritised can be even more challenging for dual-serving families. Dual-serving families are those where both parents are actively serving in the military. For spouses, problems because of military relocation such as employment, education social support or healthcare have been shown to be associated with greater psychological stress, including depression and stress (Ribeiro et al. 2023). However, a large amount of this research focuses on female spouses (Bailey, 2019) and on married spouses, without considering significant others who are not married (Ribeiro et al. 2023). For adolescents it has been shown that relocation due to a military parent is associated with higher levels of depressive symptoms (O'Neal et al. 2022) and for adolescents in military families there is also a higher rate of suicide attempts compared to adolescents in nonmilitary families (Clements-Nolle et al. 2021). However, the severity of these factors may depend on the length of deployment and some changes may be due to maturational development rather than the impact of deployment (Meadows et al. 2017). Fitzsimmons and Krause-Parello (2009) put forward a model of the emotional stages that family members experience when their military person is deployed. The full steps and emotions that children can experience, as outlined by Fitzsimmons et al. (2009) are visualised in Figure 2.3.

**Figure 2.3:**

*Emotional stages of deployment model using Fitzsimons and Krause-Parello's (2009) description of the emotional stages of deployment*



Research exploring how to mediate the negative effects of military deployment and relocation on friends and relatives highlights the importance of continued social connection (Skomorovsky, 2014; O’Neal et al. 2022). For spouses, this social support may come from family, nonmilitary friends or their military partner, among others. Rea et al. (2015) found that in a small sample of military spouses, 100% reported using online communication to maintain a connection with their deployed spouses and reduce loneliness. However military spouses use some social media sites, such as Facebook, for reasons other than communicating with their partners or other family members, such as connecting with other military spouses or finding support from spouses who have experienced deployment and can offer support (Rea et al. 2015). Social media can also be used by spouses who have relocated and are looking to integrate themselves into a new environment, as social media sites can also be a source of information on military-funded service events (Rea et al. 2015). Bittner (2014) also found that sharing pictures of events online can increase the openness of conversation and friends and relatives and create another avenue for social support.

### 2.9.3. The influence of Key Relations experiences on cyber resilience

Operational success and day-to-day efficiency within the UK’s Armed Forces is reliant on information and communications technology, which can be fatal if compromised by a cyber-attack (House of Commons, 2013). One of the concerns or threats that friends and relatives of military personnel pose is information leakage, which refers to both the deliberate and accidental sharing of private or sensitive information to an unauthorised party (Yahav et al. 2014). Denying mission information, such as details about individuals, locations, and other information such as weapons, to an adversary is part of operational security. Operational security is a key part of planning and completing a successful military operation (Davis, 2011). One of the challenges for organisations when considering friends and relatives is the lack of control over their behaviour, particularly when these individuals have a lack of knowledge about what is appropriate to share online (Cascavilla et al. 2015). This is particularly challenging when it comes to the use of social media and other forms of online communication. Garside et al. (2012) suggest that the lack of knowledge from friends and relatives about tools such as Facebook’s geo-location system, which can identify where the user has logged in and display this on their profile,

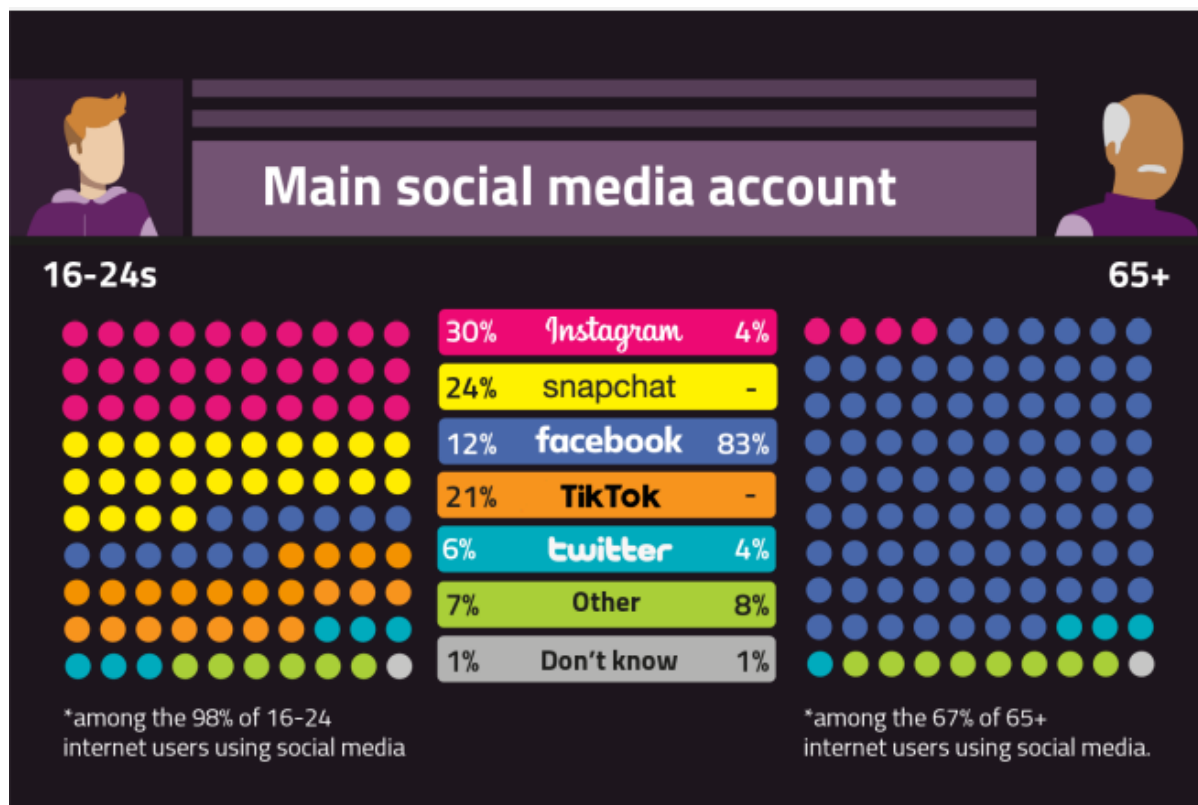


can provide sensitive location information such as the location of military barracks, without the user even intending to. This is a concern for other social media applications, such as Instagram, whose precise location tracking of users is automatically enabled and requires individuals to be aware of this setting to disable this tool (Castro, 2022). There are concerns that existing technological approaches to reducing information leakage don't address the problem of human users subverting a computer's control to leak data (Sandhu, 1998). These technology-based approaches do not align with the research that suggests that addressing cyber resilience should be human-centred (Erstad et al. 2021). However, sharing pictures containing operational information with others inadvertently is a potential cyber risk for military organisations, due to the threat of Cybercasing (Garside et al. 2012). Cybercasing involves using online tools to examine publicly available geo-information to make inferences about the location in the real world, for dubious purposes and can be done with intense accuracy by simply entering the geo-coordinates, embedded into a photo taken on a phone, into Google Street View (Friedland & Sommer, 2010). This can create a potential threat of friends and relatives inadvertently sharing information about approximate military base locations, due to the vulnerability of loneliness and attempting to stay connected with others.

In adolescents, the negative effects of relocation are moderated by social support, from family members and friends (O'Neal et al. 2022). It has been also found that teenagers within military families benefited from interacting with other military teenagers, during the deployment period (Meadows et al. 2017), therefore creating a need for the use of social media for these adolescents to stay connected. Adolescents may pose a different threat to cybersecurity than other family members due to the variation of the social media platforms that they use. Auxier and Anderson (2021) explored the use of social media platforms for different age groups and found that Facebook was used a similar amount regardless of the population age, with 70% of 18–29-year-olds reporting using Facebook, 77% of users aged 30-49 years old and 73% of users aged 50 to 64 years old. Comparatively for newer social media apps such as TikTok, 48% of 18–29-year-olds reported using TikTok whereas this drops to 22% for those aged 30-49 and 14% for those aged 50-64. This demonstrates how the threat landscape might be different depending on the age of the friend or relative and is also an important consideration for those who are on the other end of the age scale, such as parents or grandparents. Figure 2.4 demonstrates how the use of social media platforms differs depending on age in a UK population (Ofcom, 2022). Older relatives, such as parents or grandparents are not often considered in research on friends and relatives of military personnel unless they are dependent on the individual in the military (National Academy of Sciences, Engineering and Medicine, 2019). This creates a gap in the knowledge of how frequently they might communicate with their military counterparts, and how much access they might have to sensitive knowledge that could create a risk for military organisations.

**Figure 2.4:**

Findings from an Adult's media use report demonstrating the difference in social media platform usage for those aged 16-24 years old, compared to users aged 65+ years (Source: Ofcom, Adults' Media Use and Attitudes report 2022)



One example of where social media caused reputational damage for the military was during the COVID-19 lockdown, where a video was shared of a ship's crew having a BBQ on a submarine whilst it was docked for repairs. The personnel presented no risk of spreading COVID-19 at this time due to being at sea on the ship together for months previously. However, the damage done because of the video being shared online resulted in the Captain being removed from Command (Haynes, 2020). Another similar incident was the leaking of a video which showed an F-35 fighter jet crash following a take-off failure on an aircraft carrier. The video was leaked from inside a Navy WhatsApp group (The National, 2021). A more recent example is the revelation through Russian media that they had been eavesdropping on a call between German Air Force officers and overheard the suggestion that UK military personnel were actively deployed in Ukraine (Forces Net, 2024).

Whilst these examples are not specifically related to risk behaviours of military friends and relatives, they demonstrate how once information is shared online, it spreads quickly with potentially damaging consequences to the reputation of the Ministry of Defence. Reputational damage may also occur because of military friends' and relatives' online behaviours. One example that specifically focuses on the role of military friends and relatives in contributing to cyber risk is an example of a US Air Force employee sharing classified information from briefings

on the war in Ukraine with an individual on an online dating site. The employee worked for the US Strategic Command and shared information about Russia's military capabilities with an online profile that claimed to be a woman living in Ukraine (Liebermann & Britzky, 2024). This case also demonstrates the importance of considering short-term relationships, as well as long-term relationships when identifying which military friends and relatives could influence organisational cyber resilience.

#### 2.9.4. Barriers to behaving safely online in a military context

One limitation of the existing research into how Key Relations influence organisational cyber resilience is that there is no clear and consistent definition of which military friends and relatives should be considered a Military Key Relation. Whilst strategies put forward by the Ministry of Defence suggest a wide range of situations should be considered when identifying close relations, in practice it is only those known to the organisation as next of kin whom military organisations engage with (National Academic of Sciences, Engineering and Medicine, 2019). This may mean that when addressing the risk behaviours of friends and relatives and how they might impact military organisations' cyber resilience, there may be a wide range of individuals who are not being considered. Additionally, much, though not all, of the research on Cybersecurity Culture focuses on encouraging individuals to comply with information security or cybersecurity policies (Uchendu et al. 2021). However, there is no evidence in open-source literature that there is a clear cybersecurity policy for military friends and relatives to comply with. Even if this policy did exist, military friends and relatives may experience difficulties in engaging with some security behaviours. For example, they may be reluctant to engage in threat or incident reporting due to the perceived pressure to conform to military standards. It has been suggested that there is a perception within military families that the family informally carry the rank of the military counterpart and that any behaviour from friends and relatives can negatively impact on the service member's career (Drummet et al. 2003). Whilst this may seem like an outdated concept, service member spouses still report that they are often required to represent their military person at events and embody the values of military culture (Harrell, 2001). In research into health behaviour, it has been found that this concern makes family members reluctant to ask for help when required, due to concern about how this may represent the service member (Drummet et al. 2003). Therefore, if friends or relatives inadvertently engage in a cyber risk behaviour this may make them reluctant to report it to a contact at the military organisation, even if it is encouraged.

Other research on healthcare within a military family sample identified that often interventions do not get completed by friends and relatives due to relocation or deployment (Lester et al. 2012). This suggests that creating a cybersecurity training and awareness programme for military friends and relatives should consider this potential barrier and ways to address it. Initiatives for cybersecurity may be different due to the potential to disseminate education and awareness materials via post or online, and to conduct training initiatives online. However, there is a requirement to explore any potential barriers in a cybersecurity context, to understand the extent of relocation or deployment, and any other possible factors that impact engagement from Key Relations. Encouraging responsibility and accountability for friends and relatives could counteract barriers to participation in military led interventions, such as fear of asking for help or advice or lack of commitment of these individuals due to relocation (Drummet et al. 2003; Lester et al. 2012). Identifying who is accountable and responsible for the behaviours of Military Key Relations is currently not clearly defined within the research and can be a challenge for military organisations due to a lack of control over the behaviour of individuals who

are not employed by the organisation (Cascavilla et al. 2015). Therefore, this presents a gap in the literature that should be addressed to ensure any future engagement with Military Key Relations over their online behaviour in a military context, is effective in contributing positively to military cyber resilience.

## 2.10. Existing ways of addressing threats

Criticisms of the existing literature addressing the human vulnerabilities of cybersecurity suggest that often the focus is on understanding the security issues, without addressing or mitigating them (Alnifie & Kim, 2023). When focusing on social media or social networking sites, the guidance for military personnel on social media usage is reportedly inconsistent. Some recommendations discourage the use of social media entirely whereas other recommendations address how social media can be used securely (Garside et al. 2012). However, Garside (2012) also explains that in a society where social media is prevalent for work and non-work tasks, discouraging individuals from using social media at all is not an effective way of addressing cybersecurity risks. Therefore, encouraging individuals to engage in secure online behaviours when using the Internet is a more effective method. This section discusses the recommendations and challenges with existing cybersecurity training, education and awareness frameworks.

### 2.10.1. Cybersecurity training, education and awareness

When considering the factors that make cybersecurity, training education and awareness initiatives successful multiple factors are highlighted. These include ensuring that campaigns are targeted and specific for the individual, that individuals can take action on the information they are provided, and that feedback can be provided following engagement with the initiatives (Bada et al. 2015). Aldawood and Skinner's (2019) research into the limitations of training and awareness programmes for social engineering provides an explanation for why programmes are ineffective, based on the targeted portion of Bada et al.'s (2015) requirements above. They explain that the influence of social factors, such as culture, may limit the effectiveness of training and awareness programmes. This may be due to concepts like national culture being carried over into the workplace, rather than people applying different cultures inside and outside of the workplace. However, when considering the role of national culture in cybersecurity training programmes, one recommendation is for government legislation that highlights the importance of cybersecurity training for protecting against cybersecurity threats (Aldawood & Skinner, 2019). Government legislation would be beneficial in encouraging all individuals within society and consequently within an organisation to engage with cybersecure behaviours. When considering military friends and relatives, this would be beneficial to address the challenges of military organisations having limited access to engage with military friends and relatives.

In support of Aldawood and Skinner's criticism of cybersecurity training programmes, Bada et al. (2015) suggest that national culture, including Hofstede's dimensions outlined earlier in this Chapter, is one factor that influences the success of behavioural change. They advise that for a Western culture, such as the UK, that values individualistic national culture attributes such as individual goals preferences and attitudes, it is better to present the risk of not being secure rather than the benefits of being secure. However, research into using fear appeals to change behaviour might be insufficient as they may result in individuals being paralyzed from making a cybersecurity-related decision and are ethically questionable if they result in psychological harm due to unnecessary anxiety and paranoia (Dupuis & Renaud, 2020). Considering the potential of using fear to highlight the importance of military friends and relatives' online behaviour in a military context, the association with operational failure has the potential to have an extreme adverse psychological impact on friends and relatives if they perceive fatalities as their fault.

As well as the challenges highlighted above there is often a lack of interest and motivation from individuals to engage with regular cybersecurity training. In this way, providing individuals with educational materials on the importance of secure online behaviour and how their behaviours contribute within an organisation could be beneficial. This being said, Hadnagy (2010) suggests that educational materials for cybersecurity are also ineffective if individuals do not demonstrate an interest in learning about cybersecurity. They highlight that individuals can display a lack of interest if they do not believe that cybersecurity concerns them. This is consistent with Ramachandran et al. (2012) and their findings that the majority of people do not believe the responsibility for cybersecurity in an organisation lies with them but instead lies with cybersecurity professionals. In this way, pinpointing responsibility for individuals' role in cybersecurity may be pivotal for ensuring engagement with cybersecurity training, education and awareness materials.

One way of reducing the risk that online behaviours present to organisational cyber resilience is by encouraging people to adopt secure behaviours using cybersecurity awareness campaigns. Awareness campaigns differ from cybersecurity training as they do not train people to behave this way but merely make them focus their attention on what should be done to reduce cyber risk and how this might be done (Bada et al. 2018). Bada et al. (2018) highlight multiple gaps that exist when it comes to best practices for Cybersecurity awareness campaigns. Often there is a lack of understanding about what cybersecurity awareness is, supplemented by campaigns that are disengaging and distributed without evaluating how appropriate and representative of the threat landscape these campaigns are. When discussing existing cybersecurity awareness campaigns in the UK, Bada et al. (2015) discuss Get Safe Online, an organisation that frequently partners with military organisations (Get Safe Online, 2024), and is often recommended to family and friends of military personnel to provide them information on basic cyber hygiene behaviours. Bada et al. (2015) highlight that the limitation of the awareness provided by Get Safe Online is that it relies on individuals understanding the information and applying it to their context. Get Safe Online provides extremely useful insight into how users should behave when using social media to keep themselves and others' information secure. However, this may not provide sufficient detail for Military Key Relations about what is acceptable for them to post with regard to military information. For example, the advice to not post information about your holidays online until you return could apply to military deployment or relocation, but this requires friends and relatives to make that link themselves, which they might not consider. Get Safe Online's previous work with the Royal Air Force (RAF) did provide leaflets that consider online safety in the context of national security, but often focussed on the perspective of the serving person (Royal Air Force Families Federation, 2020). Additionally, this information was only accessible for a short amount of time, as most of the links provided on the RAF website are now broken, meaning that personnel nor their friends and relatives can look back to remind themselves of the guidance for staying safe online.

## 2.11. Literature review summary

When discussing how the culture within a military organisation can potentially differ from other organisations, the literature review indicated that military culture may also impact military personnel's loved ones. However, when reviewing the literature on definitions of friends and relatives, there was inconsistency and a lack of clarity over which individuals should be considered as Key Relations of military personnel. To explore how military personnel's friends and relatives may contribute to organisational cyber resilience, there is a need to define Military Key Relations. As part of exploring the characteristics of Military Key Relations, the literature

review highlighted the reliance of military personnel and their friends and relatives to use online communication due to the nature of a military lifestyle, including relocation and deployment. When considering their online behaviours the literature review highlighted risk behaviours associated with social media, particularly related to military information and location sharing, though behaviours may differ due to factors such as age. However, a gap in the literature exists that provides a clear indication of the potential online behaviours Military Key Relations engage in that could present a risk to military cyber resilience. The literature review highlighted how online risk behaviours in any organisation can be addressed through cybersecurity training, education and awareness, though there are existing limitations with the current approaches. The literature that was available and discovered during the literature search did not provide any indication of the current cybersecurity training, education and awareness initiatives that are provided to Military Key Relations. Therefore, creating a justification to identify the current approach to addressing cybersecurity training, education and awareness for Military Key Relations within research, and how this could be improved.

This literature review discussed the importance of encouraging a Cybersecurity Culture within organisations, and that this can be done by focussing on two aspects of culture: accountability and responsibility. Potential ways of increasing accountability when considering information security were discussed, introducing the concept discussed frequently in recent literature of a “just culture” wherein a positive cyber security culture is created through accountability by encouraging lesson learning from incidents rather than blame attribution. The methods of increasing responsibility in Cybersecurity Culture were also explored, and the influence of ensuring all individuals are aware of their role for cybersecurity in the organisation, using a case study example from an Italian Bank. As well as accountability and responsibility, psychological theories that can be used to explain decision-making and behaviour in the context of cybersecurity were examined. When discussing the Theory of Planned Behaviour findings from recent research explored multiple aspects of the theory in the context of cybersecurity behaviours including attitude, subjective norms, perceived behaviour control and an extension of the theory that explores the role of knowledge. When examining these findings, the importance of considering individual differences, such as culture and education was highlighted. Alongside this theory, multiple cognitive biases and their role in understanding behavioural decision-making were explored. This included the role of optimism bias in influencing the decision to engage in secure online behaviours based on a comparison with others and how this might be heightened if individuals perceive they are in control of the situation, based on their presumed competence, as discussed in the Theory of Perceived control.

There was little research found during the literature search that explored these theories in the context of military Key Relations’ influence in cyber resilience for military organisations. Potential challenges were highlighted with applying these to the extended military community, including Military Key Relations, as despite Key Relations often embodying aspects of military culture due to exposure, military organisations have no direct control over their behaviour. Therefore, there is a requirement for research that identifies how to encourage military personnel’s friends and relatives to be accountable and responsible for their online behaviour within the context of military cyber resilience.

## 2.12. Research problem and objectives

### 2.12.1. Research problem

To explore how military personnel's friends and relatives contribute to cyber resilience within military organisations, and address the gaps in the literature above, this research project will explore friends' and relatives' online behaviours. Additionally, the research will consider how potential risk behaviours could be reduced through military-provided cybersecurity training, education, and awareness initiatives. How these gaps will be addressed is outlined in the research objectives below. These objectives aim to answer the research problem: How do Friends and Relatives contribute to Cyber Resilience within Military Organisations?

### 2.12.2. Objectives

*Objective One: To create a definition explaining which military friends and relatives should be considered Military Key Relations*

Currently, there is no clear definition for which individuals should be considered a Military Key Relation. The Ministry of Defence (2023) provides an overview explaining that diverse relationships and situations should be considered. However, existing literature involving military friends and relatives is still narrow and focuses on traditional families (Gribble et al. 2020). Therefore, Objective One reflects on extended family, diverse relationship situations, and the role of friends taking on an active role as a primary contact (Rözer et al. 2016), to create a definition of Military Key Relations. This will allow any future research and initiatives, both within cybersecurity and other areas, to approach and engage with the correct people. Which individuals we consider as part of our relationship networks may differ due to other factors (Buijs et al. 2023) and so the influence of any additional factors, such as communication frequency and relationship strength will be considered. Findings from all three Phases (Chapters 4, 5 and 6) will contribute to this definition. Aim 1 and research questions 1a and 1b from Phase 1 address this objective as they focus on defining which friends and relatives should be considered Key Relations, and whether this varies with age. In Phase 2, Aim 1 and research question 1 address this objective by identifying who military organisations consider Key Relations in the context of cybersecurity. In Phase 3, research question 1a addresses this objective as it also explores communication frequency for different types of relations. The final definition of Military Key Relations will be stated and discussed in Chapter 7.

*Objective Two: To investigate the online behaviours that Military Key Relations engage in, and identify any behaviours that could create a cyber risk for military organisations*

The situational factors of a role in the military, such as relocation and deployment, means that military personnel and their Key Relations rely heavily on online forms of communication to stay connected, receive support and ensure mental wellness (Rea et al. 2015). Whilst social media has many benefits, there is the potential that the use of social media may create a vulnerability in cyber resilience. The risk of using social media insecurely is similar for a civilian and military population. Risk behaviours can include information leaks (Sandhu, 1992) and insecure use of geolocation tools on platforms (Castro, 2022), amongst others. However, for a military population, sensitive information in the hands of a military adversary can be detrimental to operation success, and in extreme cases may result in loss of life (Defense Science Board,

2013). Therefore, it is important to identify any risk that Military Key Relations' online behaviours could present to military cyber resilience.

Due to online communication behaviours having the potential to encompass such a wide array of behaviours, Phase 1 focuses on communication between military personnel and their Key Relations, through research questions 2a, 2b and 3. The findings for what online behaviours occur between Military personnel and their Key Relations will be presented in Chapter 4. This will provide insight into online behaviours that be explored further in Phases 2 and 3. These Phases will consider both online behaviours that are direct between the military person and their Key Relations, and online behaviours Key Relations engage in with any audience. In Phase 2, research questions 2a and 2b address this objective and for Phase 3 it is research questions 1b, 1c and 1d. The findings identifying these behaviours and their potential risk to cyber resilience will be discussed in Chapters 5 and 6.

*Objective Three: To explore current approaches to cybersecurity training, education and awareness for Military Key Relations and how adequately these approaches address potential online risk behaviours.*

With potential online risk behaviours being investigated in Objective Two, this will provide a basis for cybersecurity interventions with Military Key Relations. During the literature search, no publicly available research was discovered that highlighted the current approach for cybersecurity training, education and awareness interventions for Military Key Relations. Cybersecurity initiatives can ensure Key Relations are aware of the threats, how their behaviour could present a vulnerability to these threats, and how they can behave in a way that ensures no risk occurs to military organisations due to their online behaviour. Therefore, this creates a justification for exploring the current approach to cybersecurity initiatives for Military Key Relations and presenting any potential recommendations for how future initiatives can improve upon the current approaches. Chapter 5 will begin to discuss the findings of this objective from the perspective of military representatives and subject matter experts, with research questions 1 and 3 addressing this objective. Aim 3, in Chapter 6 will explore these current approaches in more detail, from the perspective of Military Key Relations, through research questions 3a, 3b and 3c.

*Objective Four: To determine who should be responsible for ensuring Military Key Relations behaviour is not detrimental to Military organisation's cyber resilience and determine accountability for the consequences of Military Key Relations online risk behaviours.*

Of the literature that is openly accessible, there is no clear information security or cybersecurity policy outlining the roles and requirements for Military Key Relations online behaviours, to guide how they can protect military information when using the Internet. Therefore, this research will explore the perspectives of military personnel and Subject Matter Experts (SMEs) in cyber education & awareness and cyber incident reporting & monitoring in Defence and, Military Key Relations. Understanding the opinions of these groups will guide recommendations for who should be responsible for ensuring Military Key Relations are behaving in a way online that does not present a vulnerability to military organisational cyber resilience. Consequently, this will also help guide where the accountability lies should a Military Key Relation behave in a way online that presents a vulnerability for a military organisation. In Phase 2, research question 3 addresses this objective and is discussed alongside findings that focus on responsibility and accountability in Chapter 5. However, due to the findings from all the



Phases focusing on providing insight into responsibility and accountability, this will be discussed further in Chapter 7.

## Chapter 3 - Methodology

### 3.1. Chapter Introduction

In this chapter, the choice to apply a mixed-methods methodology to the research is discussed. The challenges of working as an external researcher within a military context and gathering data within the extended military community are explored, including access and depth of information due to military classification. Techniques applied to tackle these challenges are outlined. The methodology that will be employed for Phases 1, 2 and 3 is discussed, along with justifications for methodological choices for each phase of the research project. The rationale for methodological choices in this chapter comes from an evaluation of the potential methodology approaches and also aligns with the guidelines for ethical approval from Dstl's Scientific Advisory Committee (SAC) and the Ministry of Defence Research Ethics Committee (MODREC). Due to having to justify methodology choices so they align with the requirements of these panels, extra consideration and reasoning were required for the decisions made.

### 3.2 Using a mixed-methods approach

This research used a mixed-methods approach, defined as the use of qualitative and quantitative approaches to provide a deeper understanding of a question or problem (Creswell & Plano Clark, 2018). This research project takes a sequential mixed-methods approach, wherein each phase of the research project guides the next phase. In a mixed-methods approach each distinct phase has individual aims and objectives, all Phases of the research and their relevant quantitative or qualitative methods interlink or mix to answer one overarching problem (Creamer, 2018). For the current research, the three sequential studies have their own quantitative and qualitative research aims and questions. However, these three phrases interlink to address the problem: How do Friends and Relatives contribute to Cyber Resilience within Military Organisations?

A mixed-methods approach encourages holism within research (Lieber & Wiesner, 2010). This is appropriate for the current thesis as Key Relations' behaviours are situated within the context of themselves as individuals but also within the wider military community. Key Relations' behaviour interacts with the military person they are connected to as well as military units and branches and the other serving personnel within them. The use of a mixed-methods approach also satisfies the requirement to disseminate findings to a variety of stakeholders at varying degrees of detail (Lieber & Wiesner, 2010). Quantitative findings lend well to communicating results to military personnel to use and disseminate amongst military units. Comparatively, qualitative findings deepen the understanding of how Key Relations understand their role in contributing to military cyber resilience to justify decisions made when creating future interventions engaging Key Relations and providing a deeper context for academic audiences.

### 3.2. Reflection on challenges of data collection within the military

Due to the research project being funded by defence and involving military personnel, there was a requirement to obtain favourable opinion from MODREC. Two separate ethics protocols were required, the first detailing Phases 1 and 2, with the second outlining Phases 3 and 4. Whilst Phase 4 was not completed as part of this research project, ethical approval was sought to conduct a pilot study and presents an opportunity to continue this Phase of the

research following the submission of the Thesis, as part of a broader programme of work with Dstl, and is discussed further in [Section 3.6](#). It is important to note that throughout this process methodological guidelines were followed to comply with MODREC which were implemented by the researchers, including refining survey and interview questions to be accessible for all participants.

Due to the research needing to comply with requirements for Dstl, access to military personnel and subject matter experts (SMEs) was facilitated by Military Advisors. This was beneficial in contacting hard-to-reach communities and was successful for Phase 2 of the research when contacting military representatives and Subject Matter Experts (SMEs). The challenge of this approach arose in the Phase 1 survey, as a survey link was posted on various discussion boards and intranet forums. This was done to remove any potential pressure to participate that might arise if a call for participants came from senior ranks, as this has the potential to make participation not completely voluntary. Posting the advert on discussion boards and intranet forums allowed participants to read about the study in their own time and decide whether it was something they would like to participate in rather than something they were compelled to participate in due to the hierarchical nature of the military. Assistance from Military Advisors as gatekeepers was used in this study to facilitate promotion of the study in areas that I could not access as an academic researcher. The use of this approach to recruitment meant that I could not address low engagement with the survey directly and multiple follow-up contact emails were required with the gatekeepers to reshare the study advert. Challenges also arose as Military Advisors are serving military members and so would often be away from emails for multiple weeks at a time, due to being on military exercises. When I realised this, I relayed all communication through the Dstl Technical Partner who was able to contact the Military Advisors more directly in person, or when attending other collaborative events. Whilst this resulted in more successful contact, it was time-consuming. This resulted in delays in reaching the required minimum number of participants for Phase 1.

Whilst the research is match-funded by Dstl, with outcomes from this thesis feeding directly into Dstl, I did not hold security clearance throughout this research. Despite being an independent researcher, the research was endorsed by Dstl. This was indicated to participants by including the Dstl logo on recruitment adverts. This demonstrated the credibility of the research to participants and attempted to provide reassurance that their information would be processed appropriately. Whilst someone from within Dstl with clearance and networking access potentially would have produced a higher uptake of participation, there were benefits of being an independent researcher. For example, participants may have felt reassured to provide more detail due to a lack of fear of potential repercussions. There was also no power dynamic interplay between the researcher and participants as I do not hold a military or civilian rank. All cited sources are from open-access articles and data collected and analysed within this research is classified at OFFICIAL. Information at this classification may be sensitive and is still subject to General Data Protection Regulation [GDPR] and Data Protection Act [DPA] (2018) regulations but is not subject to heightened threat sources (Cabinet Office, 2023). This potentially limits the depth of data collection and analysis within the research, which is reflected in Chapter 7. This is due to the potential insights into online risk behaviours and threats that military organisations are aware of that are not included in the research. However, the risk of sharing this information with myself without clearance and including them within the thesis would create an increased risk of a military adversary acting on that information. However, this level of classification in this thesis provides a sufficient level of detail to explore the phenomenon and allows the publication of findings in the public domain. There is also no advantage to having identifiable information such as scenarios or personally identifiable information. The research

focuses on exploring all the potential online risk behaviours Military Key Relations could engage in that might influence military organisational cyber resilience. Having access to existing information on these potential behaviours and threats may have encouraged me to focus on these behaviours rather than taking a broad and exploratory approach. In addition, limiting the scope of the approach has the potential to reduce the applicability of the findings to other military organisations and industries working with sensitive information.

### 3.3. Phase 1: Online Survey with military personnel

This section outlines the methodology used in phase 1 of the project, exploring the perspective of serving military personnel across the Front-Line Commands (FLCs), the Royal Navy, the British Army, and the Royal Air Force. Phase 1 aims to define which friends and relatives military personnel consider to be a Key Relation and identify the online communication behaviours between military personnel and their Key Relations. Phases 1 and 2 of this research are interlinked as both phases focus on the perspective of military personnel, compared to Phase 3 which explores the perspective of Key Relations. Phase 1 consisted of survey questions and responses, whilst Phase 2 explored topics and findings from Phase 1 in more detail with the use of qualitative approaches.

#### 3.3.1. Data Collection: Online survey

Data was collected using an online survey conducted on Qualtrics, consisting of a mix of quantitative and free-response qualitative questions. Qualtrics was used as a survey platform due to consistently scoring better across different dimensions of survey platform scores, such as administration, creation and data analysis when compared to other popular survey platforms such as SurveyMonkey (Rea et al. 2022). Qualtrics is also one of the recommended survey platforms by Bournemouth University and an individual account is provided for research by the Bournemouth University Psychology Department. Qualtrics also meets the data collection and storage requirements of Dstl.

When considering data collection methods within cybersecurity, case studies are often considered appropriate. However, only if your topic focus is refined, which is often the case when exploring a specific online threat and target group (Edgar & Manz, 2017). However, as identified in Chapter 2, the topic focus of this thesis is exploratory and encompasses a broad range of individuals within the wider military community. Phase 1 aims to identify the target group of Key Relations. Only once the friends and relatives are defined and the target group has been identified can the research attempt to understand their vulnerabilities and threats. Therefore, the use of case studies is not appropriate for such novel definitions. Naturalistic observations of military personnel engaging with their friends and relatives could potentially have demonstrated the strength of a connection between military personnel and their friends and relatives and consequently suggest who should be considered a Key Relation. The use of a naturalistic observation like this is beneficial over potentially distorted self-report data to provide a more informative overview of behaviour, however, this may not be accurate due to individuals altering their behaviour due to being observed (Coolican, 2018). This advantage is outweighed by the challenge of arranging access to this population in a natural setting and observing them. Even if access could be arranged, individuals being observed often alter their behaviour due to being monitored, creating reactivity effects (Coolican, 2018). There would also be logistical challenges with observing the communication behaviours of personnel and their Key Relations when on

deployment, even if conducted online. Online surveys which are not completed in the presence of a researcher, or any other authority figure demonstrate minimal reactivity effects. Online surveys can even be useful in reducing the effects of social desirability bias which can be seen in other data collection methods. Social desirability during observation could occur due to the influence of the researcher or even due to observation from types of friends or relatives. For example, social norms suggest individuals should display a stronger relationship with their spouses or children, compared to their friends. If participants are being observed by a spouse or child, or even the researcher, they may choose to respond in a way that fits with these social norms rather than responding in a way that accurately reflects their feelings.

Surveys are the most common data collection method used to explore Cybersecurity Culture (Uchendu et al. 2021), particularly when focusing on aspects of security culture such as accountability and responsibility, which are both key aspects of this thesis. The choice to conduct an online survey rather than via phone or in person is due to the low-cost advantage of creating and delivering these surveys. Additionally, online surveys can reach many people easily (Edgar & Manz, 2017), which accounts for the target population of serving military personnel across the FLCs in both the UK and those serving in different countries. Using a survey accounts for time differences as participants can complete a survey at a time which is convenient for them. The use of surveys also encourages privacy as it means that personnel do not need to find a private room or a secure phone line to complete the survey. However, criticisms have been made addressing this frequent use of surveys to explore Cybersecurity Culture. Concerns include the primary focus on quantitative data and the limitation of surveys and questionnaires to be able to accurately measure behaviour (Uchendu et al. 2021) or explain cause-and-effect of this behaviour (Jackson, 2011). Additionally, military personnel may experience survey fatigue due to the multitude of other surveys they complete (Miller & Aharoni, 2015). These limitations can be addressed by considering that Phase 1 included qualitative questions, as well as quantitative, to provide individuals the opportunity to explain their responses in further detail. Additionally, the topics from Phase 1 will also be explored in more detail in Phase 2, which will use a qualitative approach of semi-structured interviews. The combination of these approaches allows for initial quantitative insight to be supplemented by a more detailed explanation of qualitative findings. The full Phase 1 survey can be found in [Appendix A](#) and further detail about the question topics and participant sample will be discussed in Chapter 4.

### 3.3.2. Data Analysis: Frequency Analysis and Qualitative Content Analysis

Quantitative responses from the survey were analysed using frequency analysis, with Qualitative Content Analysis being used to analyse Qualitative Responses. A frequency analysis was chosen for quantitative responses as analysing the frequency distribution and percentage scores for individual values is useful in identifying patterns in the data (Coolican, 2018). Frequency analysis was appropriate due to this being an exploratory study where the strength of relationships is not known in advance. The explorative design of this study also justifies the analytical approach of the qualitative responses, as Qualitative Content Analysis, specifically inductive category development, is appropriate for exploratory research (Mayring, 2014). Frequency analysis allowed us to identify how many participants consider each friend or relative to be a key relation. However, this analytical approach also provided patterns in the data, to determine if military personnel's definition of a key relation alters depending on participants' age or any other factors. Exploring patterns in the data is appropriate to address the aim of Phase 1 which is to define who military personnel consider to be a key relation. Exploring patterns in the

data provided the opportunity to identify any interplay of factors such as the strength of the relationship, frequency of contact, and topic of conversation. Any patterns within these other factors might influence whether a key relation could potentially be a risk to military cyber resilience. Other quantitative methods were considered to provide a more in-depth exploration of these patterns. For example, a Chi-squared test to explore statistical significance in differences in categories of these variables. However, as mentioned above due to this being an exploratory study, the categories were not pre-determined. This phase aims to simply identify who Military Key Relations are, rather than specifically looking at differences in these variables. Due to the challenges of recruitment and the potential to only have a small sample, the decision was taken that frequency analysis is sufficient to provide insight into this topic and create a justification for the definition created of 'Military Key Relations' with the recommendation that any patterns identified should be studied in further depth in future research. Chapter 2 discusses how the definition of a dependant as a military friend or relative is outdated. Frequent distribution can identify if a wider range of friends and relatives should be considered a 'Military Key Relation'.

Due to this Phase of the research also collecting qualitative responses, a Qualitative Content Analysis was used. The use of Qualitative Content Analysis is useful in exploratory research but is also beneficial for mixed-methods research (Mayring, 2014), and so was appropriate for analysing the survey responses. An inductive analysis was used to analyse the qualitative responses in Phase 1, wherein the categories were created from the responses. The use of an inductive content analysis over a deductive one was chosen to the research project being an exploratory study, and there being limited existing knowledge in this area (Elo & Kyngäs, 2007). The steps followed for an inductive qualitative content analysis included open coding, creating categories and abstraction (Elo & Kyngäs, 2007). This was completed for each survey question with qualitative responses. The first step involved reading through the responses and generating categories based on the responses. The number of categories was then reduced by grouping responses which belong to similar and overlapping categories. Finally, the categories were labelled using content-characteristic words, this is the process of abstraction. Chapter 4, provides more detail about this approach, including an example of how one category was created and named based on the responses.

### 3.4. Phase 2: Online semi-structured interviews with military personnel and Subject Matter Experts (SMEs)

Phase 2 of the research built on responses from the Phase 1 survey, by gathering the opinions of military representatives from each of the Front-Line Commands (FLCs) alongside opinions from Subject Matter Experts (SMEs). Phase 2 used the definition of Key Relations identified in Phase 1 to explore in further detail the online risk behaviours of these individuals regarding military cyber resilience. Opinions from military representatives and SMEs were discussed in online semi-structured interviews.

#### 3.4.1. Data Collection: Online semi-structured interviews

Phase 2 used semi-structured interviews to collect data, which were conducted on Microsoft Teams. To identify cybersecurity risks and how to address them, it is necessary to understand how humans behave in an attempt to successfully interact with online systems and data (Edgar & Manz, 2017). The use of a qualitative approach for this phase allowed for a deeper understanding of the topics being discussed to identify why friends and relatives might be

behaving in a way that impacts military cyber resilience. This expands on simply identifying what these behaviours might be, as was the intention of the approach for phase 1 of the research. Within cybersecurity research the use of existing models or theories to answer a problem can be limited as they don't yet exist, and so seeking expert opinions can be beneficial to evaluate the results of studies (Edgar & Manz, 2017). Seeking the opinions of SMEs alongside military personnel in this phase helped provide a suggestion for whether the behaviours identified in phase 1 could present a risk to military cyber resilience. Half of the SMEs were considered experts in cybersecurity education and awareness in defence, and the other half were experts in cyber incident reporting and monitoring in defence. Gathering the perspective of experts in education and awareness provided an overview of the current approach to cybersecurity initiatives for Military Key Relations, and potential engagement. Exploring the opinions of experts in cyber incident reporting and monitoring provided insight into potential risk behaviours and threats that military personnel may not necessarily possess due to mainly observing the online behaviours of their friends and relatives. Experts will have a broader insight into potential risks, compared to military personnel who may only have insight into the behaviours of those they have direct access to. The insight from military personnel may not be encompassing of all potential behaviours when considering that personnel drawn to the research probably had an interest in cybersecurity that is encouraged or shared with those close to them and may not be reflective of the entire population. Opinions from these experts provided insight that potentially is not distributed in public forums, but in a way that does not provide a concern in sharing sensitive information.

Interviews were chosen as the qualitative approach over alternative qualitative data collection methods such as focus groups. Whilst some researchers suggest that individuals' disclosing sensitive information in focus groups may encourage others to share their experiences and opinions, others have found individual interviews to result in a higher level of self-disclosure due to less intimidation of sharing information with others around (Kruger et al. 2019). This is a large benefit of interviews over focus groups but is particularly key for the participant group, to reduce the influence of rank and seniority of participants and encourage participants to speak more openly. An additional benefit of interviews over focus groups is the opportunity for the researcher to build a stronger rapport with individual participants. This encourages individuals to feel comfortable with sharing their opinions and experiences. This is important for a topic where the researchers want participants to discuss their Key Relations, but also on potential online risk behaviours, as individuals may initially feel reluctant to share information due to fear of disclosing sensitive material. Conducting the interviews online was beneficial as participants were able to take part in the interviews in a quiet place of their choosing. Allowing participants to determine this location, encourages comfortability of participants, which potentially results in increased disclosure. There is also an additional benefit that online interviews are convenient, participants were able to complete the interviews on their day off, or in the evenings when they had free time.

The interviews were conducted using a semi-structured approach. The role of the extended military community in cyber resilience was highlighted as an under-researched area when determining the aims and objectives of this research project. The use of semi-structured interviews allows the discussion to be driven by the experiences and knowledge of military representatives and SMEs, which does not currently exist in the open-access literature. Semi-structured interview question topics, the participant sample and further evaluation of the method will be discussed in Chapter 5. The semi-structured interview schedule is included in [Appendix B](#).

### 3.4.2. Data Analysis: Thematic analysis

Interview data was analysed using inductive thematic analysis to create a thematic map of the reviewed and analysed data. Thematic analysis is a commonly used data analysis method for qualitative interviews and will be appropriate at this phase of the research project as there are no strong theoretical perspectives to drive the analysis from previous research (Howitt, 2019). Interpretative phenomenological analysis (IPA) could be considered appropriate for analysing data in Phase 2 as it focuses on people's descriptions of their experiences and how this can be explained and interpreted by the researcher (Howitt, 2019). This is potentially suitable for Phase 2 as the aim is to explore opinions from subject matter experts (SMEs) on risk behaviours of friends and relatives concerning military cyber resilience. However, IPA focuses on individual experiences, which was not appropriate for this phase of the research as it explores not only individual experiences but also opinions from SMEs about their own and others' behaviours. Using an inductive thematic analysis, rather than a deductive analysis ensured that the data was grounded in participant's opinions and experiences. Inductive thematic analysis was appropriate for this phase as whilst some high-level themes could be derived from the existing literature, such as accountability and responsibility (Coolican, 2018), due to the limited existing literature focusing on Key Relations of military personnel, themes were generated from participant responses.

The use of an inductive thematic analysis pairs nicely with the use of semi-structured interviews to allow participants to provide their experiences and opinions and provide the opportunity for themes to develop based on participant experiences and opinions rather than trying to fit participant experiences into themes derived from the existing literature. Grounded theory is another qualitative data analysis method where themes are generated from the data itself and was considered as an analytical approach for Phase 2 responses as it is a common approach used to analyse data from qualitative interviews (Howitt, 2019). Whilst grounded theory and thematic analysis share characteristics such as the iterative nature of creating themes and codes, thematic analysis was used to analyse data in Phase 2 of this research project. Grounded theory focuses on theoretical sampling to construct a theory from the data rather than providing a representation of the target population (Charmaz, 2015). The aim of phase 2 is to provide a representation of opinions on friends and relatives online risk behaviours from military representatives and a handful of subject matter experts, which does not satisfy the requirements of a grounded theory analysis. Additionally, the final steps of a full grounded theory analysis require collecting additional data to check the theory and research questions created against new data (Howitt, 2019). Due to the limitations of access to the participant group, and uncertainty about reaching the full proposed participant sample, this could limit the successful completion of the final stages of the grounded theory process. Therefore, the thematic analysis followed Braun and Clarke's (2021) six-step approach to an inductive thematic analysis. These six steps involve familiarisation of the researcher with the data, coding the data which then leads to theme generation, theme development, theme defining and report writing. Braun and Clarke's (2021) approach encourage a reflective stance, and so alongside the six-steps analysis, the researcher produced a reflective diary, that formed part of the results and evaluation of responses. Braun and Clarke (2021) also recommend inter-coder reliability, so two researchers independently analysed transcripts and identified themes to determine the validity of the themes created. More details about the process of this analysis, including the results, will be discussed in Chapter 5.



## 3.5. Phase 3: Online survey with Military Key Relations

Phase 3 will use insights from Phase 1 and 2 to explore the topics from an alternative perspective, the Military Key Relations. Phase 3 will recruit friends and relatives identified as Military Key Relations in Phases 1 and 2 to gather their opinions and experiences of how their online behaviour influences military cyber resilience. This will be done using an online survey, which is discussed in more detail, along with the analytical process, in this section.

### 3.5.1. Data Collection: Online survey

Phase 3 used an online mixed-methods survey, conducted on Qualtrics, to collect qualitative and quantitative data. Phase 3 is similar to Phase 1, with many of the questions from Phase 1 being asked of the Military Key Relations in Phase 3, except they were re-worded to consider the perspective of Key Relations rather than serving personnel. This provided an opportunity to identify any differences in responses between military personnel, and their Key Relations, particularly any that might arise due to Key Relations previously answering in a socially desirable way considering their job role. Due to this survey being similar to Phase 1, the justifications for using an online survey, and using Qualtrics are the same as outlined in [Section 3.3.1](#). Some additional questions were created by the researchers based on responses from Phases 1 and 2, for example talking about the use of social media groups for communication. Additionally, the researchers noticed in Phase 1 it would have been beneficial to have a more in-depth understanding of the reasons why participants chose to respond in the way they did. Therefore, Phase 3 included more qualitative follow-up questions to explore participants' decision-making process in more depth. The survey questions are discussed further in Chapter 5, with the full survey in [Appendix C](#).

### 3.5.2. Data Analysis: Frequency Analysis

Due to the survey questions taking a similar format to the questions in Phase 1, the analytical approach remained mostly the same. Quantitative responses were analysed using frequency analysis, to identify patterns in the data (Coolican, 2018). Originally the plan was to analyse the qualitative responses using an inductive thematic analysis. This would have allowed for new themes to be created from the responses, but also to consider how these responses relate to themes from Phase 2 of the research (Coolican, 2018). However, due to the length of the responses provided in the survey, which were mostly one-word responses, with only the odd response containing a full sentence, a frequency analysis was conducted for the qualitative responses also. Frequency analysis of the qualitative responses was the same as for Phase 1, wherein the responses were organised into categories, with the frequency analysis for these categories provided.

## 3.6. Phase 4: Intended Methodology and Future Plans

This PhD research project forms part of a wider programme of work in this area within Dstl. Following the completion of Phases 1 and 2 of the research project, the benefit of having in-depth qualitative responses from the interviews in Phase 2 to explore the findings from Phase 1, was evident. Therefore, when planning for the next step of the research, a fourth Phase of the project was included to provide a comprehensive overview of the perspective of Military Key Relations. Whilst this study was not completed as part of the PhD project, Phase 4 forms part of

the overall research programme, and provides the opportunity for this next Phase of the research to be completed as a non-PhD project, as it will be handed over to Dstl for onward completion,. Due to Phase 4 being so intricately linked with the studies conducted in the PhD project, Phase 4 was included in the second ethics protocol submitted for this PhD project, alongside Phase 3. Therefore, to provide context for the next steps for the research following the discussion of the findings from Phase 1, 2 and 3 conducted within this PhD project, the aims and objectives for Phase 4 are outlined below.

Phase 4 aims to apply a qualitative methodology, in the form of focus groups, to explore opinions and experiences of Military Key Relations in further detail. The focus groups intended to understand the opinions of Key Relations towards their role in cybersecurity risk for military organisations. Phase 4 also aimed to understand what Key Relations want and need from cybersecurity training, education and awareness initiatives created by military organisations. Phase 4 can be completed by Dstl following the submission of the thesis, and outputs will feed directly to Dstl and the wider military community, with the potential to publish these findings separately.

### 3.7: Chapter Summary

This chapter began with an overview of the mixed-methods approach applied to the research. It then discussed the challenges of conducting military research as an external academic researcher, and how these were overcome. The methodology for each Phase of the research was discussed, along with the rationale. This chapter summarised with the originally planned methodology for Phase 4 and the intention to complete this Phase as part of the programme of work outside of the PhD project

## Chapter 4 - Phase 1: Exploring the Perspective of Military Personnel in an Online Survey

As outlined in Chapter 2, existing research into the extended military community, including friends and relatives mainly focuses on immediate family. Individuals addressed within an Armed Forces Family are often only those who are considered 'dependents' of military personnel (Clever & Segal, 2013). This includes long-term partners such as spouses, civil partners, and cohabiting partners, alongside children. However, the current approach often does not consider the influence of extended relatives and close friends. The existing research into military families often reflects heteronormative families, with an underrepresentation of single-parent families, short-term relationships, and LGBTQ families (Gribble et al. 2020). To address this gap, the first aim of Phase 1 is to provide insight into which friends and relatives military personnel consider to be their closest, or 'Key Relations'. Dunbar (2010) explains that everyone has five close relationships, that could consist of friends or relatives, who provide advice and comfort, and are contacted once a week. In this thesis the term 'Military Key Relations' will be used to describe any friends and relatives military personnel would consider in their circle of five close relationships. This may not be the same for everyone, and so it is important to identify any potential friends or relatives that could be included in this intense relationship network and in the definition of Military Key Relations. Insight into the definition of Military Key Relations provides direction for future phases of the research, particularly when exploring the perspective of Key Relations themselves in Chapter 6, Phase 3. It also provides direction for future cybersecurity initiatives with Military Key Relations. Directing future materials to the appropriate audience ensures the online risk that occurs due to Military Key Relations' online behaviours is reduced as much as possible.

Of those who use the Internet in the general population, nearly all use at least one communication platform to interact online (Ofcom, 2022). The reliance on the internet to communicate with others is exacerbated for the military community. These individuals use online communication platforms to stay in touch when the military person is on deployment or an unaccompanied posting, or when families relocate alongside their military person and move away from friends and relatives (Rea et al. 2015). Therefore, the second aim explores the way that military personnel and their Key Relations communicate. Consideration of online behaviour is useful to understand the potential influence their online communication might have on cyber resilience. It also assists in directing any future cybersecurity initiatives to ensure they are relevant for the audience. Additionally, exploring how military personnel and their Key Relations are communicating online, and identifying what they are discussing online is explored within Phase 1. Phase 1 considers how factors such as age may influence communication behaviours, as findings from Auxier and Anderson (2021) suggest that younger individuals have an increased use of newer social media platforms, such as TikTok, compared to older individuals. Insight into the content of what is being discussed can provide a further understanding of the potential influence that Key Relations' online behaviours might have on military cyber resilience, and whether these behaviours present a potential risk that should be addressed. Therefore, the final aim of Phase 1 is to explore what military personnel and their Key Relations discuss over online communication platforms. Participants completed an online mixed-methods survey, conducted on Qualtrics, to address these three aims. The full aims with accompanying research questions are outlined below:

**Aim 1:** To define who is a military key relation by identifying who military personnel consider a close friend or relative.

**Research question 1a:** *Which friends and relatives should be included in the definition of military Key Relations?*

**Research question 1b:** *Are there any differences between younger and older participants with whom they consider to be Key Relations?*

**Aim 2:** To explore how military personnel communicate with their key friends and relatives and whether they use different communication platforms with different Key Relations.

**Research question 2a:** *What communication platforms, such as social media or traditional communication platforms including email and voice calls, do military personnel use to communicate with their Key Relations?*

**Research question 2b:** *Does participant age influence the type of communication platform personnel choose to use to communicate with their Key Relations?*

**Aim 3:** Identify what topics military employees discuss with their friends and relatives over online platforms.

**Research question 3:** *Do military personnel discuss sensitive military information with their Key Relations along with more mundane and everyday topics?*

## 4.1. Phase 1 Pilot Study

Phase 1 began with a pilot study to ensure the survey was usable and that the survey questions were relatable and appropriate for the sample of serving military personnel. The pilot study also looked to ensure the survey instructions and wording were clear. This section outlines the method of the pilot study, and changes made to the survey following analysis of the participant responses, and participant feedback.

### 4.1.1. Phase 1 Pilot Study: Method

The pilot study sample consisted of six military personnel, with 2 participants serving in the Royal Navy, 1 participant serving in the Royal Air Force, and 3 participants serving in the British Army. All participants were introduced to the researcher as being experts in their field. This therefore justifies having a smaller sample than recommended for assessing question instructions clarity and wording (Hertzog, 2008). Research (Johanson & Brooks, 2010) also suggests 12 participants per group is sufficient in a pilot study. However, this research considers military personnel as a whole rather than comparing specific military branches. Five of the participants were male and one female, with the average age of participants being 37.80 (SD = 11.90) years. Whilst this is not an even gender split, with 16.67% of participants being women, this is representative of the gender ratio of the UK Armed Forces, where 11.70% are women (Allison, 2023). The youngest participant was 18 years old, and the oldest participant was 55 years old.

Pilot study participants completed an online survey which included quantitative questions supported by free response, qualitative questions. The survey began with providing individuals with the Participant Information Sheet, and then informed consent questions, both of which were embedded in the survey. Individuals who provided consent to participate in the survey were then asked demographic questions about their age and gender, followed by more

employment-specific questions about their job role, rank, and the branch of the military they serve. The rest of the survey questions were divided into blocks based on relationship type. Participants were asked to imagine they were on deployment and then identify whether they could contact each friend or relation when deployed. If the participant responded “yes” they would contact this friend or relation on deployment, and follow-up questions were asked. The first follow-up question asked participants to score the strength of the relationship from 1-10, with 10 being a strong relationship. The second follow-up question asked participants how often they would contact this individual when on deployment. Participants were provided with multiple options including: Everyday (when possible), once a week, 2-3 times a month, once a month, twice a year, and once a year. The next question provided participants with a list of communication platforms, including options for social media platforms, email, text messages, and phone calls. Participants were asked to rank this list, in order of their most preferred method of communicating with this individual, to their least preferred. For the first round of the pilot study participants, they did not have the option to say they did not use a platform, this was altered once the researcher realised there were inconsistencies with participant responses due to this. This change is outlined in [section 4.1.2.3](#). below. The final follow-up question provided participants with a range of topics they might discuss with someone, including their daily schedule, advice about personal and work problems, and information about others such as relatives, friends, or colleagues. Participants were asked to select all the topics they discuss with their friends or relatives when communicating with them.

If the participant responded “no”, selecting that they would not contact a specific friend or relation when on deployment, the survey would move to the next question block and ask about the next type of friend or relative. There were 13 question blocks with pre-determined friend or relationship types, with 3 additional question blocks for “other” friend or relation not previously stated. The types of friends and relatives included in the pre-determined relationship blocks were:

- Husband/Wife/Civil Partner
- Co-habiting partner
- Short-term partner (less than one year)
- Grandparent
- Aunt/Uncle
- Cousin
- Friend you live with
- Friend from school
- Family friend
- Friend, you met online (but have since met in person)
- Friend, you have only ever spoken to online

The survey summarised with two free-response questions to explore what influences how the military person chooses to communicate with their Key Relationships. The first qualitative response question asked what the most important consideration for platform usage is when communicating with relatives, and the second question focused on platform consideration when communicating with friends. The researcher notes that participants were not provided with a clear definition of relatives and friends for this question, and the potential impact of this is discussed in Section 4.4, when discussing [Aim 2](#). The average response time for all pilot study participants to complete the pilot study was 30.30 minutes. However, this

response time was influenced by the pilot study participants making notes to provide feedback on the survey, to the researcher. During a discussion of this feedback, participants self-reported that the survey took between 15 and 20 minutes to complete.

## 4.1.2 Phase 1 Pilot Study: Results and Discussion

### 4.1.2.1. *Defining Key Relationships*

The pilot study aimed to identify if there were any friends or relatives military personnel would consider Key Relations that were missing from the question blocks in the survey. Table 4.1 below illustrates all the relatives provided to participants as question blocks in the pilot study, and Table 4.2 illustrates all the friend relationships included in the pilot study. Both tables visualise participants responses for how many participants would contact this individual when on deployment and the self-reported strength of this relationship. Participants were provided two opportunities to identify any “other” individuals they would contact on deployment. One opportunity was after all the relatives were mentioned, at this point no additional relatives were provided however two participants included another type of friend, a “close friend”. An additional opportunity was provided once all the friend relationships had been mentioned, and there were no other individuals reported at this point. One respondent reported that due to not having any family, they consider a close friend as equal to a partner and that they had answered the partner/cohabiting people question with this close friend in mind. To ensure no confusion in the main study, the full list of friend and relative relationships included in the survey was highlighted at the beginning of the survey. For example, the individual who noted they had considered their close friend as a “cohabiting partner”, might have instead chosen to identify them as a “friend they live with”. Due to the potential that a close friend might also fall into one of the other friendship categories, and no alternative relatives were mentioned when participants were provided the opportunity, no additional relationship types were included in the main study. [Section 4.1.2.3](#) outlines the question alterations that were made to the main study following the results from the pilot study, in further detail.

**Table 4.1.**

*Pilot study responses for relatives, outlining the frequency of participants who would contact these individuals and the mean strength of the relationship with standard deviation.*

Relationship Type (Relatives)	Frequency of participants who would contact this individual when deployed (and %)	The mean strength of the relationship (10 being strong relationship)
Husband/Wife/Civil Partner	6 Participants (100%)	8.67 (SD = 1.211)
Cohabiting Partner	6 Participants (100%)	8.83 (SD = 1.169)
Short Term Partner (< 1 year)	5 Participants (83.33%)	6.25 (SD = 2.217)
Child	6 Participants (100%)	9.33 (SD = 0.577)
Parent/Guardian	6 Participants (100%)	6.25 (SD = 0.957)
Grandparent	3 Participants (50%)	6.00 (SD = 1.414)
Cousin	0 Participants (0%)	0.00
Aunt/Uncle	0 Participants (0%)	0.00
"Other"	2 Participants (33.33%)	8.00 (SD = 0.00)

**Table 4.2.**

*Pilot study responses for friends, outlining the frequency of participants who would contact these individuals and the mean strength of the relationship with standard deviation.*

Relationship Type (Friends)	Frequency of participants who would contact this individual when deployed (and %)	The mean strength of the relationship with the individual (10 being a strong relationship)
Friend you live with	1 Participant (16.67%)	5.00 (SD = 0.00)
Friend from school	2 Participants (33.33%)	7.00 (SD = 1.414)
Family friend	1 Participant (16.67%)	5.00 (SD = 0.00)
Friend you met online, but have since met in person	0 Participants (0%)	0.00
Friend you have only ever spoken to online	1 Participant (16.67%)	4.00 (SD = 0.00)
"Other"	0 Participants (0%)	0.00

#### 4.1.2.2. Platform decisions when communicating

The first group of questions participants were asked about their platform considerations was their preferred platform when communicating with their Key Relations, from a list of pre-determined communication platforms. They were asked this question for each relationship type they responded “Yes” to contacting when on deployment. When discussing the results of this question, it is important to note that the first 4 pilot study participants were asked a slightly different question from the last 2 pilot study participants. The first 4 participants did not have the option to say that they did not and would not use a particular platform, they were only provided the option to rank it lower in their preference compared to other types of communication platforms, as seen in Figure 4.1.

#### Figure 4.1:

*Question about online communication platforms used to communicate with friends and relative, before pilot study*

*Display This Question: If Q6) = Yes*

Q9) If you were communicating with your husband/wife/civil partner, what is your preferred method of communication? Please rank from most preferred **(1)** to least preferred **(10)**.

- \_\_\_\_\_ Facebook (1)
- \_\_\_\_\_ Text message/SMS (2)
- \_\_\_\_\_ Email (3)
- \_\_\_\_\_ Phone call (4)
- \_\_\_\_\_ Instagram (5)
- \_\_\_\_\_ Snapchat (6)
- \_\_\_\_\_ Twitter (7)
- \_\_\_\_\_ WhatsApp (8)
- \_\_\_\_\_ Facetime (9)
- \_\_\_\_\_ Skype (10)
- \_\_\_\_\_ Other (please state) (11)

However, there were inconsistencies in how participants initially chose to respond to this question, so the question was changed for the 2 additional pilot study participants and the final version in the main study. The question was originally a drag and drop to rank score the types of communication platforms (Figure 4.1), this was changed to a numeric entry option (Figure 4.2). Whilst it has been found there are no differences in the distribution of ranks or time it takes to complete the task for numeric entry compared to drag and drop tasks, numeric entry ranks allow participants to rank platforms equivalently or convey they do not use the platform at all (Genter et al. 2022). After this change in ranking type, the wording of the question was changed to encourage participants to place their preferred method of communication in order. Figure 4.2 shows the question after the changes were made. There was one recommendation from a pilot study participant to include offline communication options, such as letters. However, this was not included as the aim of the study is to explore cybersecurity risk behaviours, and therefore this would be an unnecessary collection of data. The “other” option for any additional communication platforms remained an option in the main survey to ensure participants had the choice to mention any platforms that had not been originally included or identified by the pilot study participants.



#### Figure 4.2:

Question about online communication platforms used to communicate with friends and relative, after pilot study

*Display This Question:*  
If Q16) = Yes

Q) If you were communicating with your short-term partner, what is your preferred method of communication? Please rank from most preferred **(1)** to least preferred **(11)**.

For platforms that you do not use, please enter 0 next to them.

\_\_\_\_\_ Facebook (1)  
\_\_\_\_\_ Text message/SMS (2)  
\_\_\_\_\_ Email (3)  
\_\_\_\_\_ Phone call (4)  
\_\_\_\_\_ Instagram (5)  
\_\_\_\_\_ Snapchat (6)  
\_\_\_\_\_ Twitter (7)  
\_\_\_\_\_ WhatsApp (8)  
\_\_\_\_\_ Facetime (9)  
\_\_\_\_\_ Skype (10)  
\_\_\_\_\_ A dating app e.g. bumble/tinder/hinge (11)  
\_\_\_\_\_ Other (Please state) (12)

Understanding why participants choose to communicate over certain platforms can help determine how to direct awareness materials and encourages discussion over why participants may choose alternative platforms rather than those which are recommended by military organisations. Participants were asked two questions at the end of the survey to explain what influences their choice of communication platform with relations, and the same questions for when they communicate with their friends. One participant identified a difference in the platform consideration depending on whether they were communicating with friends or relatives. This confirms that there potentially is a difference in the decision behind the method of communication depending on the relationship type and consequently provides justification for keeping the question separate for friends and relatives. Based on the results and the analysis of the findings, alongside the feedback from the pilot study participants, no alterations were made to these questions.

#### 4.1.2.3. Phase 1 pilot study: Alterations made following feedback and results

Following feedback from the pilot study participants, to ensure participants were able to provide informed consent, format changes were made to the Participant Information Sheet and Informed Consent Form. The link to the 'Ministry of Defence no-fault compensation scheme' was included in the Participant Information Sheet. In the consent section, there was a question included where participants must confirm they are 18 years of age or older, see Figure 4.3. This was important to distinguish as individuals can enlist as non-serving personnel in the military from 16 years old. However, individuals were required to be 18 years or older to participate in this Phase of the research.

**Figure 4.3:**

*Section defining the relationship types of participants will be asked during the survey.*

You will now be asked some questions referring to your communication with friends and relatives. Each question refers to a specific type of friend or relative, and you can choose whether you wish to answer the question about each.

The friends and relatives you will be asked about include:

*Relatives:*

- 1) Husband/Wife/Civil Partner
- 2) Cohabiting Partner
- 3) Short Term Partner
- 4) Son/Daughter
- 5) Parent/Guardian
- 6) Grandparent
- 7) Aunt/Uncle
- 8) Cousin
- 9) Other not mentioned
- 10) Other not mentioned

*Close Friends:*

- 11) A friend from school
- 12) A family friend
- 13) A friend you met online (but have since met in person)
- 14) A friend you have only ever spoken to online
- 15) Other not mentioned

For the demographic questions, the format of the question box where participants reported their age was changed to allow both text and numeric responses. The pilot study participants reported that it would have been beneficial to know what friends and relatives they would be asked about before the questions started, so they could identify the best label for their close relations. Therefore, a section about what questions will be asked in the survey was included alongside the definitions, this can be seen in Figure 4.4. Part of the benefit of recruiting military personnel for the pilot study was to confirm the questions were appropriate for a military sample. Pilot study respondents identified that there were some errors in the list of ranks which are provided to the participants when asked to identify their rank. There were errors in the rank titles that are associated with the rank, so these were corrected and ranks for the non-commissioned were also included. This question was checked by a Dstl Military Advisor before being distributed in the main study. The final formatting change was inserting a sentence on the final page of the survey that reminded participants they needed to press submit at the bottom of the page for their responses to be included, as not pressing this would result in an incomplete response, which would not be included in the analysis of the findings. This was included as one of the participants provided feedback to the researcher but did not “submit” their survey once they had completed the question. When asked, the participant reported not seeing the button that asks them to submit the survey for their responses to be considered.

**Figure 4.4:**

*Consent questions changed following the pilot study: Ministry of Defence no fault compensation scheme link and age question.*

I understand that in the event of my sustaining injury, illness or death as a direct result of participating as a volunteer in this research, I or my dependants may enter a claim with the Ministry of Defence for compensation under the provisions of the no-fault compensation scheme, details of which can be found in the following document: [Arrangements for the payment of no fault compensation to participants in modrec approved studies](#)

Yes (1)

---

I can confirm I am 18 years old or above (please do not complete if you are 16/17 years old)

Yes (1)

## 4.2. Phase 1 Main Study: Method

### 4.2.1. Participants

Following the pilot study, twenty-eight participants completed the survey in full. Thirty-eight participants attempted the survey, 11 incomplete responses were removed where participants had not clicked “submit” at the end of the survey. Participants were provided with multiple reminders this was a requirement for their responses to be considered within the data set, and so to ensure all responses were collected ethically, any incomplete responses were removed. One additional response was removed as whilst the participant clicked “submit” at the end of the survey, they did not answer any of the demographic questions and answered “no” to all questions, which may suggest insufficient effort in responding. Insufficient effort responding is where the participant lacks either motivation or attention and so may respond with response patterns that require less cognitive resources (Alarcon & Lee, 2022), such as responding “no” to all questions. While one other participant answered similarly, they were included in the analysis of the results as they completed the demographic questions and clicked “submit” at the end of the survey. A potential justification for their response might be that they do not contact friends or relatives when on deployment but were not provided with the option to say that. Whilst potentially an unusual response in most industries, this could be seen as less unusual for military personnel who have job roles that require limited use of personal devices, for their own and others’ safety.

During the process of gaining favourable opinion from the ethics panels as part of this research a target participant sample size was identified for this phase of the research. This was based on previous research using surveys in this topic area, which range from sample sizes as small as 30 participants (Bittner, 2014), with others varying from 230 participants (Mailey et al. 2018), to research with 500 responses (Da Veiga et al. 2020). Due to the resource constraints of this being a PhD project and an exploratory topic, a target sample size was identified at 250 participants, aligning with the median number of participants of previous research in this area. During the Dstl SAC and MODREC panels the challenge of identifying such a large participant

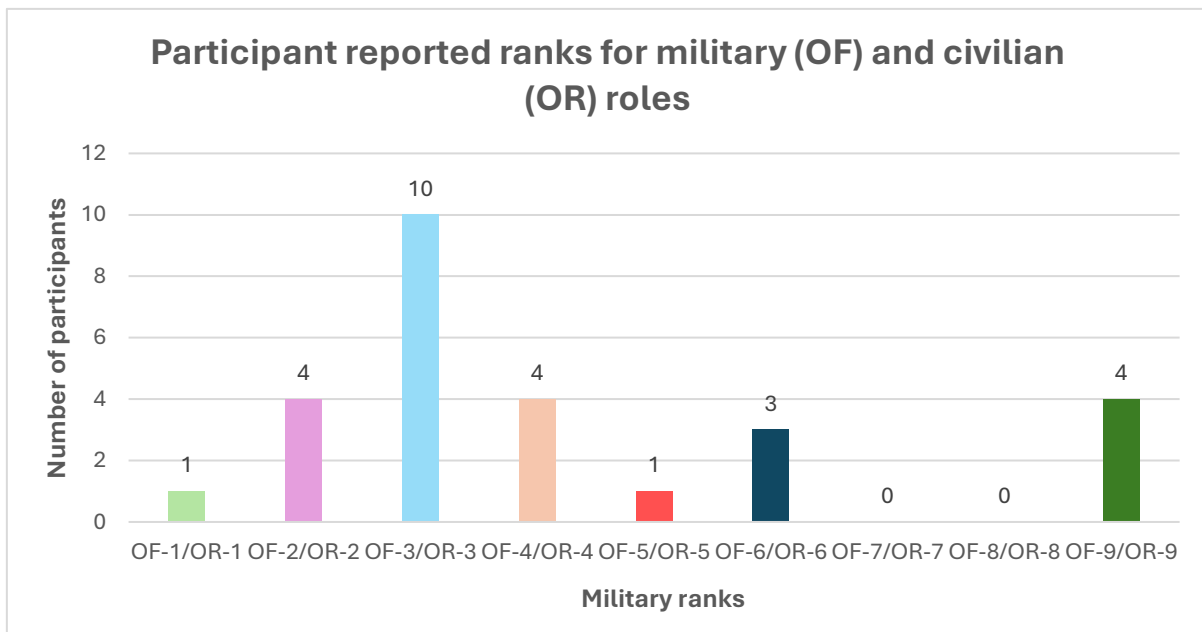
sample was highlighted and understood by the researchers. A sample size of 28 in this Phase reflects the challenges experience during recruitment of participants, potentially due to survey fatigue of the population, as discussed in Chapter 3. Lessons learned from these recruitment challenges are discussed in [Section 7.3. Evaluation of the Research](#).

Of the 28 participants who remained for analysis, 23 participants were male, and five were female, participants had a mean age of 36.1 years (SD = 9.4) with the youngest participants being 18 years old and the oldest being 55 years old. Participants were recruited via opportunity sampling, and potential participants were invited to participate by gatekeepers identified by the research sponsor to access the military community across the services. Discussions were had with these individuals addressing the benefit of inviting personnel with an upcoming deployment to participate due to the survey questions focussing on online behaviours during deployment. However, no question was asked in the survey about upcoming deployments, as this combined with the military branch, rank and age may provide an increased potential that individuals could be identified in their responses. Participants were invited to participate via an advert (see [Appendix D](#)) distributed by Dstl Military Advisors to Military Unit Commanders and on Military intranet forums. The advert included a link to the survey which interested individuals could follow to read the Participant Information Sheet and then complete the survey, if interested.

Three participants were serving in the Royal Navy, 12 participants serving in the Royal Air Force and 12 participants serving in the British Army, one participant did not answer this question. To ensure the anonymity of participants, specific job roles will not be reported within this thesis. Participants were from a range of ranks to encourage diversity across the participant group, with participants early in their military careers included, with a spread across to those with a high level of military qualifications. Figure 4.5 includes the full range of military and civilian ranks that individuals can hold, with OF indicating the ranks for military roles and OR indicating the ranks for civilian roles. Those further to the left of the chart with a lower number are associated with a lower ranking role, and those further to the right with a higher number are associated with a higher-ranking role. The visualisation of results in Figure 4.5 demonstrates the range of ranks participants held for both military and civilian roles.

**Figure 4.5:**

*Bar graph depicting the ranks that participants self-reported. Including both serving military (OF) and civilian roles (OR)*



#### 4.2.2. Materials

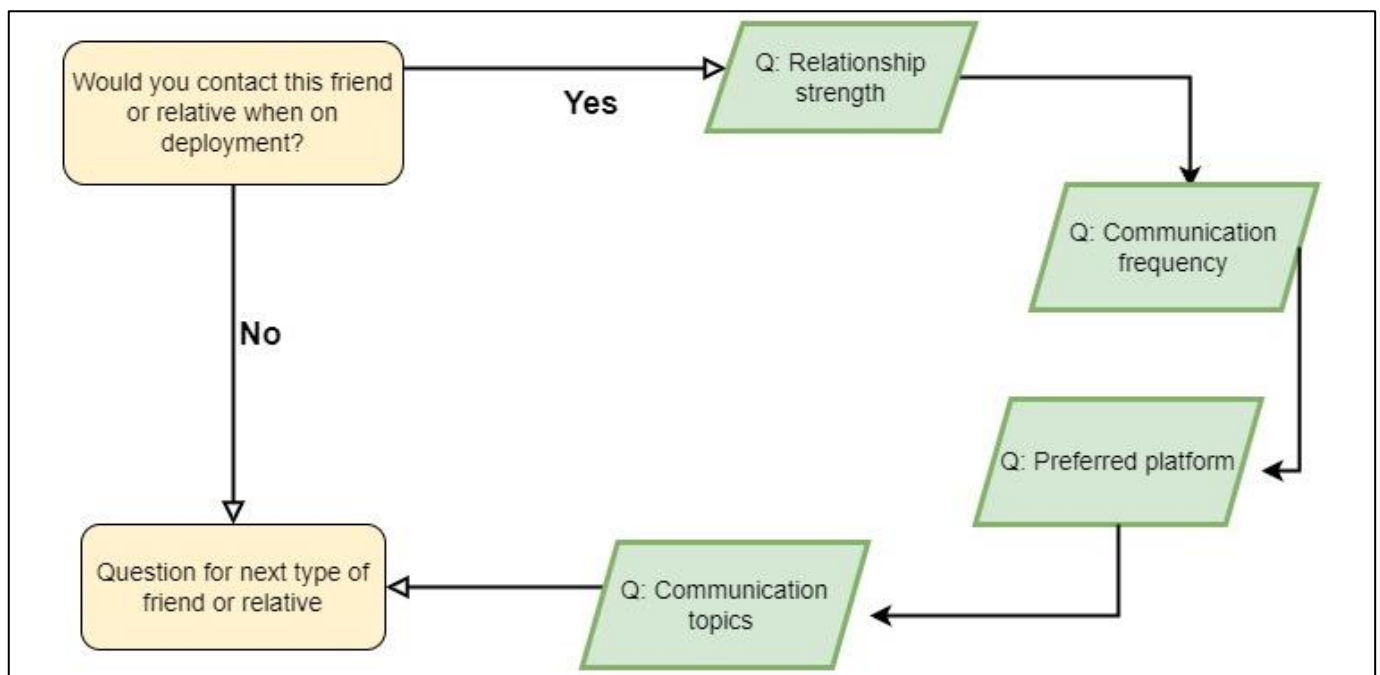
An online survey was created and distributed on the survey platform Qualtrics, and participants could complete the survey on any type of device. [Appendix A](#) includes a copy of the full survey. The survey began with the Participant Information Sheet and Informed Consent Form. The opening survey questions were demographic questions, including asking participants' age, gender, job role, military rank and what branch of the military the participant serves. Before the focused questions participants were provided with a definition of the term social media, they were also informed of the types of relationships that would be explored within the survey, so that participants could consider which relationship type best suited their friends and relatives. Figure 4.6 outlines how these relationships were identified to the participants. During data analysis, the researchers highlighted that there was no clear mention to the participants that there were differences in whether the relation type was considered a friend or relative, this consideration is discussed further in section 4.5 of this chapter, [Limitations and Future Research](#). Three types of partner relationships were included within the survey options, with husband, wife, or civil partner reflecting the traditional definition of spouse as a dependent. This relationship was differentiated from a cohabiting partner, which may not be considered a next of kin, or a dependent within military organisations due to the lack of legal connection, but still reflects a long-term commitment to a partner. Thirdly, an option for a short-term partner was included, and defined as a partner of less than one year. The option for a short-term partner addresses the gap in the existing research, which often focuses on spouses and next-of-kin relationships (Gribble et al. 2020). These relationship types may vary in relationship length, but not perceived relationship strength, and therefore may not alter the amount of sensitive information that could be shared between intimate partners. Exploring all types of relationships within this research provides an understanding of any potential risk behaviours that any military friends and relatives could present to military cyber resilience, to address these behaviours.

The rest of the questions were split into question blocks, with each block focusing on a single type of friend or relation, with three additional opportunities to identify any additional friends or relations. The friends and relations included in the pre-determined question blocks included:

- Husband/Wife/Civil Partner
- Co-habiting partner
- Short-term partner (less than one year)
- Grandparent
- Aunt/Uncle
- Cousin
- Friend you live with
- Friend from school
- Family friend
- Friend, you met online (but have since met in person)
- Friend, you have only ever spoken to online

**Figure 4.6:**

*Question flow for each section consisting of one relationship type, demonstrating the question flow depending on if the respondent answers 'Yes' or 'No' to the initial question.*



For each relationship question block the same five questions were asked. The question block opened by asking if the participant would contact this type of friend or relation via social media for messaging and video calls, when on deployment. Researchers discussed during analysis that due to the wording of the question, it is unclear how participants should respond if they don't have a certain relation, the implication of this ambiguity is discussed further in [section 4.5](#) of this chapter, Limitations and Future Research. If the participant responded 'No' to this opening question, the survey moved on to the next question block and asked the same opening

question about the next type of relationship. If the participant responded 'Yes', four additional questions were presented to the participants, Figure 4.6 provides an overview of this process.

The first follow-up question asked participants to score the strength of the relationship on a Likert scale, which was scored from one to ten, with one being a low relationship strength and 10 being a high relationship strength. Secondly, participants were asked to choose how often they would contact this friend or relative from pre-determined frequency options. These options were: Once a year, twice a year, once a month, 2 to 3 times a month, once a week, and Every day (when possible). Whilst the length and frequency of deployment varies depending on the branch of the military, these options align with a typical deployment length of 6 months, up to 12 months (Keeling et al. 2015). Participants were then asked to rank their preferred communication platforms they use to communicate with a friend or relation when on deployment. Participants were provided with 10 pre-determined options which included: Facebook, Text message/SMS, Email, Phone call, Instagram, Snapchat, Twitter, WhatsApp, Facetime, and Skype. Participants were also provided the option to rank an 'other' option. If selected they were asked to state what this other platform is, in a free-response box. Participants were asked to rank these from 1 to 10, with 1 being the most preferred platform and 10 being the least preferred platform. Finally, they were asked to select the topics they might discuss when communicating with this individual. These topics were pre-determined and ranged from discussing the military person and their work, asking their advice about personal or work problems, what the friend or relation did with their day, and information about relatives, friends, or colleagues. Figure 4.7 provides an example of what this question looked like when participants were asked about their husband, wife, or civil partner. Individuals were provided with the opportunity to answer these questions for all the relationship types identified in the previous paragraph. Once the question blocks were completed for each relationship type, participants were provided with two final questions that asked them to identify what most influences their consideration of how to communicate with their Key Relations: one question for relatives and one question for friends. The survey included a debrief section outlining support services, contact details of the researcher, and how to receive Experimental Test Allowance (ETA) for completing the survey. ETA is a payment set up to recognise the effort involved by military personnel participating in MOD approved experimental tests. The compensation rate for each research Phase was calculated based on the published rate for ETA at the time and guidance from the Ministry of Defence Research Ethics Committee (MODREC).

**Figure 4.7:**

*Question to explore what topics military personnel discuss with their friends and relations when on deployment, using the example of the question block for husband, wife, or civil partner*

Q) Please select all the topics you might discuss when communicating with your husband/wife/civil partner

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify)

### 4.2.3. Procedure

Participants completed the survey on Qualtrics and took approximately 30 minutes to complete the survey (M = 28.18 minutes, SD = 38.662). Participants were able to complete the survey in multiple sittings if they desired, and could complete the survey on any personal device, including computers, mobile phones or tablets.

### 4.2.4. Ethical Considerations

The Participant Information Sheet and Informed Consent Form were embedded at the beginning of the online survey distributed on Qualtrics ([see Appendix A](#)). Individuals were asked to read through the information sheet and consent form and then take 24 hours to consider whether they wished to take part in the study. At the time of seeking ethical approval for this phase, this thinking time was the recommendation from the Dstl Scientific Advisory Committee (SAC) and Ministry of Defence Research Ethics Committee (MODREC). Informed consent to participate in the survey was provided by participants via tick boxes on the landing page of the survey. In the information sheet participants were informed they could withdraw at any time from the survey by closing the browser, and that there is no requirement to answer the survey questions if they do not want to. However, participants were advised that once the survey



responses had been submitted they would not be able to withdraw their responses, due to the survey being anonymised. The Participant Information Sheet also explained that the participants' decision to participate or not to participate in the research would not influence service members' careers, and anonymity was highlighted.

An important consideration for this survey was the anonymity of participants and their responses. To facilitate this, personally identifiable information collected was limited to age, gender, military branch, and rank. Participants were notified of this in the Participant Information Sheet, and it was explained individuals would not be attributable in any publications. Participants were prompted to remove any identifiable information from free response questions but were informed that any identifiable information accidentally included would be redacted during analysis. As compensation for their time spent completing the survey, participants could apply for Ministry of Defence ETA, at a total of £6.12. ETA is processed through payroll and requires personal information to process the compensation. To ensure participants could claim compensation for completing the survey without compromising the anonymity of their responses, participants could apply for ETA by contacting an individual within Dstl who did not have access to the survey responses.

The survey summarised with a debrief section. This provided individuals with directions to support services, including military-specific services, the contact details of the lead researcher and the contact details of the volunteer advocate for the research. Whilst the survey did not directly ask questions that would cause participant distress, there is the potential that questions may evoke sensitive or upsetting emotions and memories in the participants. Therefore, ensuring a range of appropriate support services for military service members were included was important. This phase of the study received favourable opinion from the Dstl Scientific Advisory Committee (SAC) and the Ministry of Defence Research Ethics Committee (MODREC), evidence of this is included in [Appendix F](#). Bournemouth University Ethics Committee also provided ethical approval for Phase 1 of the research, evidence of this is included in [Appendix G](#).

#### 4.2.5. Data Analysis

The survey produced quantitative and qualitative data, which was analysed using frequency analysis. Frequency analysis was completed by counting the sub-categories, for example, the number of people that responded "Yes" when asked if they would contact a child when on deployment. Frequency analysis for this phase presents results as the number of participants who responded in a particular way for each question, as well as the percentage of participants who responded in this way. When participants were asked about the strength of their relationship with their friends and relatives, the question required selecting a number on a scale of 1 (low strength) to 10 (high strength). For this question, the mean strength score was calculated for each relationship type. For example, the mean strength score for all participants who rated the strength of their relationship with their parents. The qualitative responses were grouped into sub-categories that were created during the analysis. Independent coding was applied during the analysis and was particularly evident when creating these sub-categories for the free response questions. For example, when participants were asked what their main consideration was when deciding what platform to communicate on with their friends and relatives, one participant responded "Connection". Independent coding helped to determine whether this was perceived as a network connection, or the perceived attachment individuals felt to each other when communicating. The data was analysed using JASP, version 0.15.0.0.

Microsoft Excel was used to analyse responses when JASP was not compatible. For example, when analysing the free-response questions.

### 4.3. Phase 1 Main Study: Results

This section will outline the results of the survey questions outlined in the method section above. As the survey questions were asked to participants separately for each friend or relative, this is how the questions are presented, to demonstrate patterns in the data influenced by type of relation. This includes the number of participants who would contact each of this type of relation when on deployment, with participants responding they would contact a wide range of friends and relatives. Differences in mean relationship strength score is reported for each relationship type, as well as including the pattern in the data that suggests this might interact with regularity of communication between military personnel and their Key Relations. Platform usage behaviour split by relationship type and age is presented, alongside participants' most important considerations when determining how to communicate with their Key Relations. Results from the qualitative responses are reported based on the categories that were created during the qualitative content analysis, and the frequency of each category is provided. Additional quotes from the participants are included where appropriate to provide context for the responses.

#### 4.3.1. Defining Key Relationships: Relationship frequency and strength results

This section of the chapter focuses on providing results for the questions designed to determine which friends and relatives should be considered as a Key Relation. The question focuses on a deployment situation and asks participants which friends and/or relatives they would contact when on deployment. Table 4.3 identifies the percentage of participants that would or would not contact each type of friend or relative when on deployment, in order of the highest percentage of those that 'Yes' they would contact this type of relation, to the lowest.

**Table 4.3.**

Percentage of participants that responded 'Yes' when asked which friends and relatives they would contact when deployed, in descending order. \*This was a free-response question; percentages may differ if all participants were provided with the option to select this relation type.

<b>Relationship Type</b>	<b>Percentage of participants responding "Yes"</b>
Husband/Wife/Civil Partner	89.29%
Child	89.29%
Parent/Guardian	89.29%
Cohabiting Partner	82.14%
Short-term partner (< 1 year)	67.86%
Grandparent	35.71%
Other Friend (Close/Best Friend)	32.14%
Friend from school	28.57%
Friend you live with	21.43%
Aunt/Uncle	14.29%
Cousin	7.14%
Family friend	7.14%
Friend met online (met in person)	7.14%
Friend met online (not met in person)	7.14%
Other Family (Siblings)	3.85%*
Other Friend (Work colleague)	3.85%*

As the survey was divided into question blocks based on the type of friend or relation being identified, the results will be explored for each relationship type individually. This includes the results of the questions asked about the strength of the relationship with these friends and relatives and how frequently the military personnel participants would contact these individuals when on deployment.

#### *Husband, Wife or Civil Partner*

As Table 4.3 displays, one of the relationships participants most frequently reported they would contact on deployment would be a husband, wife or civil partner. The mean strength of this relationship was reported at 9.16 (SD = 1.068, lowest 7 and highest 10). Table 4.4 indicates the number and percentage frequency of how often participants would contact these individuals. Three participants highlighted they would contact this individual but did not respond to the follow up questions. These findings demonstrate that communication regularity with this type of relation is common and will be included in the definition of ‘Military Key Relation’ going forwards.

**Table 4.4.**

*Number and percentage of participants who would contact a Husband, Wife or Civil Partner at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Every day (when possible)	17	60.71%
Once a week	7	25%
2 to 3 times a month	1	3.57%
Once a month	0	0%
Twice a year	0	0%

#### *Cohabiting Partner*

When asked about a cohabiting partner, results were only slightly lower when compared to a husband, wife or civil partner. The mean strength of this relationship was reported at 9.09 (SD = 1.240, lowest 6 and highest 10). Table 4.5 indicates the number and percentage frequency of how often participants would contact these individuals. Five participants highlighted they would contact this individual but did not respond to the follow up questions.

**Table 4.5.**

*Number and percentage of participants who would contact a Cohabiting Partner at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Every day (when possible)	16	57.14%
Once a week	6	21.43%
Once a month	1	3.57%
2 to 3 times a month	0	0%
Twice a year	0	0%

### *Short-term partner (less than one year)*

Whilst more than 50% of participants identified that they would contact a short-term partner when on deployment, this number was lower than other types of partners. The self-reported strength of the relationship with a short-term partner was also lower, with a mean of 7.17 (SD = 1.581, lowest 4 and highest 10). Frequency of contact also differed for this type of partner for some individuals. Table 4.6 demonstrates how participants who identified how often they would contact this individual were more evenly split, than the previous partner types. One participant did not answer the follow-up questions.

**Table 4.6.**

*Number and percentage of participants who would contact a Short-term Partner at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Every day (when possible)	9	32.14%
Once a week	9	32.14%
2 to 3 times a month	0	0%
Once a month	0	0%
Twice a year	0	0%

### *Child*

Another one of the most frequently reported relationships by participants in the survey was child, alongside husband, wife or civil partner and parent or guardian. The researcher reflects the use of restrictive language of son or daughter in the survey. Throughout the results, this question block will be referred to as “child”. When asked how strong the relationship was with a son or daughter, participants were more varied than with the relationship strength for partners, with a mean score of 2.91 (SD = 2.959, lowest 0 and highest 10). A suggestion for why this might be based on question wording and is discussed in [Section 4.4](#). Despite this lower relationship strength, participants still reported they would contact their child regularly, as indicated in Table 4.7. One participant did not respond to the follow up questions.

**Table 4.7.**

*Number and percentage of participants who would contact a Child at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a week	12	42.86%
Every day (when possible)	11	39.29%
2 to 3 times a month	1	3.57%
Once a month	0	0%
Twice a year	0	0%

### *Parent or Guardian*

The final most frequently reported relationship by participants in the survey was parent or guardian. The mean strength of the relationship was reported at 8.17 (SD = 1.90, lowest 4 and

highest 10). Despite the higher relationship strength score, the responses for how often participants would contact these individuals were less regular, as displayed in Table 4.8. Two participants did not respond to the follow up questions.

**Table 4.8.**

*Number and percentage of participants who would contact a Parent or Guardian at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a week	13	46.43%
2 to 3 times a month	7	25.00%
Once a month	2	8.70%
Twice a year	1	3.57%
Every day (when possible)	0	0%

#### *Grandparent*

Whilst a large proportion of participants identified they would not contact a grandparent, the mean strength of this relationship between military personnel and a grandparent did not drop much lower than the most frequently contact relationships, with a mean score of 7.56 (SD = 1.33, lowest 5 and highest 10). The regularity of communication was much lower, as demonstrated in Table 4.9.

**Table 4.9.**

*Number and percentage of participants who would contact a Grandparent at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a month	5	17.86%
Once a week	4	14.29%
2 to 3 times a month	1	3.57%
Every day (when possible)	0	0%
Twice a year	0	0%

#### *Aunt or Uncle*

The mean relationship strength for the aunt or uncle relationship was similar to grandparent, with a mean relationship strength score of 7.50 (SD = 1.00, lowest 6 and highest 8). Table 4.10 shows how the regularity of this contact varies.

**Table 4.10.**

*Number and percentage of participants who would contact an aunt or uncle at different regularities*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a month	2	7.14%
Once a week	1	3.57%
Twice a year	1	3.57%
Every day (when possible)	0	0%
2 to 3 times a month	0	0%

### *Cousin*

When participants were asked about the strength of their relationship with their cousin, both rated the strength of the relationship at 8, resulting in a mean relationship strength score of 8.00. The regularity of the contact of this relationship was less than the more frequently contacted relationships above, as highlighted in Table 4.11 below.

**Table 4.11.**

*Number and percentage of participants who would contact a cousin at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a month	1	3.57%
Once a week	1	3.57%
Every day (when possible)	0	0%
2 to 3 times a month	0	0%
Twice a year	0	0%

### *Other family relationship*

Participants were provided with the opportunity to identify any additional relationship types which had not been included in the previous questions. When participants were asked this, there were 9 responses for additional types of relationship, with only 1 being an additional relative, the other 8 responses will be explored when discussing friends [below](#). The one other relative identified in this category was ‘Sisters and brother’. The individual rated the strength of these relationships an 8, and identified they would contact these individuals once a week.

**Table 4.12.**

*Number and percentage of participants who would contact a sibling at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a week	1	3.57%
Every day (when possible)	0	0%
2 to 3 times a month	0	0%
Once a month	0	0%
Twice a year	0	0%

### *Friend you live with*

When participants were asked about a friend you live with participants gave this relationship a mean relationship strength score of 6.83 (SD = 1.835, minimum 5 and maximum 10). Table 4.13 shows how the regularity of contact varies.

**Table 4.13.**

*Number and percentage of participants who would contact a 'Friend you live with' at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
2 to 3 times a month	2	7.14%
Once a month	2	7.14%
Once a week	1	3.57%
Everyday (when possible)	1	3.57%
Twice a year	0	0%

### *Friend from school*

Participants were also asked about a friend from school, the mean score of the strength of this relationship was 7.25 (SD = 1.035, lowest at 6 and highest at 8). When participants were asked how often they would contact this friend from school, there was a variety of responses, as displayed in Table 4.14.

**Table 4.14.**

*Number and percentage of participants who would contact a 'Friend from school' at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a month	3	10.71%
2 to 3 times a month	2	7.14%
Once a week	2	7.14%
Twice a year	1	3.57%
Every day (when possible)	0	0%

### *Family friend*

Two participants identified that they would contact a family friend when on deployment, with a mean relationship score of 4.50 (SD = 0.707, lowest 4 and highest 5). Table 4.15 demonstrates the regularity of contact with this individual is infrequent.



**Table 4.15.**

*Number and percentage of participants who would contact a ‘Family friend’ at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a month	1	3.57%
Twice a year	1	3.57%
Every day (when possible)	0	0%
Once a week	0	0%
Once a month	0	0%

*Friend, you met online (but have since met in person)*

Participants were asked about their online friends, with one option providing them the option to select a friend that they originally met online but have since met in person. The mean relationship strength score for this individual was 5.50 (SD = 2.12, minimum 4 and maximum 7). Table 4.16 provides the frequency results for the regularity that participants contact this individual.

**Table 4.16.**

*Number and percentage of participants who would contact an ‘Online friend (met)’ at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a week	1	3.57%
Once a month	1	3.57%
Every day (when possible)	0	0%
2 to 3 times a month	0	0%
Twice a year	0	0%

*Friend, you have only ever spoken to online*

Participants were also given the option to identify if there’s anyone that they have only ever spoken to online that they would contact when on deployment. Two participants selected ‘Yes’ they would, with a mean relationship strength score of 4.50 (SD = 0.707, minimum 4 and maximum 5). Table 4.17 demonstrates the regularity of this contact is the same as the previous individual Friend you met online (but have since met in person).

**Table 4.17.**

*Number and percentage of participants who would contact an ‘Online friend (not met)’ at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
Once a week	1	3.57%
Once a month	1	3.57%
Every day (when possible)	0	0%
2 to 3 times a month	0	0%
Twice a year	0	0%

*Other types of friend relationship 1: Close or Best friend*

When participants were provided with the opportunity to identify any additional relationship types that had not been previously discussed, 9 participants identified they would contact a ‘close’ or ‘best’ friend. The mean strength of this relationship between a close or best friend and the participants was 7.63 (SD = 1.19). One participant did not answer the follow-up questions. Table 4.18 shows how the regularity of contact with this individual varies.

**Table 4.18.**

*Number and percentage of participants who would contact a ‘Close or best friend’ at different regularities.*

Communication regularity	Number of participant responses	Frequency percentage of participant responses
2 to 3 times a month	3	10.71%
Once a month	3	10.71%
Once a week	1	3.57%
Twice a year	1	3.57%
Every day (when possible)	0	0%

*Other type of friend relationship 2: Work colleague*

One participant also identified an additional type of relationship; a close work colleague, who had been through military training with the participant. The participant reported the strength of this relationship was an 8.00.

**Table 4.19.**

*Number and percentage of participants who would contact a ‘Work colleague’ at different regularities.*

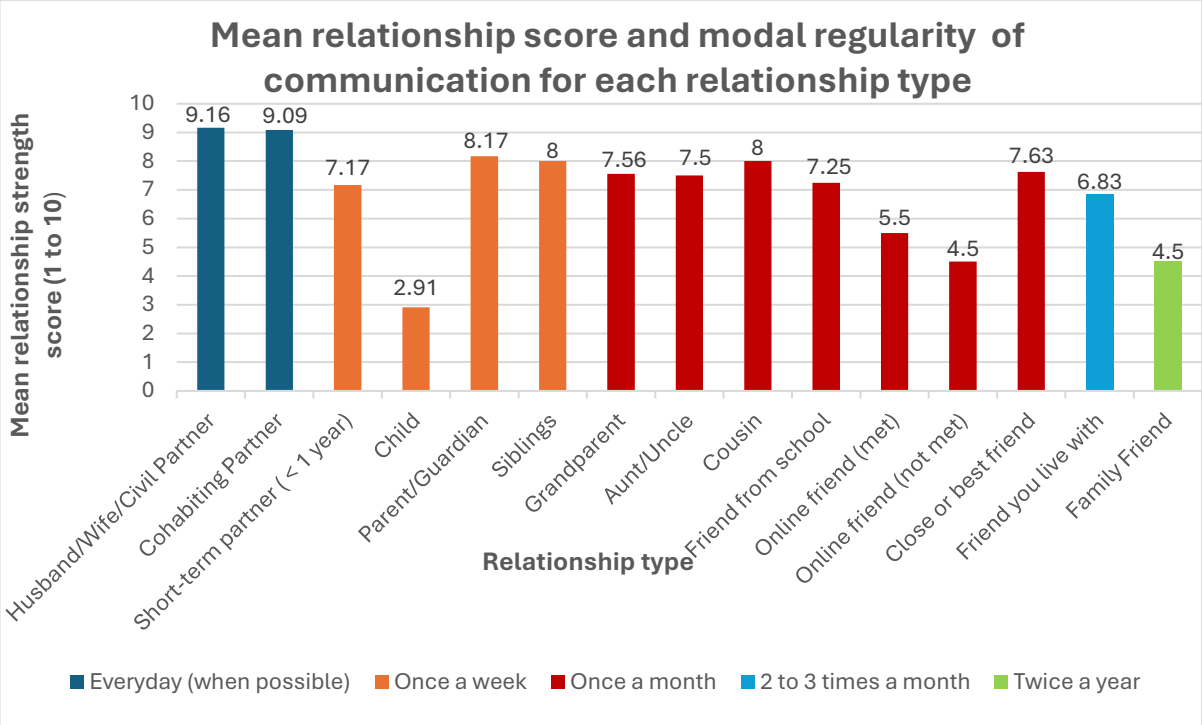
Communication regularity	Number of participant responses	Frequency percentage of participant responses
2 to 3 times a month	1	3.57%
Every day (when possible)	0	0%
Once a week	0	0%
Once a month	0	0%

Twice a year	0	0%
--------------	---	----

There is some indication that relationship types with a higher mean score of relationship strength across the responses would also be contacted more often when individuals are on deployment. Figure 4.8 demonstrates how those relationships that participants would contact most regularly, had the highest mean relationship strength score. The highest mean relationship score was for Husband, Wife or Civil Partner and Cohabiting Partner, and the modal communication regularity for these individuals was Everyday (when possible). The modal communication regularity for each relationship type is indicated by the colour of the bar chart, with a different colour for each option that participants were provided.

**Figure 4.8:**

*Graph showing the mean relationship strength score and the modal regularity of communication, for each relationship type.*



### 4.3.2. Communication platform choices and considerations

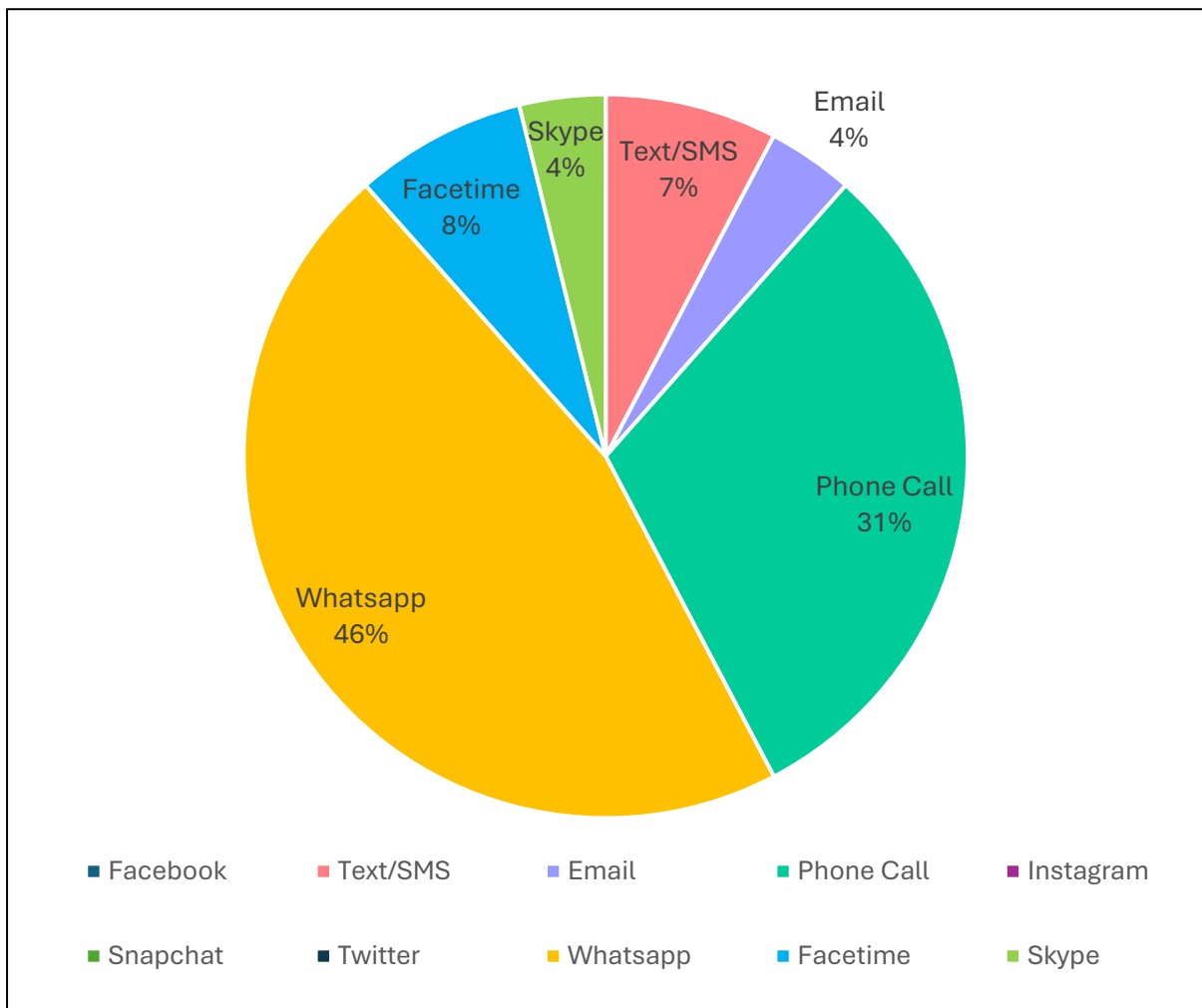
For each relationship type participants were asked to rank the communication platform from most to least preferred to use when on deployment and communicating with each relationship type. When considering all participant responses, WhatsApp was most frequently rated as the preferred platform to communicate with friends and relatives when deployed. Figure 4.9 shows the percentage frequency of participants who identified each platform as their preferred communication platform.

The results also provide insight into differences in communication platforms when considering additional factors, such as relationship type and age. Figure 4.10 provides an overview of which platform participants would prefer to use when communicating with each relationship type. Whilst many participants still stated WhatsApp was their most preferred communication platform across a range of relationship types, some relation types had a higher

frequency of participants stating a different platform was their most preferred. For example, when communicating with a grandparent, more participants would prefer to call them on the phone, than use another platform. Figure 4.11 demonstrates the results did not suggest age influences communication platform preference when deciding how to communicate with their Key Relations on deployment. However, the results suggest age influences whether an individual uses some of these platforms at all, regardless of preference. Figures 4.12, 4.13, and 4.14 indicate that participants who are in older age groups are less likely to use social media apps Snapchat, Twitter, and Instagram. They are also less likely to use dating apps to communicate with short-term partners, as visualised in Figure 4.15.

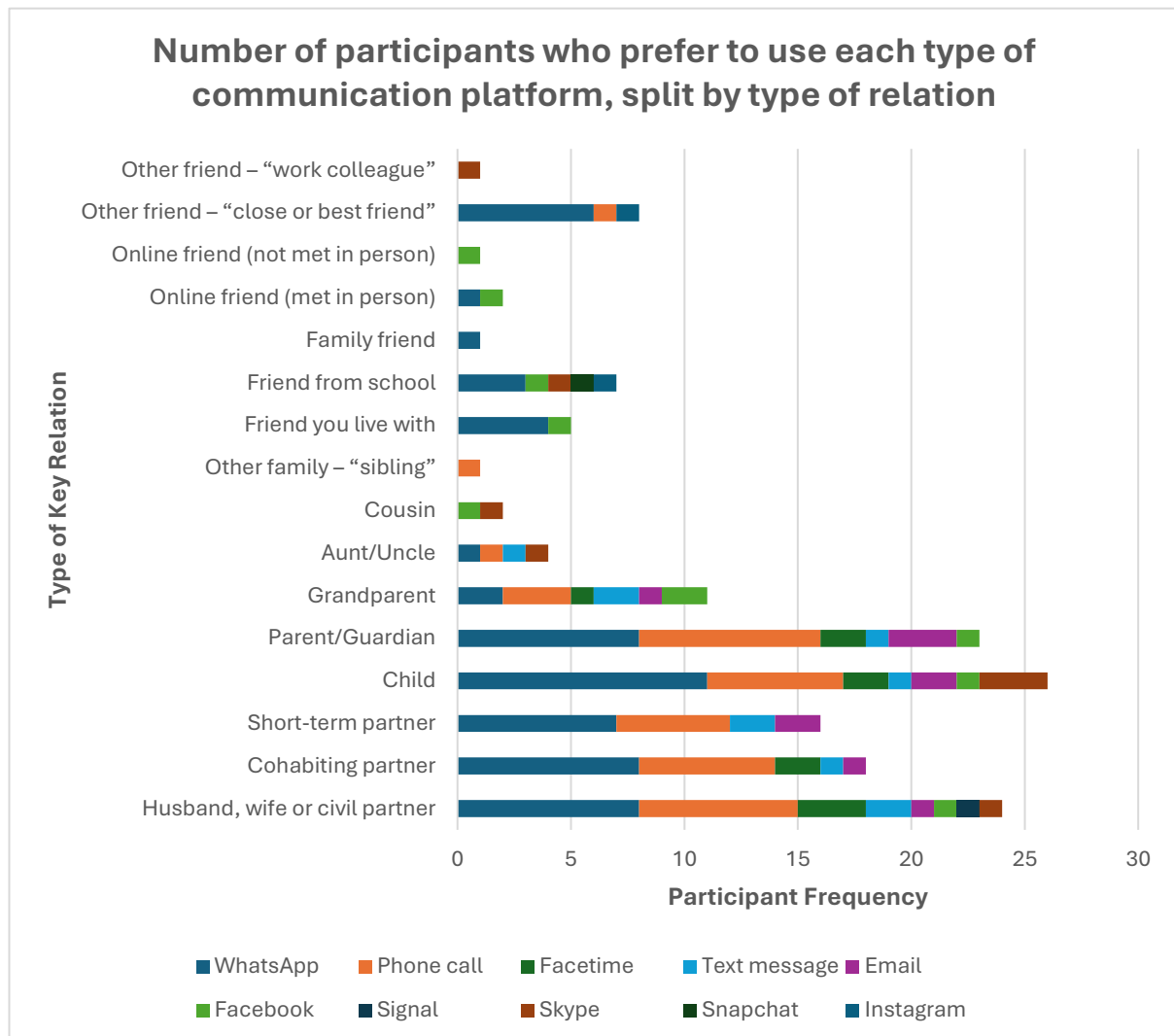
**Figure 4.9:**

*Pie chart depicting the percentage of participants who consistently rated this communication platform as their most preferred platform, across a range of types of relation.*



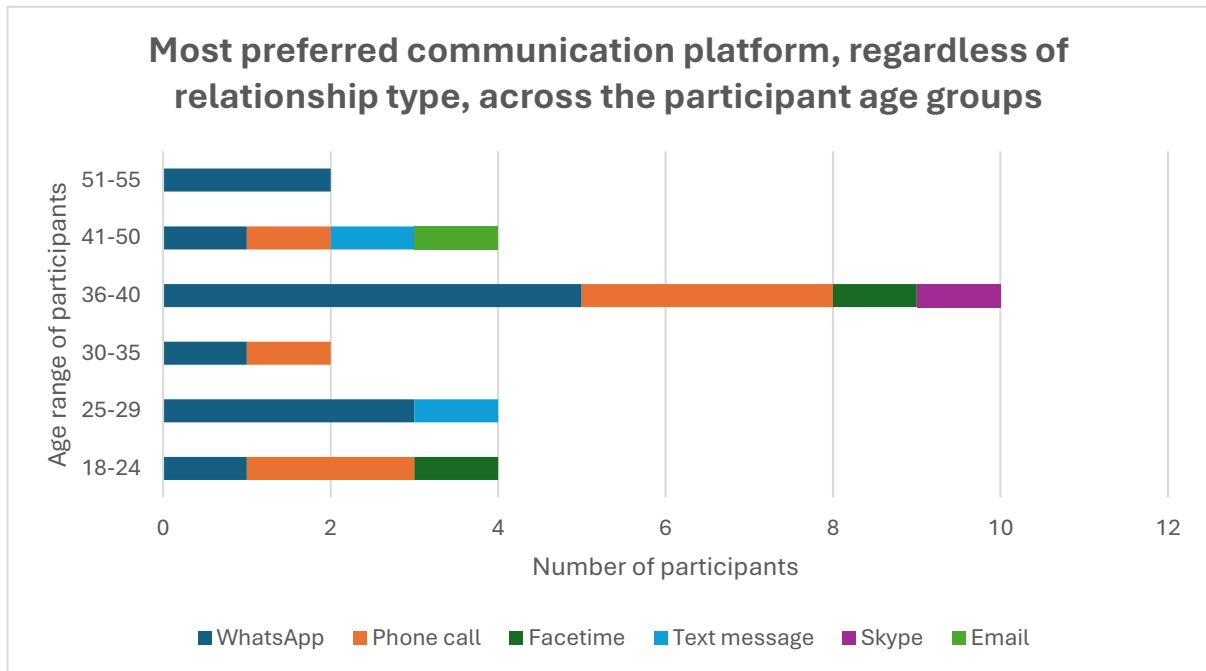
**Figure 4.10:**

Graph showing the frequency of participants who most preferred to use these platforms to communicate with their Key Relations.



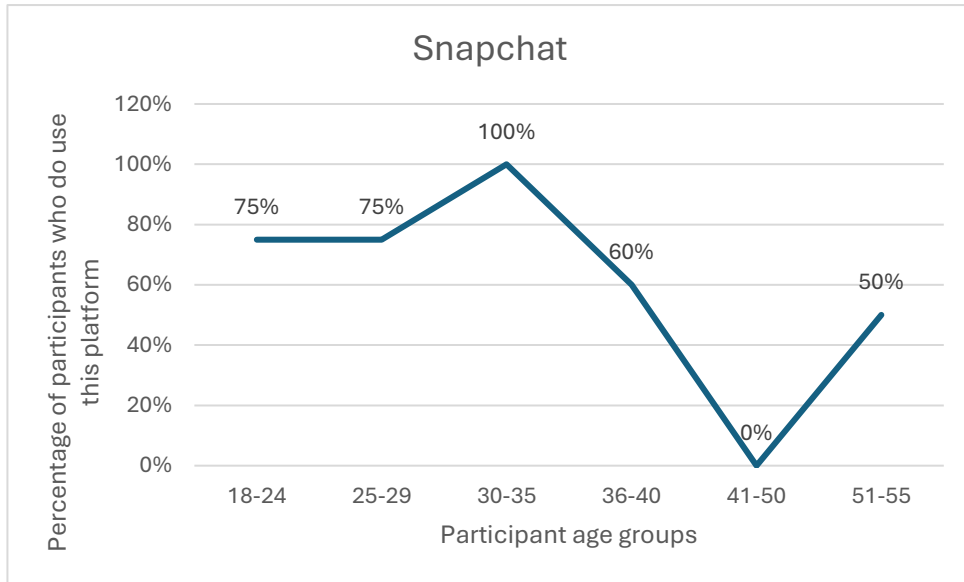
**Figure 4.11:**

Graph showing the frequency of participants who prefer to use each communication platform, split by age



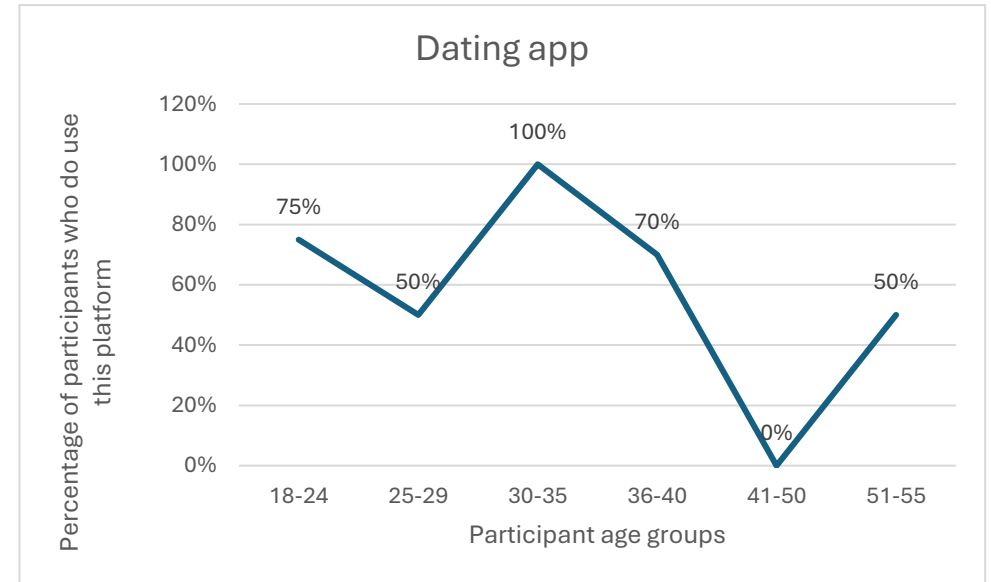
**Figure 4.12:**

Percentage of participants who use Snapchat to communicate with their key relations, split by age group



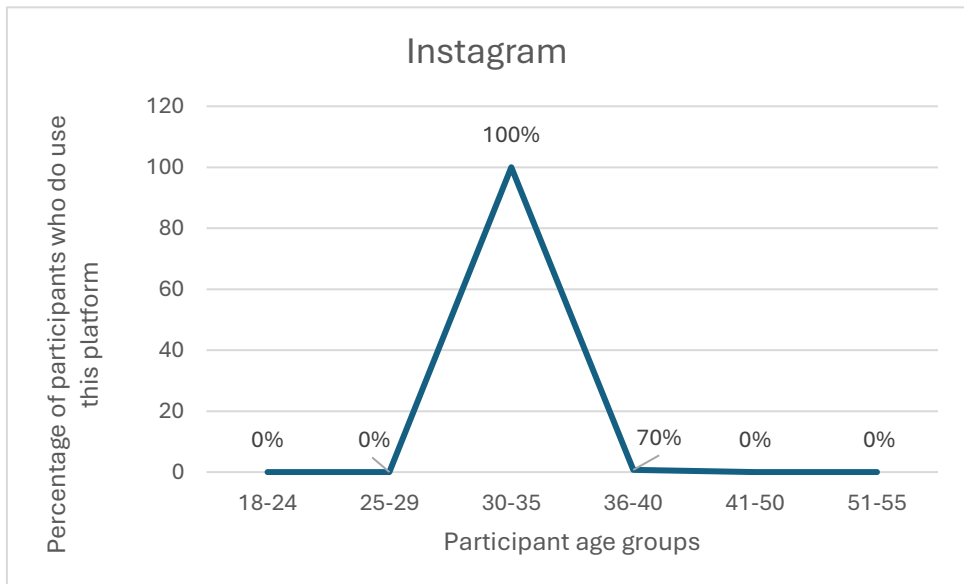
**Figure 4.13:**

Percentage of participants who use a Dating app to communicate with their key relations, split by age group



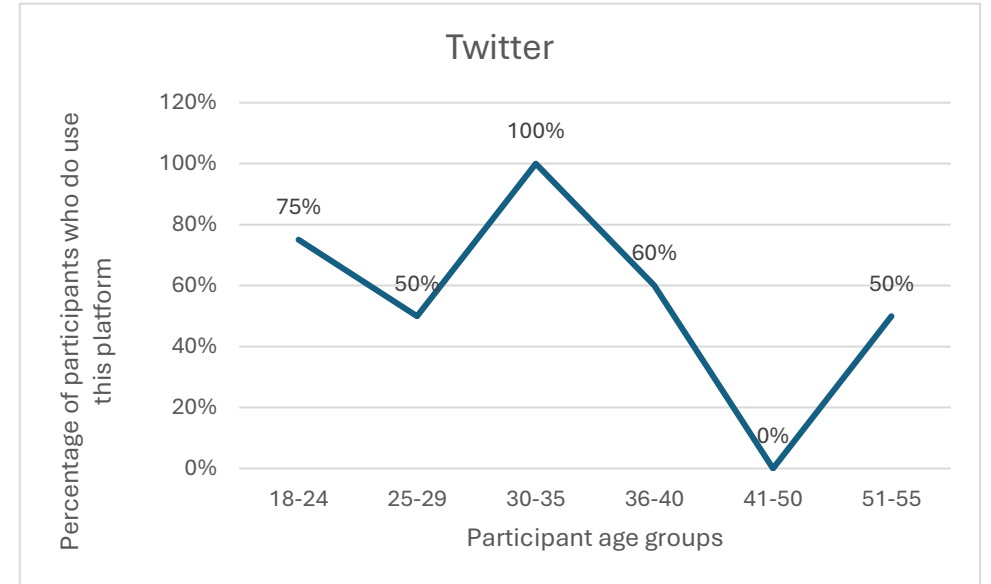
**Figure 4.14:**

Percentage of participants who use Instagram to communicate with their key relations, split by age group



**Figure 4.15:**

Percentage of participants who use Twitter to communicate with their key relations, split by age group



To explore these choices further, participants were asked what considerations are most important when deciding what online platforms to use to communicate. This free response question was asked separately, first for relatives and then for friends. To analyse frequency from the qualitative responses, sub-groups were created. These sub-groups were guided by participant responses. As described in Chapter 3 Methodology, this is one of the steps of Inductive Category Development, which is a part of a qualitative content analysis (Mayring, 2014). Chapter 3 explores how this is useful when working on a mixed-methods research project.

Example responses included, 'bandwidth and clarity', 'clarity of call', 'connection', and 'good connectivity' formed the sub-group 'connection clarity'. In total, 10 sub-categories were created which were:

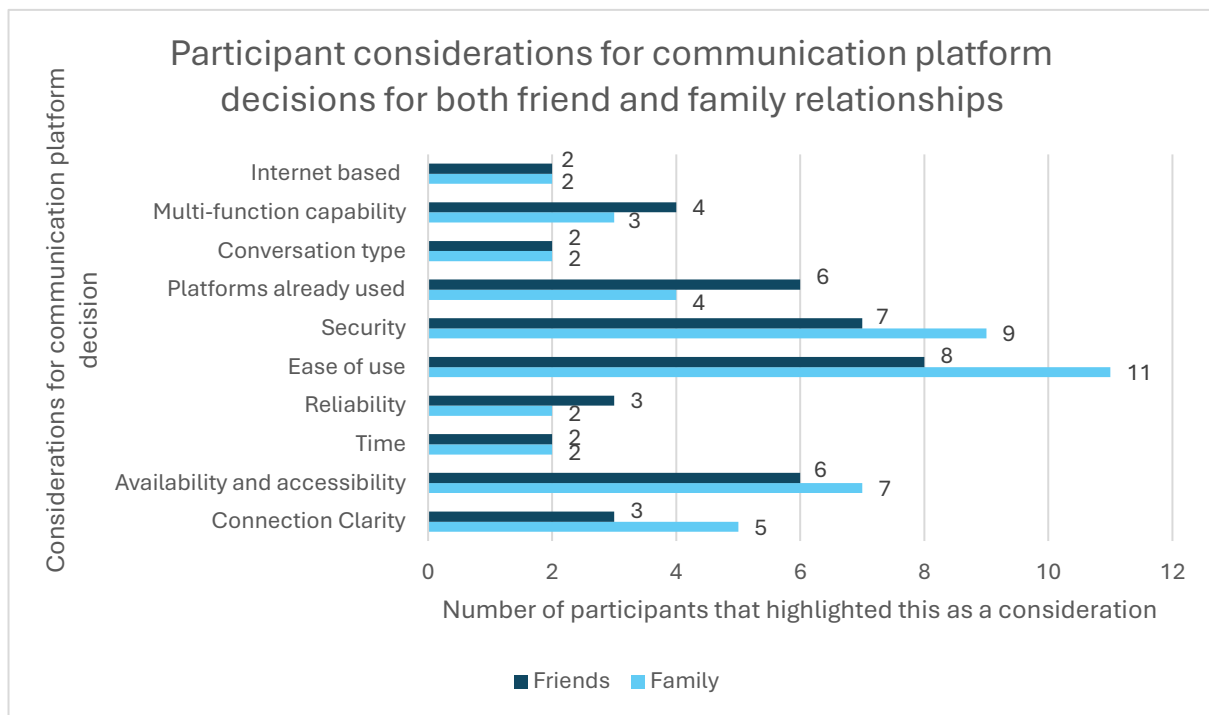
- Connection clarity
- Availability and accessibility
- Time
- Reliability
- Ease of use
- Security
- Platforms already used
- Conversation type
- Multi-function capability
- Internet based

When considering both the friends and relatives questions together, the total number of responses for both questions reached 58, which is higher than the number of participants. However, this was due to the question being a free-response question, meaning some participants included multiple points which could be allocated into several categories. The sub-groups most frequently reported were 'ease of use' and 'security'. The least frequently reported were 'internet-based' and 'conversation type'. One participant reflected that when considering what platform to use to communicate with their relatives the type of conversation influences the platform choice. This was reinforced when discussing with their friends, where they noted that banter and memes are shared on Instagram, whereas full conversations are had on WhatsApp. Figure 4.16 shows the number of participant responses for each category of communication platform considerations, for both friends and relatives.



**Figure 4.16:**

Graph showing the frequency of participants that mentioned categories of considerations for what communication platform to use when contacting family and friends



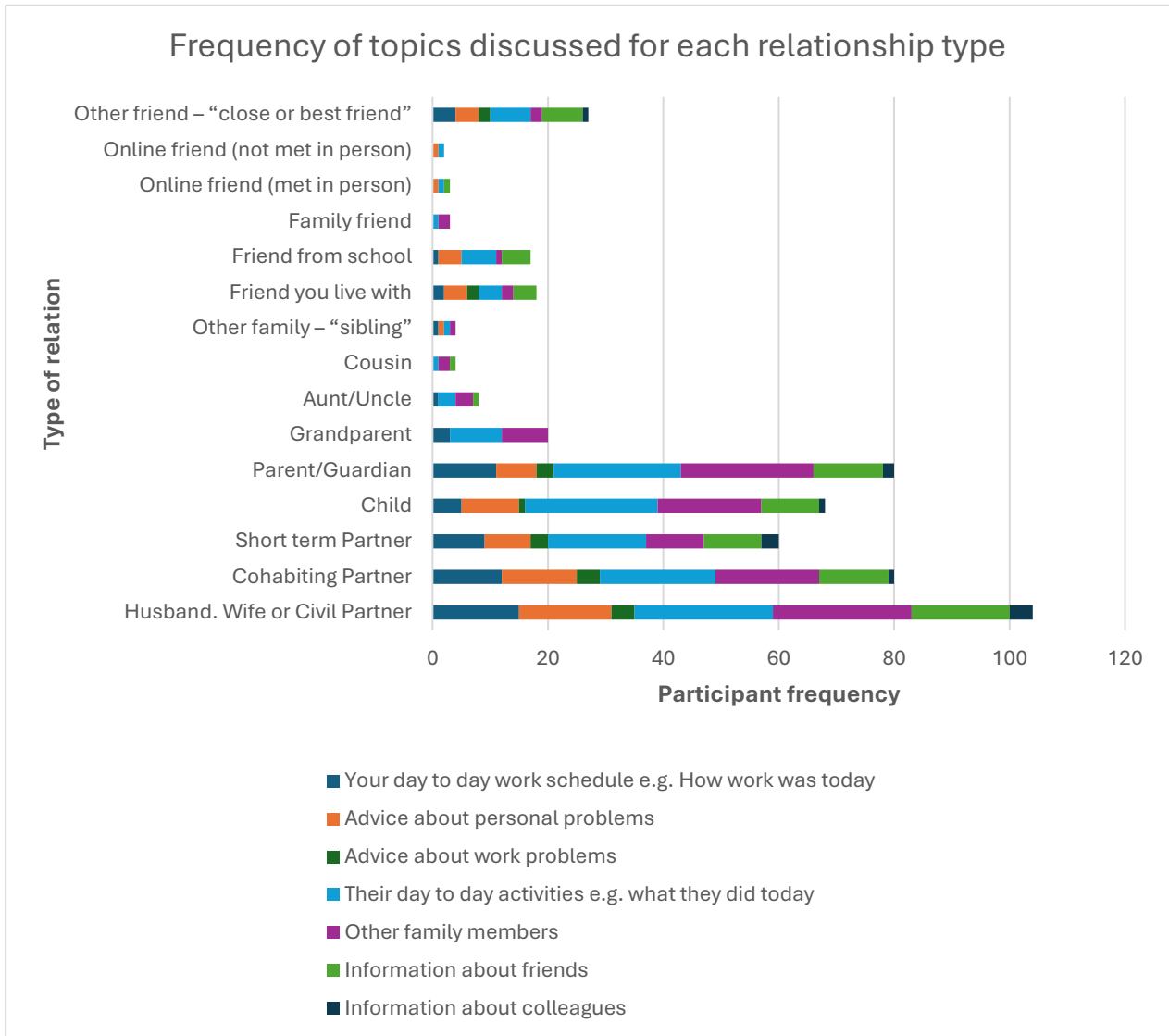
### 4.3.3. Topics discussed when communicating

Participants were provided with a list of potential topics and were asked to select the topics they discussed with their Key Relations when communicating with them. The biggest variety of topics discussed occurred with partners, children and parent or guardian, with at least one participant saying they would discuss each topic with these relations. All of these relationship types were the ones that had the highest frequency of participants saying they would contact these individuals when on deployment. Figure 4.17 visualises the frequency of topics discussed, split by type of relation.

Participants were also provided with an additional free response box to highlight any other topics they discuss with their friends and relatives, not already listed. This mostly focussed on plans for when the participants would return home, and any future plans their Key Relations had. Also mentioned as additional topics were sport and hobbies, and one participant highlighted they would discuss house information with their friend they live with. One participant used this free response box to explain that when discussing information about colleagues with their friends and relatives, it was less about work information, and more about the individuals themselves.

**Figure 4.17:**

Graph showing the topics that military personnel talk about with their Key Relations, split by relation type.



## 4.4. Phase 1 Main Study: Discussion and implications for Phases 2 & 3

**Aim 1: For military personnel to define who is a key relation by identifying who is considered a close friend or relative.**

This section will discuss the findings in relation to Aim 1, including support for the research questions. The first aim of Phase 1 has two research questions which are:

- **Research question 1a:** *Which friends and relatives should be included in the definition of military Key Relations?*
- **Research question 1b:** *Are there any differences between younger and older participants with whom they consider to be Key Relations?*

Addressing research question 1a, military personnel participants identified that they would contact a range of friends and relatives when on deployment. Relatives who participants most frequently reported contacting when on deployment were ‘Husband, Wife or Civil Partner’, ‘Child’ and ‘Parent or Guardian’. This perhaps explains why the existing research mainly focuses on these ‘next of kin’ or ‘dependent relationships’ (Clever & Segal, 2013), particularly if considering the additional resource allocation of involving the extended military community in cybersecurity. Wirth (2017) discusses how often organisations are reluctant to invest in cybersecurity as it is perceived as a large investment for intangible benefits. This is even more so if there is limited hard evidence to demonstrate the risk exists, until it is too late (McCants, 2022). This may be particularly the case for military organisations examining the extended military community’s cyber risk, including military friends and relatives. Due to there being limited evidence to suggest a cybersecurity incident has occurred due to their online behaviour. When considering ways to reduce the potential avenues for a cybersecurity risk to military cyber resilience, this study provides evidence to suggest that the definition of Military Key Relations should be extended to include a wider range of relationship types. Participants reported they would frequently contact a broad range of friends and relatives and gave high scores when asked to rate the strength of these relationships. For example, cohabiting partners not necessarily legally associated via a marriage or civil partnership, but also those in shorter-term relationships, defined in this study as a relationship of less than one year. This study begins to address Gribble et al. (2020) concern that the existing research into military families often focuses on a married couple with children, and should explore a wider range of partner relationships, as well as extended relations and friends. However, they also discussed that the research lacks specific representation of LGBTQ families (Gribble et al. 2020). Whilst the language used within the survey in this thesis represents a variety of family and relationship dynamics, there was no question that asked participants to distinguish whether this was an opposite or same sex relationship. This question was not included as it could increase the potential participants could be identified from their responses and this disclosure may deter individuals from participating. Future research may wish to include an optional question to understand the relationships in further detail, to ensure recruitment is providing under-represented military families the opportunity to share their experiences. Whilst only one participant reported their siblings in the free response box for ‘other’ types of relationship, there is no way of telling if the responses would be higher if this was provided as an option for all participants. Including this type of relationship within the list of

relations provided to participants in the survey was an oversight by the researchers. Therefore, 'sibling' will be included in future Phases of the research as part of the definition of a key relation.

One of the limitations that arose during analysis of the responses was question phrasing for the questions about whether military personnel would contact a particular relationship type when on deployment. The initial question to identify whether the military personnel would contact this individual was phrased as "Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls. Assuming you have a [Husband/Wife/Civil Partner], would you contact them?". The follow-up question then asked participants to score the strength of this relationship. Some respondents who identified that 'Yes' they would contact this type of relation, then did not respond to this question about relationship strength. Whilst this happened for multiple types of relation, one example was for the group of questions about a 'Child'. This potentially could have been due to participants misinterpreting the use of "would" in the initial question about whether this type of relation would be contacted when on deployment. The question phrasing may have meant participants interpreted this question as being that they don't currently have a child but if they did have a child, then they would contact them when on deployment. If participants chose to interpret and answer the question in this way, this could explain the missing responses for relationship score, as they could not score the strength of a relationship that does not exist. Whilst no participants identified a concern with the interpretation of this question during the pilot study, this is something to consider when interpreting the strength of the relationship scores, as individuals may have been rating the relationship on different things i.e., real, and perceived relationship strength. For example, in the 'child' question section, 9 participants gave the relationship strength score a rating of zero. This could be for multiple reasons, including their child being very young, and therefore judging the strength of a relationship could be difficult to determine.

Considering the responses to the question about topics that participants would discuss with their Key Relations, only 1 participant who said they would contact a husband, wife or civil partner when on deployment reported that they would not discuss other family members. This could be one suggestion as to why the relationship strength between participants and their child was much lower. If participants have a limited amount of time to contact their Key Relations when deployed, this may result in them communicating with their partner over other relations, as this was the highest mean strength relationship. Participants may ask their partners about their children, particularly if communication occurs at a time when children are at school with no access to personal devices, or if they are asleep due to time differences. This may result in participants experiencing a perception of a lower relationship strength with their children, due to not being able to connect with them as frequently. This may also happen with parents or guardians, where participants ask partners to check in with their parents in person, and to relay information about the participants' own wellbeing in between being able to talk to their parents or guardians themselves. This could be one suggestion as to why the frequency of contact between participants and their parents or guardians was much lower, even though the mean relationship strength for this key relation was high. This is consistent with findings that suggest individuals contact their parents at least once a week, but that this frequency may reduce as the distance between parents and their adult children increases, and time spent at work increases (Rubin, 2015). Follow up research may look to explore whether online communication behaviours change in a non-deployment scenario. Regardless of their reasoning for participants answering in this way, the responses justify including children and parents or guardians in the

definition of Key Relations. The nature of relationships between military parents and their children is something that could be explored in more detail in future research, for example exploring why the perceived relationship strength is lower than for other types of Key Relations. Additionally, it would be useful to explore the role of other family members in facilitating communication between military personnel on deployment and their children. For example, this survey did not ask participants to state whether their children were adults or dependents, which may also influence the results. This should also be explored when considering cybersecurity education and awareness for Military Key Relations.

Relationship strength was another factor in determining whether a relationship type should be included in the definition of Military Key Relations. Fewer participants reported that they would contact a 'Short-term partner', defined as a partner of less than 1 year, when on deployment. When comparing the mean relationship score participants provided for their 'Short-term partner' compared to longer term relationships 'Husband, Wife or Civil Partner' or 'Cohabiting Partner', the mean score was lower. However, participants still provided a high mean relationship strength score for these individuals. Some research suggests that military personnel are more likely to engage in marriage earlier than their civilian counterparts (Hogan & Seifer, 2010). This may be due to the benefits that are associated with being married compared to single (Hogan & Seifer, 2010). Military personnel may also marry earlier to provide commitment and dedication to the relationship in times of instability due to their job, such as relocation or deployment (Keeling et al. 2015). This suggests that short-term relationships for military personnel may be viewed as more serious, than compared to societal norms for a short-term relationship in a civilian population. Even if not in a marriage or civil partnership, the mean strength score provided by participants indicates the potential that military personnel still view a short-term relationship favourably. For military personnel, if relocation or deployment occurs early on in their relationship, they may share operational information about their location and length of deployment with a short-term partner, when discussing the potential challenges this may bring to the relationship. In this way it is important to consider all types of potential relationship situations for military personnel, when considering the definition of Military Key Relations. Including short-term relationships in the definition of Key Relations in the context of cyber resilience can help provide awareness to these individuals of the requirements for military information sharing to ensure they do not share sensitive military information online that could be exploited by a military adversary. Keeling et al. (2015) explain how partners of military personnel in unmarried relationship may require more support, for example from peers, due to not being able to access the same welfare services as spouses.

Additionally the mean strength score is influential in determining which extended relatives should be included in the definition of Military Key Relations. For aunt or uncle and cousin, four and two participants respectively reported they would contact these individuals when on deployment. This is a low percentage of the overall participant group, however the mean relationship score for these relationships were similar to other more frequently contacted relationship types including parent or guardian and short-term partner. Therefore, this presents a justification to include these types of relationships in the definition of Military Key Relations. Particularly siblings will be included as a potential participant when recruiting for Phase 3, which involves engaging with the various military friends and relatives themselves to explore their experiences. Additionally, friendship types with higher mean relationship strength scores included friend you live with, friend from school, and the free responses when participants were asked about another type of friend; 'Close or best friend'. These three were also the most frequently reported friendship-type relationships that participants would contact when on

deployment. The remaining other types of friend relationships include family friend, as well as both types of online friend; the ones participants have since met in person and those they have not. These friendships type each only had two participants identify that they would contact this type of relationship when deployed, and the mean relationship strength score was lower than for other types of relationship. However, the survey did not provide the participants to identify if any of their relationship types overlapped. For example, participants could have described their family friend as being a different type of relationship, such as a close or best friend. Therefore, these types of friend relationships will be included in the definition of Military Key Relations. Phase 2 will discuss types of Key Relations in more detail with qualitative interviews, with the intention to provide more insight and context into the friends mentioned in responses to the Phase 1 survey. In the results, one participant included a work colleague as a type of another friend. This research aims to explore the role of military personnel's key friends and relations in organisational cyber resilience. This research does not have the main aim of exploring the approach to military personnel's cyber risk behaviours and how to reduce them. Therefore, a work colleague would not be considered a key relation, as they have an existing relationship with military organisations including access to cyber training, education, and awareness in a military context. For the purpose of this research, this type of relation has not been included in the definition of a Military Key Relations.

When looking at patterns in the data with ages it is useful to have context of the age distribution across the British Armed Forces currently. As mentioned in Chapter 2, the largest age group of serving personnel are people aged 25-29 years old, with 28,270 active personnel, closely followed by those aged 20-24. As the age of individuals increase, the number of serving personnel decreases (Clark, 2023). For participants in Phase 1, the oldest participant was 55 years old, which means they are 1 of 1350 serving personnel aged 55-59 years old serving in the British Armed Forces. The findings from the survey do provide some support for research question 1b that there is a pattern of age influencing who military personnel decide to contact when on deployment. Participants that highlighted they would not contact a parent or guardian were in the 36-40 years old, 41-50 years old and 51-55 years old age groups. Whilst this is only a small percentage of participants in the study, the representation of ages in the study for older participants is relative to the age group distribution for the entire population of the British Armed Forces. Comparatively, 90% of 36-40-year-olds would still contact a parent or guardian when deployed, this does indicate a pattern in the data of age influencing deciding who to contact. Those who said no to contacting a parent or guardian may have responded in this way due to their parents passing, rather than deciding not to contact them. For example, the oldest participant in the sample aged 55 years reported they would not contact a parent or guardian. However, considering the average life expectancy in the UK is around 80 years old (Office for National Statistics, 2024), this may provide a potential explanation for this pattern. This might also explain a similar pattern for the grandparent relationship group, where there was higher percentage of participants in age groups 18-24 years old and 25-29 years old saying they would contact a grandparent, which is the opposite for those aged 30 and older. There also appears to be a pattern of age depending on the type of friendship that is being discussed, partly supporting research question 1b. The results show that those in the 18-24-year-old age group responded 'yes' they would contact a particular type of friend. 100% of those that said they would contact a family friend and an online friend (not met) were in the 18-24-year-old age group. Additionally, all of those who were in the 18-24-year-old age group said they would contact a friend from school when on deployment, whereas no one aged 25-35 years old said they would. This could be due to participants being of an age where they would have only just recently left school. There is also

evidence to suggest that our friendship network size increases as a young adult but then decreases as we get older (Wrzus et al. 2013). One additional factor that influences the size of a friendship network is relocation, where friendship group size decreases regardless of the age of the individual (Wrzus et al. 2013). This is potentially due to the perception of a supportive friend being one that lives close by and can provide assistance when other life-changing events occur (Wrzus et al. 2013). This may provide a suggestion for why there was no clear pattern dependent on age group for friend you live with or close or best friend in the results, as participants perceived these individuals as either living close and therefore being able to provide support, or the friendship offering support regardless of the location, therefore resulting in this individual being considered a 'best' friend. The influence of relocation is particularly relevant for this participant group, as military personnel may often experience relocation due to their job. Wrzus et al. (2013) identified that even though relocation influences friendship network size, family network size is unaffected by relocation, as contact is maintained regardless of geographical location. This may explain why overall the number of participants that would contact friends of any type is lower than those that would contact most family members. However, another explanation for this finding is that colleagues are a significant aspect of personnel's friendship network. High quality interactions with colleagues can provide more support in certain stages of the service person's career, than non-military friends, and relatives (Crane et al. 2022). As highlighted earlier in this section, the role of colleagues as friends were not included in this research due to them already receiving cybersecurity training, education and awareness materials from the military organisation they serve. However, if participants were asked about this type of relation, there is the potential the number of participants who identified a colleague as being a Key Relation, would be higher.

The distribution of frequency across age groups for partner types addresses research question 1b, which suggested there might be a difference in Key Relations for younger and older participants. For all types of partner: husband, wife or civil partner, cohabiting partner and short-term partner (less than 1 year) there was an even distribution across the age groups of participants that said they would contact these individuals. As highlighted earlier in the section, this may be due to military personnel marrying earlier (Keeling et al. 2015). However, as with the other types of relation, question wording could have influenced participant response here. If participants are basing their responses on their current relationship status, then it would make sense that a spouse or civil partner is also a cohabiting partner. Therefore, those who responded 'no' to not contacting a short-term partner could be due to not having one. Even though research question 1b is partly supported by the findings, the results do not present sufficient evidence that the definition of Key Relations should alter depending on the age of the military person, though this is something that could be explored in more detail in future research.

Aim 1 intended to define Military Key Relations. This definition provides a clear direction for which military friends and relatives should be included when considering the potential online risk behaviours Key Relations could present that influence military cyber resilience. Aim 1 does not outline any risk behaviours that Key Relations exhibit, but merely guides the direction to explore potential risk and threat in future steps of the research. When addressing cyber resilience it is important to consider that risk can never be fully eliminated, but cyber secure measures aim to reduce the amount of risk an organisation is exposed to from cyber vulnerabilities (Kopp et al. 2017). The findings from this survey suggest that a wide range of military friends and relatives should be considered in the definition of Military Key Relations. These friends and relatives potentially present a risk to military cyber resilience, due to the possibility of military personnel

sharing information with them, which if shared onwards could be detrimental to military organisations. Further exploring the extent of this vulnerability on cyber resilience by military friends and relatives can help identify how potential online risk behaviours could be addressed through cyber training, education, and awareness. Therefore, this definition also guides questions for Phase 2 and participant recruitment for Phases 3 and 4 of the research. For that reason, all the friends and relatives mentioned in this survey, except a work colleague, have been included in the definition of Military Key Relations. This is to ensure a broad range of perspectives are considered in future Phases. There is the potential the survey responses do not include all friends and relatives that should be considered a Military Key Relation, and so this definition will continue to be developed, throughout the research project.

In addressing Aim 1 a definition of Military Key Relations is put forward that encompasses a wide range of friends and relatives identified in the responses from the survey. In support of some of the existing literature addressing the limitations of the current definition of military friends and relatives (Gribble et al. 2020) short term and unmarried relationships should be considered by military organisations. The responses from the survey also highlighted the strength of relationships with extended family members and close friendships. Patterns in the findings suggest there is a potential role of age in influencing who personnel consider a Key Relation. However, this definition should also consider the influence of the demands of serving in the military on relationships, when compared to a civilian population. This expanded definition has implications outside of the cyber area, with suggestions for physical and mental health approaches for military friends and relatives. As well as industries outside of Defence where employees handle sensitive information and may work away from home for a period of time.

## **Aim 2: To explore how military personnel communicate with their key friends and relations and whether they use different communication platforms with different relations.**

This section will discuss the findings in relation to Aim 2, including support for the research questions. The second aim of Phase 1 has two research questions which are:

- **Research question 2a:** *What communication platforms, such as social media or traditional communication platforms including email and voice calls, do military personnel use to communicate with their Key Relations?*
- **Research question 2b:** *Does participant age influence the type of communication platform personnel choose to use to communicate with their Key Relations?*

Addressing research question 2a, participant survey responses suggest that military personnel use a variety of platforms to communicate with their Key Relations when deployed. Participants still frequently reported using phone calls and email to communicate with their friends and relatives when on deployment. However, participants frequently highlighted WhatsApp as being their most preferred communication platform, across the range of family and friend relationships. This addresses research question 2b, which explored whether there would be an age difference in platform usage. One suggestion for the results found is due to age potentially influencing how participants use WhatsApp rather than their decision to use it or not. Matassi et al. (2019) explored the influence of age on WhatsApp usage and identified that younger and older adults both use WhatsApp to socialise with peers and family, whereas those in the middle stages of their life use WhatsApp for work purposes and family responsibilities such as



children's hobbies, alongside connecting with family and friends. Regardless of age, Matassi et al. (2019) explain that all participants understand WhatsApp as being a normal part of communicating every day.

Communication platforms such as phone calls and video calls, where additional context from non-verbal communication such as body language and eye contact can be shared, may be beneficial in building intimacy and connection between personnel and their Key Relations (Kaiser et al. 2022). However, these types of platforms also consider that users may not have constant access to personal devices. Therefore, using platforms that mediate immediate conversation, rather than the potentially delayed format of instant messaging, is understandable when you only get a specific amount of time daily or weekly to use personal devices. The findings in the current thesis suggests popularity of WhatsApp for participants could be due to its multi-function capability. This platform is able to send instant messages, images and videos for free regardless of the device, as well as voice and video call (WhatsApp, 2024). One participant who consistently highlighted WhatsApp as their preferred communication platform stated their main consideration when deciding how to communicate with their family is the platform being able to videocall, phone call and message (P16). The popularity of WhatsApp within these participants may explain why some individuals did not use platforms such as Facetime, due to an alternative app having multiple functions which address the requirements of participants' communication needs. Additionally, WhatsApp is available on Apple and Android devices, whereas Facetime may not be suitable for all family members and friends, as it is only available on Apple devices. This is consistent with the findings for what participants reported as being their most important consideration when choosing what communication platform to use with both their friends and relatives. The most frequently reported consideration was 'ease of use'. This provides a rationale for using WhatsApp as one platform for different forms of communication, due to it being easy to set up and communicate on one platform with all type of friends and relatives, on a large number of devices. Furthermore, WhatsApp is more beneficial than traditional SMS or text messaging due to the ability to use it over Wi-Fi at no cost (Church & de Oliveira, 2013). This is beneficial for sharing pictures of videos when personnel are deployed and cannot see their Key Relations frequently as it can build a feeling of openness and social support (Bittner et al. 2014). It can also reduce the cost of roaming charges on personal devices if personnel are deployed overseas, which may otherwise prevent personnel with communicating frequently with their Key Relations. Participant 13 highlighted in a qualitative response in the survey that they would use WhatsApp for all phone calls when deployed due to the cost of doing this when overseas. One additional benefit of WhatsApp discussed in the literature is the role of group chats, whether that be for keeping in touch with multiple family members or a group of friends (Taipale & Farinosi, 2018; Matassi et al.,2019). The role of group chats in communication in a variety of platforms was asked about in Phase 3 of this research to address the gap, and Chapter 6 discusses supplementary vulnerabilities presented by the use of group chats.

Addressing research question 2b, the results suggest that age may play a role in influencing the use of social media platforms such as Snapchat, Instagram and Twitter. Participants aged 41-50 years old consistently used these communication platforms less than the other participants. Comparatively 100% of participants aged 30-35 years old reported using all types of communication platforms provided to them. However, it is important to consider there were only 2 participants in this age group, and 28 participants in this study overall. Therefore, whilst this study presents initial evidence that age may play a role in influencing the choice of communication platform, there is no clear indication on the direction of this influence on behaviour. Whilst this is something that would benefit from being explored further with a larger

participant sample, Phase 2 of this research discusses the role of age in online behaviours further in Chapter 4. This being said, the situation of deployment may also explain why social media sites such as Facebook, Snapchat, Instagram and Twitter are less frequently used. Due to the research aiming to understand the role of military friends and relatives in organisational cyber resilience, the questions in this study focus on communication platforms used when contacting friends and relatives.

The results of the current research found that alongside 'ease of use', 'security' was the most frequently identified consideration that is important for participants when determining what platform to use when communicating with their Key Relations. Sixteen participants mentioned security when asked what the most important consideration is for deciding which platform to use to communicate with a friend or relative. Despite this being a free-response text box, participants mainly provided short responses that consisted of multiple one-word responses rather than full sentences with justifications or context for their responses. For example multiple participants simply stated "Security" or "secure" alongside other considerations such as "Ease of use". One participant provided more detail by stating "the security of the information I am telling them", however it would be beneficial to have more context into why they consider this important. This is explored further in Chapter 5, with the Phase 2 findings, and in Chapter 6, with the Phase 3 findings.

The frequency of participants mentioning security suggests that participants are considering the importance of security when deciding how to communicate with their Key Relations. However, whilst it is a positive finding for a study focusing on cyber resilience within military organisations that personnel consider security in their decision making, there are multiple suggestions for why this may not be representative of the entire military population. The research and the survey itself were advertised as exploring cybersecurity and cyber resilience within military organisations. Therefore, participants may have responded in a way that addresses the aim and demonstrating demand characteristics. Additionally advertising the research as being about cybersecurity may have encouraged those with an interest in cybersecurity, whether that be a personal interest or due to their job role, to take part. These individuals would have a higher knowledge and awareness about cybersecurity and therefore may have wanted to respond in a socially desirable way. This means that they could have identified they consider security as a top priority, due to possessing the knowledge that is the desired behaviour, even though this may not be the case. Whilst these biases are difficult to avoid in surveys, this phase is supported by Phase 2 of the research, which conducted interviews with military personnel and defence subject matter experts. The more relaxed and immediate response of a conversation in an interview provides the opportunity to reduce the effect that these biases may have on any final conclusions.

An element that could be considered here, though not explicitly stated by participants is the influence of trust of a platform, as trust intersects with security when considering the success of a social media platform (Zhang & Gupta, 2018). Social media platforms which experience security concerns, particularly if they have been involved in a cybersecurity attack resulting in a breach of user information, are perceived as less trustworthy to users (Ayaburi & Treku, 2020). Dechand et al. (2019) identified that individuals feel vulnerable to online threats when using WhatsApp and lack trust in technical situations, including encryption, implemented by WhatsApp to keep users safe. However, due to the high proportion of Military personnel using WhatsApp to communicate with their Key Relations, this may not be the case for the population group in this thesis. An additional consideration of trust for social media platforms, is that is trust

may not be entirely dependent on the platforms themselves. Abbas Naqvi et al. (2020) suggest that an individual's intention to use a social media platform can be influenced by others regularly using the platform and recommending it to others. Therefore, the decision to use a platform may not be determined by the individual's personal trust of a platform, but rather the trust of others they are close to. In the context of this study, Military Personnel may have knowledge that WhatsApp is less secure than other platforms, and they have a low level of trust towards the platform, but ultimately use it due to their Key Relations trusting the platform. Future work would benefit from directly exploring the trust of military personnel towards online platforms, as well as security, to provide more insight into the understanding of their online behaviour when communicating with their Key Relations.

When addressing Aim 2, it was found that military personnel do use a variety of communication platforms when communicating with friends and relatives on deployment, though WhatsApp was frequently highlighted as the most preferred platform. Participant responses suggest this may be due to the WhatsApp's ability to video call, voice call, voice message, instant message and send videos and images all in one platform. This can be done with Internet access which reduces the negative impact of roaming charges when deployed overseas. However, future work would benefit from exploring how the consideration of security influences military personnel's decision-making process when determining which platforms to use to communicate with their Key Relations, when on deployment.

### **Aim 3: Identify what topics military employees discuss with their friends and relatives over online platforms.**

This section will discuss the findings in relation to Aim 3 of Phase 1, this aim has one research question which is:

- **Research question 3:** *Do military personnel discuss sensitive military information with their Key Relations along with more mundane and everyday topics?*

Addressing research question 3, the results from this study identified that participants discuss a range of topics with their friends and relatives. Whilst no participant specifically identified that they discuss sensitive military information with their key relation, some participants did report that they discuss topics with their Key Relations that could accidentally contain sensitive information. These topics include: 'Your day-to-day work schedule', 'Advice about personal problems', 'Advice about work problems' and 'Information about colleagues'. Research into self-disclosure explains that a range of factors may determine someone's decision to disclose information about themselves (Greene et al. 2006). However, relationship strength appears to play a role in this process, with a higher perceived quality of relationship resulting in higher levels of emotional disclosure (Gore et al. 2006). Particularly as this can then continue to positively impact how the relationship is perceived (Sprecher & Hendrick, 2004). This suggests that military personnel may be more likely to share sensitive information, including operational information, with those who they consider a strong relationship. For the current thesis research, the highest mean relationship score was with a husband, wife or civil partner, closely followed by a cohabiting partner. With all of these types of relationships, participants reported they would discuss a wide range of topics. At least one participant identified they would discuss the topic outlined above as potentially containing sensitive military information. Some research suggests this effect of a perceived strong relationship encouraging self-disclosure is replicated online. For example, finding that those who perceive their online social network as close friends were more likely to self-disclose online (Wang et al. 2016; Bak et al. 2012). Whilst the results are able to

identify what the strongest mean relationship was for the participants, it is difficult to determine what other scores are considered a strong relationship. Results from participants in the current thesis found that on average participants rated their online friendships as lower in relationship strength than their offline relationships. However, participants still reported they would discuss personal problems with these types of friends, potentially resulting in incidental disclosure about operational information. This is particularly concerning for a friendship that is purely online due to the risk of a threat actor posing as a friend to gain information. This being said, the question wording and response did not ask participants to identify if they were discussing their own personal problems, or the problems of their friend. Whilst the intended meaning was that it was the participant's problems during analysis some responses, for example participants responding they would discuss personal problems with a child, suggest participants viewed it differently. Therefore, this could potentially convey less risk than the results suggest. Phase 2 provides the opportunity to explore risk behaviours that military personnel and their Key Relations engage with online that could impact on military cyber resilience. Further discussion on potential risk behaviours relating to information sharing and disclosing sensitive military information is included in Chapter 4.

## 4.5. Limitations and Considerations for Future Research

The main limitation for the results of the research is the size of the sample with only 28 participants completing the survey. However, this is a challenging population to recruit from due to difficulties in accessing the population as a civilian researcher, but also due to the survey fatigue that military personnel experience that may make them reluctant to take more in more research (Miller & Aharoni, 2015). The findings still provide valuable insight into the definition of a military close relation when considering the percentage of the sample that identified a wide range of friends and relatives as people they would contact on deployment and have a strong relationship with. This provides support that this definition should be expanded to incorporate these extended relations and friends. Not only to address cyber resilience within military organisation, but also in considering that those who may be adversely affected by supporting their military person mentally and physically. Additionally, whilst a similar number of participants from the British Army (11 participants) and Royal Air Force (12 participants) completed the survey, this was much lower for the Royal Navy with only 3 participants serving this branch of the British Armed Forces. As this study did not compare differences between these groups, this is sufficient to provide insight for this study. However, it is noteworthy to mention that the lack of responses from individuals within the Royal Navy could mean there are perspectives that might not have been considered within the findings of this phase of the research. Each branch of the Armed Forces has various services which may require different levels of security and challenges with communication. For the Royal Navy, submariners experience unique communication challenges due to spending a large amount of time underwater, where operational success is dependent on being covert and unidentifiable, therefore communication emissions are limited, which reduces their ability to keep in touch. Similarly Royal Navy ships deployed at sea will have less connectivity due to there being less infrastructure at sea, satellites are used but often they rely on communications infrastructure when they go near coastlines. Whilst the responses from this survey are sufficient to provide insight, that can be developed in Phases 2 and 3 of the project, future work may benefit from exploring a wider range of perspectives from military personnel across the Front-Line Commands. The findings from this phase of the research are supplemented by Phase 2, discussed in Chapter 4. Phase 2 explores similar topics, including who military personnel consider to be their Key Relations, in a more open dialogue format, providing the opportunity to understand these relationships in more detail.

This research used an online survey distributed using a survey platform, Qualtrics. However, a meta-analysis of literature using surveys identified that when comparing the use of online surveys compared to more traditional survey formats, including mail, e-mail and phone surveys, online surveys could yield a lower response rate compared to more other traditional formats (Wu et al., 2022). There were multiple justifications for using an online survey for this research, as outlined in Chapter 3. The main justification was due to access to participants through Dstl, who contacted unit commanders to send out the link to the survey, and the link to the survey was also posted online on staff intranets and forums. This ensured ethically that all participants were encouraged to complete the survey anonymously and through their own choice rather it being perceived by individuals as a direct command to complete the survey. The researchers reflect that the choice to conduct a mail study could be more useful in future research to gain more responses. However, this may not be appropriate considering the study explores cyber resilience and focuses on online experiences. Providing participants the option to complete the survey either online or in a paper-based format could address any concerns of low response rate due to the online nature of the survey. Additionally, any replications or

developments of the survey should consider question wording of the survey to provide participants with more clarity. For example, it should be explained to participants that if there is a relationship that could fit into more than one category of relationship type, they should respond in the category that is most suitable for the person they are considering. Furthermore, future research should consider how to delineate if participants are discussing one or multiple people within a category. For example, with grandparents, parents, siblings and other relationships, where the category could be one or multiple of the same type of relationship. This provides participants with the opportunity to discuss any differences in communication behaviours with these individuals.

## 4.6. Takeaways from Phase 1

The findings from Phase 1 indicate that a wide range of relationships should be included in the definition of Military Key Relations. Participants reported they would contact a range of relatives, including short-term partners and extended family, alongside ‘dependents’ or ‘next of kin’ relationships. Additionally, a large proportion of participants highlighted they frequently contact friends, as well as relatives when on deployment. The results suggest a pattern of military personnel more frequently contacting Key Relations who they consider themselves as having a stronger relationship with. The definition of Military Key Relations based on findings from Phase 1 includes the following friends and relatives:

- Wife, Husband or Civil Partner
- Co-habiting partner
- Short-term partner (less than 1 year)
- Parent or Guardian
- Child
- Sibling
- Grandparent
- Cousin
- Aunt or Uncle
- Cohabiting friend
- Friend from school
- Family friend
- Friend met online (met in person)
- Online friend
- ‘Close’ or ‘Best’ friend

The findings also suggest a wider range of topics are discussed with these Key Relations who participants contact more frequently. As discussed, this communication happens on a wide range of communication platforms, with WhatsApp being the most frequently preferred platform to communicate regardless of relationship type, or participant age. Participants most frequently reported ‘ease of use’ and ‘security’ as being their most important consideration when deciding how to communicate with their Key Relations. Deeper insight into why this might be and how this influences the decision-making process would be beneficial in understanding online behaviours, and potential risk behaviours associated with Military Key Relations that could contribute to military cyber resilience. Additionally, to investigate the influence of age on these factors, future research would benefit from recruiting a larger participant sample to reflect the age distribution

of the British Armed Forces. Particularly including more participants aged 20 – 29, to accurately reflect this is most common age group for personnel in the British Armed Forces.

## 4.7. Chapter Summary

This Chapter provided an overview of Phase 1 of the research project, beginning with conducting the pilot study and explaining how this influenced the main study. The process of the main study method, and results were outlined, followed by a discussion of how these results relate to existing literature in this area. Finally, limitations of the research were highlighted, along with suggested directions for future research to provide a deeper understanding of how military personnel perceive their communication with their friends and relatives. This Phase provided a definition of Military Key Relations that was used to guide Phase 2, which is discussed in the next Chapter.

## Chapter 5 - Phase 2: Exploring the perspective of Military Representatives and Subject Matter Experts (SMEs) in Online Semi-Structured Interviews

Phase 2 builds on findings explored within Phase 1, as outlined the previous chapter. Phase 1 defined which friends and relations should be considered as Key Relations of military personnel, and includes dependents, alongside extended family members and close friends. Phase 2 incorporated the definition outlined in Phase 1 and built on these findings with qualitative methods, to provide a more detailed overview of who should be considered as a key relation for military personnel, using semi-structured interviews. Phase 1 also provided an overview of the online communication behaviours between serving military personnel and their close relations. Phase 2 sought to build on this by identifying which online behaviours exhibited by Key Relations could create a risk for cyber resilience in military organisations. This was achieved by exploring the perspective of military representatives across the Front-Line Commands (FLCs) and subject matter experts (SMEs) in two areas: Cyber education & awareness, and Cyber Incident Reporting & Monitoring. By exploring the perspective of SMEs alongside military representatives Phase 2 can also start to identify what materials for cybersecurity training, education and awareness exist for military friends and relatives. This material provides friends and relatives with an overview of which threats they should be aware of that might pose a risk to UK defence, it's people and capabilities and how to engage in secure cyber behaviours to mitigate these risks and keep information safe. Participants were also asked their opinion on how future cybersecurity training, awareness and education initiatives can best engage military personnel's Key Relations. Effective initiatives will provide Military Key Relations with the opportunity to learn how to keep their own, and their military person's information safe online to protect the military individual and unit.

Chapter 2 outlined the role of Cybersecurity Culture in exploring cyber resilience, identifying a key aspect within Cybersecurity Culture is the notion of responsibility. Responsibility within cybersecurity is defined as the process of ensuring everyone involved within cybersecurity is aware of their role and how their behaviour contributes to security (Nel & Drevin, 2019). Phase 2 gathers the opinions of military personnel and SMEs to provide insight into their understanding of who should be responsible for monitoring the online behaviours of military personnel's Key Relations. Additionally, Phase 2 explores the role of the military organisations, the military personnel and the Key Relations in supporting behavioural awareness and change for Key Relations, to encourage secure online behaviours. The opinions of military representatives and SMEs in this phase are compared to the perspective of Key Relations themselves in Phase 3, in Chapter 5.

Participants engaged with online semi-structured interviews with three aims and three related research questions to address these aims. Aim one focuses on exploring the current approach for engaging with Key Relations about their online safety. With the second aim focusing on exploring potential online behaviours that are being exhibited by Key Relations. The final aim focuses on understanding who the responsibility of Key Relations' online behaviour and online safety should fall to. The qualitative approach allowed participants to explain responses they gave and for us to understand why these responses were given. The full aims and the respective research questions are outlined below:



**Aim 1:** Map the existing situation for how organisations involve Key Relations in cyber resilience

**Research Question 1:** *Are the military friends and relatives who are identified as Key Relations the same individuals who currently receive cybersecurity training?*

**Aim 2:** Gather opinions from military representatives and SMEs about the potential online behaviours being exhibited by Key Relations

**Research Question 2A:** *What types of online behaviours are friends and relations displaying?*

**Research Question 2B:** *How could these behaviours present a cybersecurity risk to military organisations?*

**Aim 3:** Gather opinions on responsibility of Key Relations cybersecurity training and online behaviour from military representatives and SMEs

**Research Question 3:** *Who should be responsible for Key Relations' online behaviour and their cybersecurity training, education and awareness?*

**Aim 4:** Gather opinions from military representatives and SMEs about how to guide future research

**Research Question 4:** *What should Key Relations be asked in Phases 3 & 4 to help guide creation of engaging cybersecurity initiatives?*

## 5.1. Phase 2: Pilot Study

Phase 2 began with a pilot study to ensure the interview schedule questions were appropriate and relatable to the sample. The pilot study also provided an opportunity for me, as the researcher conducting the interviews, to become comfortable with the interviewing process with this population, including ensuring questions did not stray outside of the required classification of information. The pilot study process also provided the researcher with the opportunity to familiarise themselves with the process of inductive thematic analysis. The following section outlines the pilot study method including the procedure and the participants followed by an overview of the results and reflections and amendments required following the pilot study process.

### 5.1.1. Method

The pilot study conducted online semi-structured interviews, which took place on Microsoft Teams. The pilot study sample consisted of 2 military representatives, both who are considered experts in their field, with longstanding careers within the military. One participant serves in the Royal Air Force and the other in the Royal Navy. Prior to being distributed to the participants the questions were reviewed by members of the Dstl Military Advisor Community to ensure they were appropriate for the population and adapted accordingly. Question topics consisted of:

- Opening questions:
  - Job role overview
  - Overview of who they consider close relations
- Friends and relatives specific questions:
  - Opinions on potential online risk behaviours of friends and relatives
  - Opinions on recommendations to mitigate against these potential risk behaviours

- Overview of any cybersecurity training and awareness they receive as part of their role
- Opinions on what should be included in cybersecurity training and awareness initiatives for Key Relations.
- Opinions on potential barriers for Key Relations engaging with cybersecurity initiatives.
- Opinions on the responsibility for Key Relations' online behaviours in a military context.
- Future research questions:
  - Opinions on what is important to ask Key Relations to guide formation of future cybersecurity initiatives.

The full question schedule, including optional questions can be found in [Appendix B](#). The interviews were recorded and transcribed before being analysed using inductive thematic analysis (Braun and Clarke, 2021), as outlined in the methodology chapter, [section 3.4.2](#).

### 5.1.2 Results and Discussion

An inductive thematic analysis of the pilot study data was conducted to test the feasibility of using an inductive thematic analysis in this study. This thematic analysis identified 8 main themes. Figure 5.1 provides a thematic map outlining the main themes and sub-themes for each main theme and the directional relationship between the themes. The theme table outlining the main themes, sub-themes, and transcript codes can be found in [Appendix H](#).



**“Defining close relations”** was the first main theme identified, it provides additional support for the definition of friends and relatives outlined in phase 1. This theme highlights how participants identified dependent relationships as close relations, whilst still maintaining additional relationships with friends and extended family, though these different types of relationships can require different approaches. This is reflected in the sub-themes ‘maintenance of non-Key Relationships’ and ‘different approaches to relationships.’

**“The role of individual differences in online behaviour”** reflects how online behaviour exhibited by friends and relatives is not identical for everyone and can be influenced by age, personality traits and embracing military culture. Participants suggested younger and older generations behave differently to each other, and to the military personnel themselves, in sub-theme ‘generational differences influence behaviour’. Sub-theme ‘adopting military culture’ summarises how friends and relatives with experience of military life, including relocation or dual-serving households adopt the military culture and tend to be more considerate of what they post online. This links to sub-theme ‘difference in threat acceptance’, outlining how civilians view social media as memories and a way to promote their business, whereas military personnel see online information sharing as a risk. One participant spoke about people with a desire to be accepted by others sharing more information online to increase public opinion of them, termed ‘desiring acceptance from others online’. Individual differences in information sharing behaviour can influence consequences, thus this theme relates to the main theme *“Impact of friends and relatives’ cyber risk”*. This theme also links to the main theme “Friends and relatives online risk behaviours” as participants suggested individual differences in behaviours influence cyber risk. Particularly when considering the individual differences in the level of awareness and knowledge people have about online safety in terms of themselves but also their military person, presented in the sub-theme ‘Different knowledge levels for the importance of online safety’.

To distinguish online behaviours exhibited by friends and relatives which present risk to cyber resilience, a main theme termed **“Risk behaviours of friends and relatives”** was created. Participants suggested ‘Generational differences in behaviour influences risk’, with older generations risk arising through lack of technological experience, and younger people not knowing the implications of their behaviour. Participants suggested the main risk presented by friends and relatives is sharing date, time and location information about military personnel and military equipment, termed ‘risk of sharing operational information’. This risk increases when considering Key Relations necessity of knowing where their military person is, represented by sub-theme ‘Expectation of access to personnel information’. The sub-theme ‘reduced understanding results in accidental compromise’ reflects how participants highlighted that risk from incidental information sharing can arise when friends and relatives are unaware of what information they should and shouldn’t be sharing online, with ‘word of mouth’ behaviour presenting an avenue for how this information can be shared. These risk behaviours influence recommendations for training and awareness, and link to main theme *“Improving training and awareness for friends and relatives”*, but also result in consequences for the military, as outlined in main theme *“Impact of friends and relatives’ cyber risk”*.

In theme **“Impact of friends and relatives’ cyber risk”**, participants outlined two types of consequence for military friends and relatives engaging in online risk behaviours, forming two sub-themes. ‘Information can be targeted by an adversary’ summarises how information shared about operational information can be used by an adversary to plan an attack. ‘Political and social ramifications of information sharing’ addresses the impact of how defamatory comments or

negative opinions from personnel shared with a friend or relative can be shared onwards into the public domain and viewed as representative of the military's opinion.

Whilst participants were asked questions specifically on how friends and relatives are currently involved with cyber resilience, additional information about their own approach to cyber training and awareness was discussed, forming the main theme **“Existing cyber training and awareness approach”**. The sub-theme ‘no existing approach for friends and relatives’ highlights the reliance of friends and relatives to use their own understanding of cybersecurity to make decisions when it comes to online behaviours that influence their military person. This is accompanied by sub-themes surrounding the existing military culture towards cyber of relying on cyber experts, due to fear of being embarrassed or not knowing the answers, reflected in sub-themes ‘Military culture does not encourage cyber mindset’ and ‘fear of embarrassment or not knowing’. The sub-theme ‘limitations of cyber training and awareness for employees’ details how participants identified challenges of cyber training being inconsistent with no information about friends and relatives online risk habits. This theme links with the main theme “Improving training and awareness for friends and relatives” as recommendations for future initiatives built on conversations about the existing situation.

*Main theme “Improving training and awareness for friends and relatives”* discusses suggestions for future initiatives to improve the contributions friends and relatives make to military cyber resilience. Three sub-themes focussed on creating content, the first focusing on ‘keeping up with threat landscape’. Additionally, participants highlighted that cyber can be complicated, but everyone should be able to understand the basics in sub-theme ‘accessible materials for everyone’. One participant re-iterated the importance of explaining why secure online behaviours are important to keep their military person safe to Key Relations, represented in the sub-theme ‘importance of the why, as well as the what’. The two other sub-themes summarised suggestions for engaging friends and relatives in cybersecurity initiatives, with ‘pride encourages engagement with materials’ focussing on the role of utilising the role of pride in information sharing behaviours as proud Key Relations are keen to get involved any way possible. Sub-theme ‘overcoming fear and information overload’ suggests that content needs to avoid scaring friends and relations or overloading them with information.

The final theme **“Responsibility for friends and relatives’ online behaviour”** feeds into the previous theme surrounding training and awareness, identifying who should manage aspects of friends and relatives’ online risk. Both participants suggested the military person should know what information is sensitive and what should be shared, reflected in sub-theme ‘military personnel to keep their information secure’. This relates to sub-theme ‘military personnel to communicate requirements to friends and relatives’ as military personnel should have open discussions and create boundaries with friends and relatives to reduce opportunity for compromise. This was supplemented with ‘barriers of communication between friends and relatives and military personnel’ where participants outlined open discussions about friends and relatives’ online behaviour and how it affects the military person may cause tension or upset with some Key Relations.

### 5.1.3. Alterations and decisions made following results and feedback

No questions were altered during the pilot study process as the use of a semi-structured interview schedule allows for the interview schedule to follow the lead of the participant, which occurred for both pilot study participants, and still covered all questions. However, it was found for the question which focussed on future research and seeking participants opinions about what

to ask Key Relations in Phases 3 and 4, both participants requested more information about what each phase would consist of. Therefore, in the main study the researcher provided more detail than the interview schedule originally detailed stating Phase 3 aims to explore online behaviours in an online survey, similar to a survey completed with military personnel and that Phase 4 aims to identify what Key Relations would like from any future cybersecurity training, education and awareness initiatives to help them engage with these programmes and highlight how best to keep their military person safe.

During the transcription of the interviews, the researcher noted considerations in the interview approach taken during the interviews. The first consideration was that some follow-up questions had taken more of a leading approach which reflects the experience of becoming familiar with the interview process and questions and served as a learning point and something to consider when asking questions in the interviews in the main study. The additional consideration was that sometimes the conversation naturally strayed away from the topic of friends and relatives to military personnel themselves. Knowledge of the approach by military personnel can be helpful in providing context, especially when considering the role of military personnel communicating rules and up to date information about cybersecurity threats and mitigation behaviours. However, the researcher reflected that it was important in the main interviews to bring the conversation focus back to friends and relatives whenever it strayed too far away, to ensure the objectives of the research are addressed.

## 5.2. Phase 2 Main Study: Method

### 5.2.1. Participants

Not including the pilot study participants, a total of 17 participants took part in the semi-structured interviews. Nine of the participants were military representatives from each of the Front-Line Commands. Eight of the participants were subject matter experts (SMEs), who had expert experience of working in cyber roles within the defence industry, specifically a military organisation. Table 1 provides an overview of the number of participants recruited from each job role and sub-category. Opportunity sampling was used to recruit participants, and potential participants were invited to participate by gatekeepers identified by the research sponsor to access the military community and SMEs. The researchers provided the gatekeepers with an overview of the research and contact details for the researcher, so interested individuals could contact the researcher directly ensuring voluntary participation. Whilst the intention was to recruit an equal number of participants for each role, there was some crossover of job roles within the SMEs which meant that after initial invitation and completion of interviews, additional SMEs with experience in Cyber Incident Reporting & Monitoring were recruited to adequately represent that population.

**Table 5.1.**

*The number of participants in Phase 2 and their specific job role*

Job Role	Number of Participants
Military Representative – Royal Navy	3 Participants
Military Representative – British Army	3 Participants
Military Representative – Royal Air Force	3 Participants
Subject Matter Expert – Cyber Education & Awareness	5 Participants
Subject Matter Expert – Cyber Incident Reporting & Monitoring	3 Participants

### 5.2.2. Materials

The materials consisted of a semi-structured interview schedule with questions divided into sections consisting of opening questions, friends and relative specific questions, responsibility questions, and a future research question. These questions were shaped by the experience from the pilot study and the full interview schedule can be found in [Appendix B](#). The interview schedule began with an opening section for the researcher to introduce themselves and the research and provide the opportunity for participants to verbally consent to take part. The opening questions followed this, of which the first consisted of asking participants about their job role. This was to provide the researcher with detail about what participant group the individual belonged to and provide context to ensure future prompts were relevant to the

individual. The second opening question aimed to support the findings from Phase 1 about the definition of Key Relations by asking participants who they describe as their close relations. Participants were prompted to consider friends, as well as relatives. As both opening questions provide the opportunity for participants to divulge personal information, these questions were framed to ensure participants only answered with as much detail as they were comfortable with. The friends and relative specific questions began by asking participants about their opinion on friends and relatives online behaviours that could present a risk to military organisations. Prompts focused on social media and risks of shared networks and devices. To develop the conversation towards training, education and awareness initiatives, participants were then asked about their own cybersecurity training and awareness they have in their own job, including their opinion on this training and areas for improvement. Participants were then asked what existing cybersecurity programmes they knew of for friends and relatives, with prompts about what they think would be good to include, and if there's anything they receive as part of their training that would be worthwhile friends and relatives becoming aware of. There was only one question about responsibility which asked participants to consider that as Key Relations can be a target for military adversaries, who they think the responsibility of Key Relations online behaviour should fall to. Prompts asked whether it should fall solely to Key Relations or others, and then why they directed responsibility in this way. Finally, participants were provided with information about Phases 3 and 4 of the research project, outlining these Phases focus on the perspective of friends and relatives themselves and consist of an online survey about online behaviours (Phase 3) and then focus groups to inform training, education & awareness programmes (Phase 4). Participants were then asked their opinion on what questions should be asked of friends and relatives in Phases 3 and 4 of the research project.

Whilst questions were nearly identical for all the participant groups, additional prompts were included for some participant groups to draw on their experience in their role. For SMEs in Cyber Education & Awareness, it was expected they would be aware of existing materials friends and relatives could access about online safety behaviours and cybersecurity risk, so an additional prompt was included to address if they think there are any gaps to address in these materials. For SMEs in Cyber Incident Reporting & Monitoring, the question schedule was altered slightly with the question about their own training being included as an opening question. Additionally, these SMEs were also asked about recommendations they had to mitigate online risk behaviours friends and relatives might have to military cyber resilience. This question allowed them to use their experience to provide an opinion about online security behaviours that should be a priority for friends and relatives.

### 5.2.3. Procedure

Participants were invited to participate in the interviews by a Military Advisor and Technical Partner at Dstl who acted as a facilitator to enable access to potential participants via email. These individuals provided an overview of the aims and objectives of the research, what the interviews consisted of details about compensation and the interviewers contact details. Participants interested in the research contacted the interviewer who provided the Participant Information Sheet (PIS) and Informed Consent Form (ICF). Participants returned the consent form via email either by including an online signature or by printing and scanning the forms with a handwritten signature. Once the ICF was returned completed, a time was arranged to conduct the interview. Interviews took place on Microsoft Teams and participants were invited to choose whether to have their cameras on or off. The researcher had their camera on, to encourage rapport with participants. The interviews were participant led with the researcher following the



semi-structured interview schedule outlined above and took approximately 45 minutes to complete. At the end of the interview, participants were fully debriefed.

#### 5.2.4. Ethical Considerations

To encourage voluntary participation, individuals interested in taking part in the research contacted the researcher directly, who provided a copy of the PIS and ICF. Participants were encouraged to read the PIS and take at least 24 hours thinking time to consider the points and ask any questions they had. The PIS also highlighted to participants that deciding to take part would not affect their career, to mitigate participants feeling obliged to participate because of the nature of military organisations and following an order from the Chain of Command. Only once the ICF had been returned completed did the researcher and participant agree a time for the interview to take place. At the beginning of the interview, participants were provided with a reminder of the aims of the study, and what would be asked of them in the interview, including a reminder that there was no requirement to answer any questions, and that they could choose to end the interview at any point, and asked to confirm if they were still happy to continue. A copy of this overview is provided at the beginning of the interview schedule in [Appendix B](#). At the end of the interview, participants were provided with a debrief sheet which signposted support services, some of which are military focussed. Participants were compensated for their time by following the process of the Ministry of Defence's Experimental Test Allowance (ETA). The compensation rate was calculated based on the published rate for ETA at the time and guidance from the Ministry of Defence Research Ethics Committee (MODREC), totalling £9.51.

A Dictaphone was used to record audio from the interviews, rather than the capability to record available on Microsoft Teams which automatically records audio and visual data. This allowed participants to have their cameras on if they desired. Immediately after completing the interviews, audio files were stored on a password protected electronic drive and deleted from the Dictaphone. Participants were informed they could choose to withdraw from the study up to seven days after completing the interview. After this period, the audio recordings were transcribed and labelled with a pseudonym so that participants could not be identified. Transcription occurred in the two weeks following the 7-day cooling off period, and audio files were then deleted. Data including transcriptions, codes, theme tables and thematic maps were stored on a password protected drive with multi-factor authentication enabled. Data passed between researchers during the process of assessing inter-coder reliability was sent between researchers via email in a password protected format. The data (not including the audio file) will be stored for 5 years in accordance with the ethical guidelines provided by the British Psychological Society. The phase of the research was examined by and received favourable opinion from three separate ethics panels, the Dstl Scientific Advisory Committee (SAC), MODREC and Bournemouth University. Evidence of this is included in [Appendix F](#) and [Appendix G](#).

#### 5.2.5. Data Analysis

The interview transcripts were analysed using Braun and Clarke's (2021) process of inductive thematic analysis, which follows a six-step approach to analysing qualitative data. These steps were discussed initially in Chapter 3, the following section describes how the analytical approach was applied to the current dataset.

The interviews were manually transcribed for security reasons, however this also provided the opportunity for the first step of the analysis to begin to take place, familiarisation

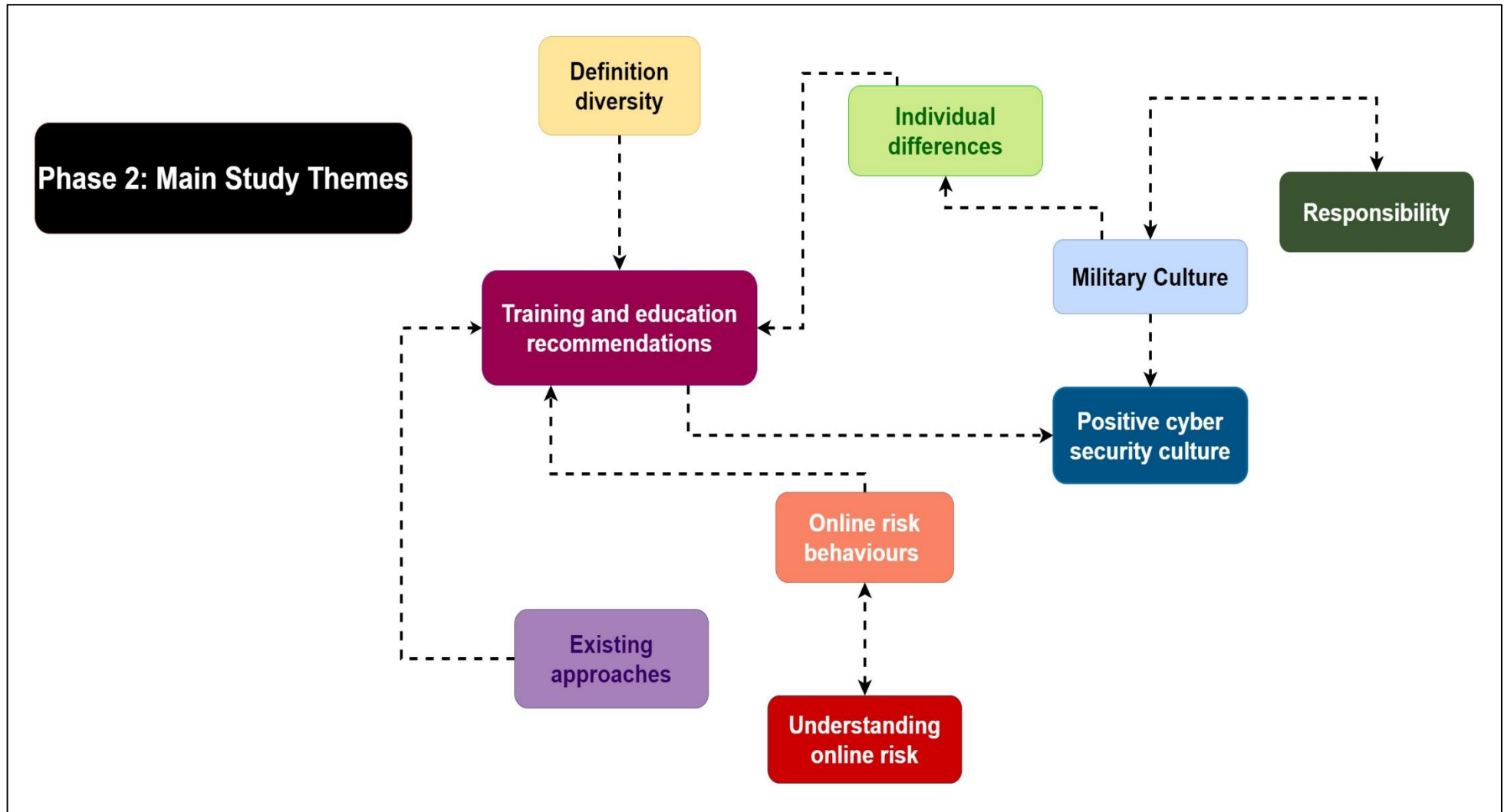
with the data set. As the researcher using the analysis, conducting the interviews and transcribing the interviews, I was able to start the familiarisation process early and continued the process by reading the transcripts multiple times. During this period of familiarisation, I made reflective notes about the interview process but also made notes about any of my initial thoughts about codes. No actual codes were created until the next step of analysis, coding. When reading through the transcript I applied code labels to describe the data, using the comment function in Microsoft Word. Code labels were not included for each line of the data, with some code labels reflecting multiple lines of the interview. During this process both semantic and latent codes were created. Semantic codes reflect surface level information, such as clearly stating risk behaviours, whereas latent codes reflected more implicit meanings. An example of latent codes occurred when participants discussed how the role of framing engagement between military organisations and Key Relations about online behaviours should be positively reinforced and positive stories about Key Relations shared, which was coded as accountability and discouraging blame culture. To assess reliability of the analytical process, inter-rater coding occurred. This process involved a second researcher analysing three transcripts, two transcripts were from military representatives of different Front-Line Commands, and one transcript was an SME in education and awareness. Following the coding of each transcript, the codes were collated, and similar codes clustered together to identify patterns within the data from codes. In this stage, the early draft of a theme table was formed. Due to the length of the transcripts, this was done initially for each transcript, and then transcripts were collated to identify themes for all the data from all transcripts. This allowed for a natural progress of the next step of analysis, developing and reviewing themes. The step of developing and reviewing themes aims to understand whether the themes that have been identified are representative of the full data set. For this research, some themes that appeared frequently within early transcripts became less poignant as the analysis process developed and became sub-themes of a main theme, rather than a main theme. Once themes and sub-themes were identified from the analysis of all transcripts, and all relevant code data collated, the process of fine tuning the names of the themes and sub-themes, as well as their description occurred. For example, one initial theme was created which encompassed the variety of online risk behaviours related to military friends and relatives, such as social media behaviours and lack of understanding about technology. As the analytical process progressed, this theme became expansive to the extent one theme was not representative of the facets of these risk behaviours, and so two separate themes were created. One to address the online behaviours that could pose a cybersecurity risk to military organisations, termed *Online risk behaviours*, and a second theme reflecting the potential reasons individuals might engage in online risk behaviours, termed *Understanding online risk*. Throughout the process of refining the themes, codes which did not initially align with any of the themes and ideas were placed in an 'unallocated' theme. As the themes become more refined, some of these unallocated codes were included in these refined themes.

During the theme refining process a large element of inter-rater coding occurred. Once the data was collated into a refined theme table, the second coder reviewed the results to assess any discrepancies in theme creation or wording. The final step of a thematic analysis is the writing up, which has been done in this thesis in the results section of this chapter. The results section provides a written overview of the themes and sub-themes, as well as detail about the reflective process which I used throughout the analysis process. Once the data had been collated into the final theme table and thematic map, the second coder assessed the results to provide agreement on themes, and how they were represented. The results of this analytical process will

be discussed in the following section, with Figure 5.1 being a thematic map which outlines the relationship between the themes. The theme table for these results are included in [Appendix I](#).

Figure 5.2:

Main study themes following a thematic analysis and the relationship between the themes



### 5.3. Phase 2 Main study: Analysis

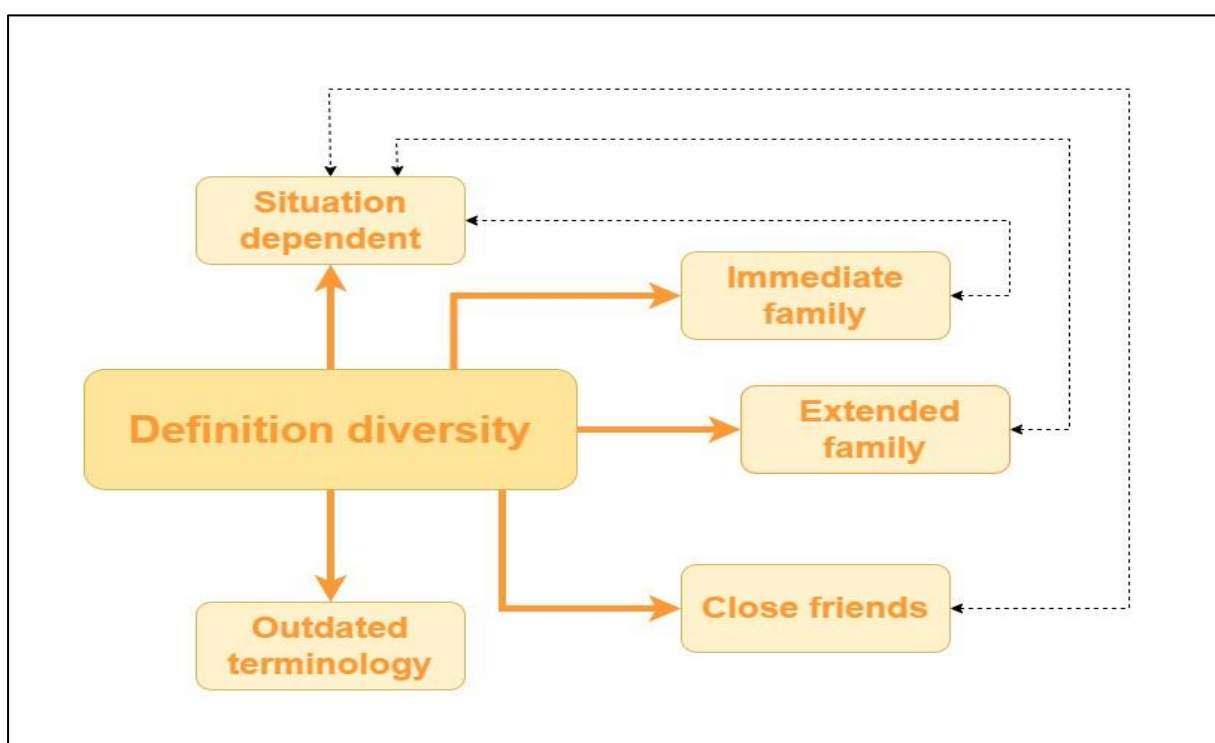
This section approaches the findings from a qualitative style where the results and discussion are reported together. This style of writing is recommended when applying Braun and Clarke’s (2021) approach to thematic analysis as it allows interpretation of the results to be integrated into the explanation of the findings. This chapter reports 9 main themes, (1) **Definition diversity**; (2) **Online risk behaviours**; (3) **Understanding online risk**; (4) **Individual differences**; (5) **Existing approaches** (6) **Training and education recommendations** (7) **Military culture**; (8) **Positive Cybersecurity Culture**; (9) **Responsibility**. This analysis section will provide an overview of these themes, including the relevant sub-themes. Whilst each main theme is distinct, some themes approach different aspects of the same topic. Theme 2, **Online risk behaviours**, is closely related to theme 3, **Understanding online risk**, as theme 3 discusses potential reasons for why individuals might choose to engage in the online risk behaviours outlined in theme 2. Figure 5.2 is a thematic map outlining the main themes and how they relate to each other, the full theme table including transcript codes can be found in [Appendix I](#).

#### 5.3.1. Main theme 1: Definition diversity

This theme explores the individual friends and relatives that participants identified as those they consider Key Relationships, during the interviews. Participants highlighted a range of friends and relatives, which are discussed further in sub-themes: *Immediate family*, *Extended family* and *Close friends*. Participants also highlighted that the definition of a key relation can be dependent on other factors, in sub-theme *Situation dependent*. Finally, this theme explores how the language currently used within military organisations and the approach to friends and relatives does not reflect current society in sub-theme *Outdated terminology*. Figure 5.3 provides an overview of these sub-themes and the relationship between them, and this section then discusses these sub-themes in more detail, and in relation to existing literature.

**Figure 5.3:**

*Sub-themes of Theme 1, **Definition diversity**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.*



When asked who they consider to be their Key Relations participants frequently mentioned family relations such as parents, spouses, siblings, and children, which was reflected in the sub-theme *Immediate family*. During the reflexive part of the analysis, the researcher noticed that participants tended to distinguish these individuals from other family members and friends by listing them first in one group and then pausing to consider any additional relatives or friends that they considered in their definition of Key Relations. Supporting the findings from Phase 1, most participants mentioned a spouse as a key relation, with one participant claiming their wife was their closest relation (P11). This point is reinforced by the suggestion that participants tend to disclose much more information to their partner about their job compared to other Key Relations, “it’s almost unavoidable to talk to your spouse about all of these things [...] there’s only so much obfuscation you can actually achieve” (P17). An additional consideration from the sub-theme *Immediate family* is the frequent mention of siblings, alongside parents, partners, and children. This consideration of family relationships extended outwards including blood relatives such as aunts, uncles, and grandparents, termed as sub-theme *Extended family* as demonstrated by participant 6 “There’s a lot of security things out there concerning family and not just direct family, aunties and uncles”. The researcher reflected that these types of relations differed from immediate family as they are not generally people personnel would cohabit with but would see frequently and may have access to information that could present a cyber risk if shared online. Relations are not limited to blood relatives, with some participants discussing how family through marriage such as in-laws and other members of partners’ families, would be considered a key relation, “and some of my wife’s family” [P8]. Additionally to family participants also identified friends as Key Relations in sub-theme *Close friends*. There was no consistent definition of which friends were considered Key Relations by participants and the type of friend varied in strength with friends from school (P13), a close neighbour (P8) and friends considered acquaintances that have frequent contact through hobbies and sports (P3). Supporting findings from Phase 1 the term ‘best friend’ was used which supports the notion that friends can be considered as close as family relations by some people. Many participants mentioned colleagues as friends, with some even stating their colleagues are closer friends than non-serving friends (P2), but that their life is led in two parts with friends from home and work friends not integrating, “in the military you have the two parts of your life so friends from growing up but then you meet a whole host of people along the way you’d class as friends” (P13). Friends who are immediate colleagues or serving in another unit or branch would already receive similar cybersecurity training to any military person, due to being a military person themselves therefore are not included within the definition of Key Relations in this thesis.

There was some suggestion that the inclusion of certain friends and relatives is conditional to the situation and environment, with the definition being open for interpretation, in sub-theme *Situation dependent*. Participants highlighted the importance of considering the role of technology when defining Key Relations as our contacts have become more widespread, with one participant stating, “it’s a really difficult one to define especially with globalisation and how well connected we are across the world” (P15). As technology plays an increasingly important role in our everyday lives, and when considering cybersecurity, participants suggested that a close relation when could be anyone that can reach us on social media. This access may be direct as a friend or connection, or indirect through viewing our online activity, “anyone who can access your social media page or is able to post something about you could be counted as close” [P13]. Additionally, one participant reflected how blended families may present a unique approach to Key Relations, and the importance of considering an ex-spouse as a key relation due to the logistics of co-parenting [P8]. This is an interesting point when considering the extent Key

Relations have access to information about military operations when the individual is deployed. Someone who would not necessarily be considered a key relation by the individual or military organisation may still require cybersecurity education and training to understand their role in keeping sensitive military information secure. This lack of consideration from military organisations about the diversity of Key Relations is discussed in sub-theme *Outdated terminology*. Military organisations currently focus on next of kin relationships and dependents recorded by personnel in the Joint Personnel Administration (JPA) system. This sub-theme, *Outdated terminology*, highlights how friends and family have concerns that the term dependent isn't reflective of current society and how Key Relations "had their own working capacity and their own goals, they weren't dependent on the military personnel for daily living" (P15). Gribble et al. (2020) in a review of the literature focusing on military families, suggested the terminology most commonly used reflects a heteronormative and two-parent family, with family dynamics such as single-parent families, unmarried relationships and LGBTQ families being under-represented. Therefore, it is important to provide terminology that reflects the variety of loved ones that a military person may have in their life, when approaching all research on military families, including cyber resilience.

This theme of **Definition diversity** supports the findings from Phase 1 where an initial definition of the term 'Key Relations' was created. Sub-themes reflect participants' range of Key Relations including immediate family, extended family, and friends and corresponds with initial findings from Phase 1, which can be found in Table X in Chapter 3. Based on the findings from both Phase 1 and Phase 2 sub-themes, the definition of 'Key Relations' identified from this research includes the following friends and relatives: Spouse/Civil Partner, Unmarried partner, short term partner (less than one year), Parent or Guardian, Child, Sibling, Grandparent, Extended family e.g. Cousin, Aunt, Uncle, Niece, Nephew, Co-habiting friend/roommate, Friend from school and 'best friend'. Whilst this definition was created with the intention of directing future cybersecurity initiatives, there is the potential for this to be extrapolated to different areas military organisations consider friends and relatives. A plethora of research exists on the detrimental effects of a relative serving in the military on dependents mental health, however this research mostly focuses on spouses and children, without considering that an individual with an unmarried partner, not identified as a next of kin may not be offered the mental health services to help them support their military person. This is important when you consider the role of family and friends in supporting the welfare of military personnel, so they can complete their role successfully. Woodall et al. (2021) found that military personnel with spouses that had dissatisfaction with the military and perceived the same for their serving person, had higher marital conflict and the service person was more likely to leave the military. However, this effect was mediated when the spouses had a higher level of social support (Woodall et al. 2021), demonstrating the importance of military organisations supporting Military Key Relations, wherever possible, as this ultimately benefits the personnel and the organisations themselves.

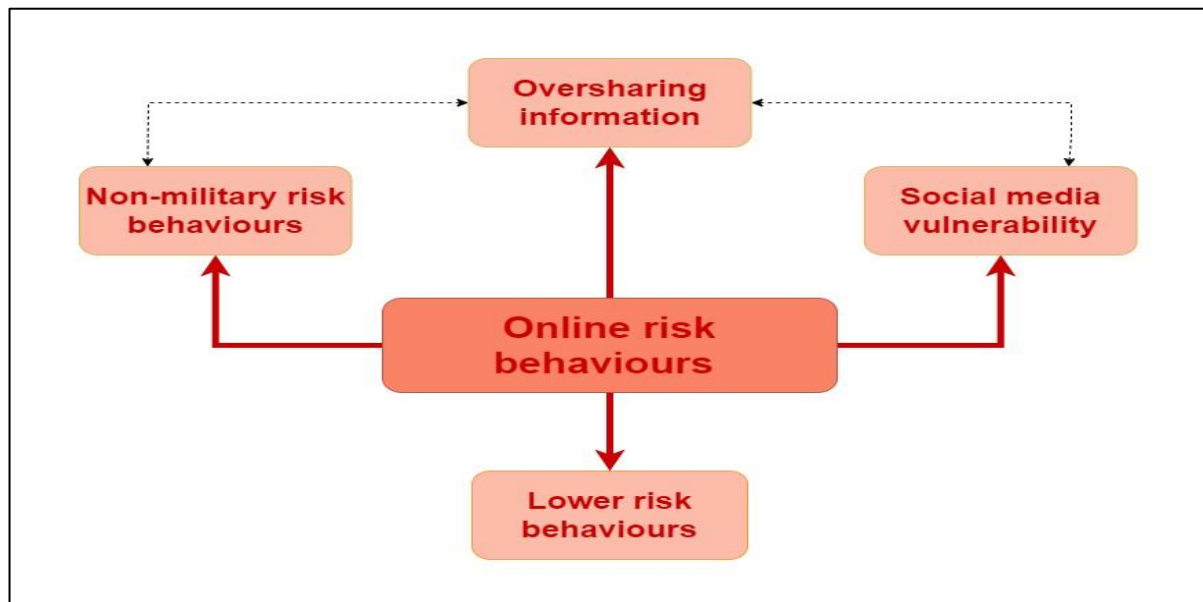
### 5.3.2. Main theme 2: Online risk behaviours

Theme 2, **Online risk behaviours**, discusses the online behaviours that Military Key Relations engage in that could present a vulnerability and consequent risk to military cyber resilience. Participants in the interviews were concerned about Key Relations oversharing information online, in sub-theme *Oversharing information*. This oversharing often happens on social media platforms, and the sub-theme *Social media vulnerability* discusses the risks associated with Key Relations' behaviours on social media. Some participants highlighted they were concerned about their Key Relations behaviours online creating risk not associated with the

military in sub-theme *Non-military risk behaviours* and they suggested Key Relations also exhibit behaviours that present a low cyber risk in *Lower risk behaviours*. Figure 4 visualises these sub-themes and the relationship between them.

**Figure 5.4:**

*Sub-themes for Theme 2, **Online risk behaviours**, and the relationship between them as indicated by dotted lines. Arrows indicate the direction of the relationship.*



When asked about their opinions on the online risk behaviours friends and relatives can engage in that presents a risk to military organisations, there was a large focus on online information sharing discussed in the sub-theme *Oversharing information*. Participants were concerned Key Relations behaviours creates more cyber risk for individuals inside and outside of the military, than necessary. Participants highlighted that Key Relations view information sharing as innocent, but the behaviour is risky as information can be aggregated by a military adversary to create pattern of life [P3]. Pattern of life is movement and behaviours of people, and movement of equipment such as vehicles, vessels and aircraft, that are consistent within an area of interest. Due to the potential a threat actor would be able to identify the location of people or equipment based on pattern of life, these online risk behaviours create a vulnerability for individuals to become the victim of a more sophisticated physical or cyber-attack. Whilst participants suggested the classification of information that Key Relations can share may not be sensitive, there is a potential risk to military cyber resilience through threat actors triangulating this information, “all the adversary needs is just the last bit of information in the puzzle” (P5). When suggesting examples of the type of information that an adversary could target to triangulate or create pattern of life participants mentioned location, timings, mention of weapons and information that details the movement of senior or very important people. Additionally, participants’ opinions were that personnel and Key Relations who share information about their security classification were more likely to be at risk from an individually targeted attack from an adversary. Adversaries may choose to target these individuals due to the perception they will have access to more detailed information, “policy driven not put classification on social media or job websites [...] that could be a target for threat actors for spear phishing” (P15).

A common vector for sharing this information online is social media. One participant highlighted the main concern for military cyber resilience is “people being crap on social media”



(P17), which is explored in sub-theme *Social media vulnerability*. Participants highlighted Key Relations' behaviour on social media makes them more vulnerable online and consequently increases the cyber risk for military organisations. Participants identified a variety of social media platforms that presented a risk including WhatsApp, Facebook, Instagram, Twitter, LinkedIn, BeReal and Snapchat. Much of the concern focuses on the lack of control people have over their pictures and videos once shared on social media platforms, "once it's out on WhatsApp, you've lost it" (P5). Whilst participants mentioned a variety of platforms that could present a risk for Key Relations sharing sensitive information online, research into oversharing on social media identified oversharing happened more on Facebook compared to other social media platforms including Instagram, Twitter and Snapchat (Brammer et al. 2022). Military personnel and SMEs in the current thesis considered how the risk of Key Relations posting military information online grows when social media profiles are made public. This risk is further increased when individuals share classified information in the public domain [P5], as "friends and relatives [...] having open social media profiles and posting movements of where they're based and going to visit can be quite detrimental" (P14). Key Relations may also present an increased risk to cyber resilience if they have open profiles on fitness tracking apps, such as Strava. Whilst participants frequently spoke about how personnel can be vulnerable to an attack if they openly share their running routes, this is something that ought to be raised to families who live on or near a military base, especially those residing outside the UK in locations where their use of a Western app may be more easily attributable [P14, P16]. Individuals with open or public social media profiles are also vulnerable to a targeted attack if threat actors are able to connect military personnel to their Key Relations, "the hostile threat actor might go onto your social media account [...] not actually target either of you but maybe 3 or 4 people down in your contacts list because that's the weak point" (P15). One example of this is the previous MI6 chief, John Sawers' wife having an open Facebook profile with easy to access information about their location, addresses, personal connections, and children. The risk of such a prominent individual's information being shared by a key relation into the public domain creates a physical risk for himself but also of his family of being kidnapped or assassinated (Boorman, 2012) or potentially becoming the victim of online blackmail.

This vulnerability also occurs for social media groups, such as Facebook groups designed for military spouses to provide support to one another. Vulnerability can occur for these groups when they are public as they could be infiltrated by an individual that wishes to gain military information. One participant highlighted this as a potential outcome if Key Relations social media groups are public, "even though there's no malicious intent there, there could be IP addresses [...] from countries that you wouldn't necessarily want" (P14). The role of perceived control could be influential in determining the extent individuals choose to share information within these groups. Perceived control exists when an individual believes they have control of a situation if they think they can predict it sufficiently to make a rational decision (Skinner, 1996). Hajli and Lin (2016) identified that individuals with a higher perceived control on social media networks, are more likely to share information on social media. If Military Key Relations perceive that social media groups are created with the purpose of offering support and guidance, they may be more likely to share sensitive or classified information within these groups. This can create a potential risk if group admins are not closely monitoring group access and the group is infiltrated by a threat actor. This vulnerability on social media can also be explained by the Privacy Paradox. This theory suggests individuals who are actively aware of the online risks on social media and how to mitigate against these risks, predict there is a low probability of these risks occurring for themselves, and so don't actively engage in online safety behaviours (Barth & De Jong, 2017).

Whilst the existing research into this mainly focuses on this paradox first-hand, the participants in the current thesis appear to make justifications for why their Key Relations' are less vulnerable. One example includes a key relation living remotely, "on his network as an example he can have no password as his house is in the middle of nowhere" (P9). If personnel perceive their Key Relations having a low online vulnerability, and thus the risk to themselves in their military role is lower, this may influence the extent they encourage their Key Relations' to apply online safety behaviours. The privacy paradox is closely linked to Optimism bias, which is explored further in sub-theme *Overconfidence and complacency*, in Theme 3.

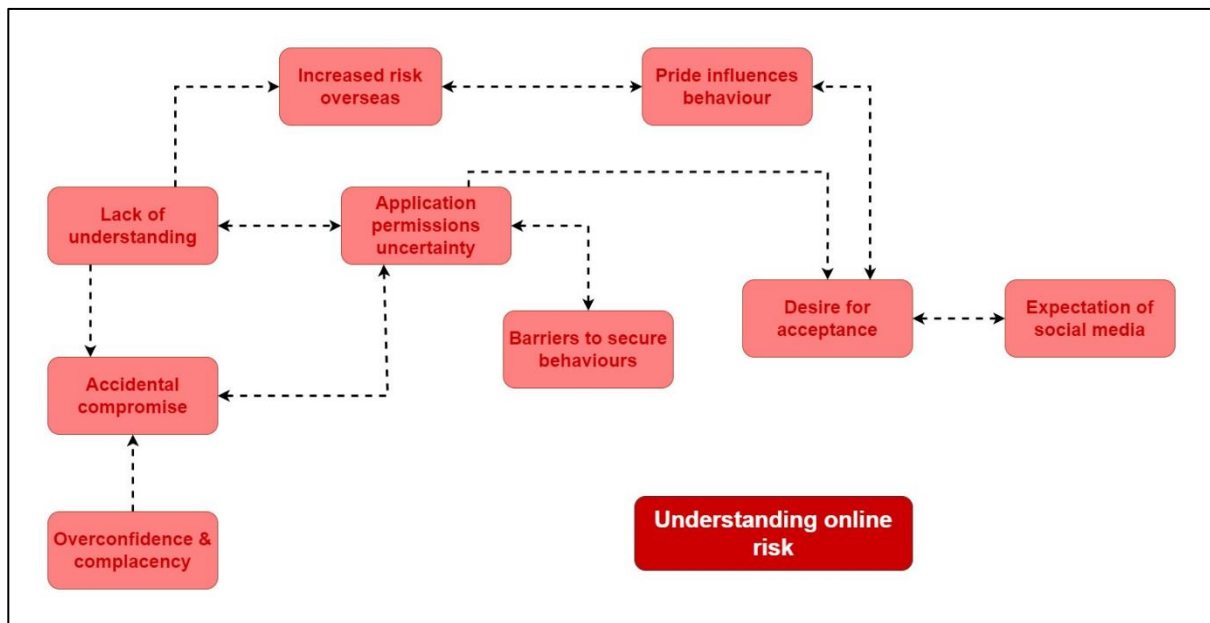
Participants conversely highlighted behaviours their Key Relations exhibit online that present less cyber risk, in the sub-theme *Lower risk behaviours*. Participants spoke about the older generation being less engaged with newer technology, including social media, which makes them less worried about their online safety. For example, one participant spoke about their lack of concern about their father-in-law due to him only using technology he understands and not getting involved with newer technology "well he's not getting into the new tech, so there's not the threats" (P9). However, there is the potential that participants identify lower risk for these Key Relations, without considering the possibility their Key Relations are vulnerable by not actively engaging in behaviours to protect themselves online. During the inter-coder reliability process, both researchers perceived some participants initially identifying their Key Relations as behaving in a way online that presents a low cyber risk and then contradicted themselves later by suggesting they were concerned about their Key Relations' online behaviour. This could have been because the behaviours they were concerned about do not directly relate to military cyber resilience, such as those discussed in sub-theme *Non-military risk behaviours*. This sub-theme highlights participants' concerns about online risk behaviours that Key Relations engage in that wouldn't directly influence military organisations but demonstrates they are potentially engaging in insecure online behaviours. These risk behaviours mainly focused on being a victim of a scam and losing their money. This behaviour can be applied to a military context as the attack format could be similar such as social engineering, but the outcome differs as the threat actor is attempting to reach the military person or seek military information rather than financial information. This sub-theme is closely linked to theme 4; **Individual Differences** as when participants were discussing their concerns about these risks, the Key Relations they were discussing were mainly from an older generation. Theme 4 discusses the role of generational differences in online behaviours and consequent online risk behaviours.

### 5.3.3. Main theme 3: Understanding online risk

Theme 3 is closely linked to theme 2, **Online risk behaviours**, as both focus on cyber risk for military organisations and how friends and relatives' online behaviours contribute to military cyber resilience. Whilst theme 2 focuses on the online behaviours that can present a cyber risk to military organisations, theme 3 explores the suggested reasoning and understanding participants mentioned during their interviews for Key Relations might choose to engage in these risky online behaviours. Sub-themes included as these suggested explanations include: *Expectation of social media*, *Desire for acceptance*, *Application permissions uncertainty*, *Barriers to secure behaviours*, *Accidental compromise*, *Lack of understanding*, *Overconfidence and complacency*, *Increased risk overseas* and *Pride influences behaviour*. Figure 5 depicts these sub-themes and the relationship between them.

**Figure 5.5:**

Sub-themes of Theme 3, **Understanding online risk**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.



One of the challenges for keeping personnel and Key Relations safe online that participants frequently mentioned is the pervasiveness of technology, and how it has changed throughout participants' careers. The use of technology within the military, especially when mobile phones are a necessity for most military operations (P17), makes it difficult to control when devices are used and what information is shared, meaning Key Relations may have access to real-time information. In the sub-theme *Expectation of social media* participants ruminated on the challenge of living in a society dependent on technology and the internet, and the requirements to share everything about our lives on social media, "otherwise it's not real or it doesn't exist" (P13). Participants spoke about a cultural shift of sharing information online and becoming more dependent on social media. One participant explained information about their children's hobbies and school trips are communicated via social media, and can be challenging to access without social media profiles, "it's all on Facebook so we had a right rigmorole to say right can you send it to us please, because we're not on Facebook" (P3). This culture of sharing information on social media could stem from the perceived benefit that occurs from sharing information about oneself on social media. Research suggests these benefits can include an improved relationship quality (Valkenburg & Peter, 2009), increased connection with others and reduced loneliness (Deters & Mehl, 2013) and increased social support (Haslam et al. 2017). The feeling of connectedness might be especially important for Military Key Relations as online communication has been found to mediate the negative effects that military families experience due to relocation (O'Neal et al. 2022) and frequent separation from their military person (Rea et al. 2015; Bittner, 2014).

This aspect of wanting to share our lives online is heightened when Key Relations overshare online due to seeking gratification from others, as highlighted in sub-theme *Desire for acceptance*. Participants stated that Key Relations may choose to post online if they desire social acceptance and gratification from others, and use information about themselves and their military person to their social benefit. This social acceptance may be sought in the form of a popularity contest online [P14] but also to benefit their military person's career, "their way of

climbing the social hierarchy is having that information and sharing it” (P9). Affect heuristics suggest that an individual engages in an online behaviour that violates the privacy of the information, if they perceive the behaviour as favourable. Behaviours that are viewed positively have a lower perceived amount of risk associated with engaging in this behaviour (Dincelli et al. 2017). An example of this is posting information on social media due to seeking a positive consequence, such as validation or acceptance from others. As chapter 1 discussed, it is important to distinguish between privacy and security behaviours, particularly as research has identified that there may be distinct explanations for these behaviours (Chassidim et al. 2020). Whilst affect heuristics are included as a potential explanation for making information privacy decisions, availability heuristics are potentially a more appropriate explanation for decisions about information security decisions, discussed further in Theme 7, **Military Culture**. It is important to understand the reasoning behind Key Relations’ decisions to post information on social media, to ensure any attempts at reducing this vulnerability through cybersecurity initiatives are relevant and effective.

Social norms may provide a suggested explanation for why individuals perceive that sharing information about themselves online may result in acceptance from others in society, with individuals attempting to balance disclosure of information with appearing likeable online (Spottswood & Hancock, 2017). Neubam et al. (2023) conducted cross-culture research into the effect of social norms of adopting privacy behaviours online in Germany and the US and found that social norms that were strong in encouraging privacy online were met with less positive attitudes. Whilst potentially due to the dislike of participant’s perception of being pressured to engage in privacy behaviours (Neubam et al. 2023), this finding has implications for recommendations of how to encourage Key Relations to protect their information online. If Key Relations feel pressure from military organisations to engage in secure online behaviours and alter their behaviour online drastically, it could have a detrimental effect rather than the intended positive influence on cyber resilience. In this thesis, participants mentioned that one way Key Relations may seek acceptance online is through sharing increasingly more information, due to social media becoming a “popularity contest” (P14) of likes, views and follower count. The level of information required to gain popularity is increasing over time as “You have to hit certain criterias to be accepted and have to do even more things to be accepted” (P9). In terms of Key Relations keeping themselves and their information safe online, there is a connection between individuals desiring social approval and having a public social media profile, and having a large number of social media followers leading to more positive emotions for those with a high need for approval (Sciara et al. 2023). One participant highlighted their concern that this risk will increase as careers in social media increase, “there’s so many careers you can get in social media now [...] but if that’s done in a base or accommodation then it could give identifiable information” (P14). This will make it more difficult for those with a career that requires them to share information about their life online, such as content creators and social media influencers, to balance privacy and security with career success.

This risk can increase further when individuals decide to post this information without considering how application settings can protect this information and keep it within an individual’s online circle rather than in the public domain. The sub-theme *Lack of consideration of app permissions* discusses how participants suggest the societal norm is to not consider permissions for applications (apps) and to automatically allow apps to default to the most public settings on social media accounts. Whilst participants highlighted individuals lack consideration of the risk of insecure security settings, one participant reinforced that anyone with a connection to the military should be even more considerate of their security settings, “if you download an

app or use a new platform you have to be so ruthless about finding out what the security settings are and how to minimise the risk” (P8). This is to ensure that not sensitive military information that could be used by a military adversary, is shared. This sub-theme, *Lack of consideration of app permissions*, is closely linked to sub-theme *Barriers to engaging in secure behaviours*, which discusses how the default settings of technological devices or communication platforms may create an indirect source of vulnerability for Key Relations. There is the potential that Key Relations may be unaware of their vulnerability to cyber risk due to the assumption that platforms and technology default to their most protective setting.

Some participants suggested device and platform functionality may hinder the ability to be secure online. This is because social media platforms benefit from difficult to find privacy settings as “they want as much exposure as possible” (P8), to ensure they are profitable companies. This is highlighted in sub-theme *Barriers to engaging in secure behaviours* and explored suggestions from participants for why even though Key Relations may understand that they should engage in secure online behaviours, there might be reasons this does not occur. There is an increased risk of using technological devices such as mobile phones and SIM (Subscriber Identity Module) cards. This technology is designed to help device networks function efficiently, rather than to protect the location of the users, including military personnel and their Key Relations when overseas [P17]. Functionality also becomes a barrier when secure online behaviours hinder Key Relations being able to communicate with their military person, and so individuals may revert to insecure behaviours down to the priority being communicating with their loved one. One participant was concerned Key Relations will revert to insecure methods of communication such as Whatsapp and Facebook if they cannot communicate with their military person, “hit and miss [communication] will push them to revert to [...] taking shortcuts and moaning and start posting on Facebook again rather than being secure” (P12). Participants explained that military personnel and their Key Relations are discouraged from using WhatsApp as a communication platform due to the security vulnerabilities of the platform and their over-reliance on WhatsApp’s advertised end-to-end encryption [P1, P12]. However, participants discussed that safer online behaviours and communication choices can only be implemented if Key Relations know that they exist and how to implement them, “that works if parents or the family know how to do that or are aware of it or even know what that would be for” (P12). The role of technological experience, knowledge and understanding of technology is important, as an individual with no other opportunity in their life to learn about cybersecurity, will not be able to apply these solutions. Therefore this sub-theme relates to the sub-theme *Non-military training*, in theme 5, **Existing Approaches**. This sub-theme provides additional justification for creating cybersecurity materials that provide Key Relations with information about online risks and secure online behaviours that can help them make smarter decisions to keep themselves and their military person safe online.

Often sensitive information is shared by Key Relations incidentally, such as not realising that sensitive information is in the background of a selfie or not understanding the importance of the information they are posting. The sub-theme *Accidental compromise* covers the idea that individuals may accidentally reveal something based on information their military person has told them without realising the magnitude of their behaviour. Participants highlighted that sometimes Key Relations might realise their error and regret posting, but the action is irreversible and the information cannot be retrieved, “I don’t think people always realise what is coming out of their mouths at the time [...] and then it’s kind of like oh shoot I shouldn’t have said that” (P6). For example, incidental information sharing may occur when Key Relations divulge military information shared to them by their military person, to prove their side of a debate is correct [P7,

P17]. Participants highlighted that Key Relations often have access to information provided by their military person about where they are or where they're going. Consequently the cyber vulnerability occurs due to Key Relations not realising the potential impact of their information sharing behaviour, for their military person. One participant described Key Relations as "a really influential audience and if we don't get that right they can leak just as much information as someone else can inadvertently" (P12). The sub-theme of *Accidental compromise* is closely related to the sub-theme *Lack of understanding* as Key Relations may accidentally reveal information due to a lack of understanding about technology and the associated risks. Participants suggested that Key Relations may lack the understanding of what technology exists such as the plethora of online communication platforms, and this influences their ability to use technology effectively. Additionally some participants highlighted that their Key Relations only focus on the positive influences of technology and the internet, without considering the potential dangers, "I don't think people are quite aware of the danger the internet poses, it's an amazing tool but it's also quite scary" (P14). Increased risk for military organisations due to Key Relations behaviours could be due to limited understanding about the security of end-to-end encryption on Whatsapp [P1], not understanding that information online can be accessed by anyone [P7], and that friend requests may not be legitimate [P17].

Conversely, participants may have the understanding of technology and the associated risks but have an overconfidence their behaviour only presents a small amount of risk that does not affect their military person. This is explored in sub-theme *Overconfidence and complacency*, where participants identified that information oversharing online may be due to Key Relations relying on their behaviour being a one-off, or a threat actor not paying attention to their online behaviour. This overconfidence and choice to not behave securely increases the online risk to cyber resilience for military organisations as it provides threat actors the opportunity to aggregate small amounts of information. This provides an opportunity for a threat actor to create a big picture about operational information and providing sufficient evidence to act on this information, "piecing together bits of information that friends or relatives are posting that is innocuous could accumulatively be less than innocuous" (P4). This behaviour can be explained through optimism bias, which suggests that even when individuals are aware of the risks of engaging in certain online behaviours, an error in judgement makes people perceive they are less likely to be the victim of a cyber attack. Therefore, they do not prioritise safe online behaviours, and make themselves more vulnerable online (Alnifie & Kim, 2023). However, one participant highlighted that Key Relations behave in this way to achieve security through obscurity, "there's so much information out there that you could sort of hang out in the background and not be detected" (P3). Stutzman and Hartzog (2012) describe how this move to obscure information, where one or multiple key elements are removed from online information to limit comprehension of the information. Security through obscurity has been considered a solution for more practical interactions on social media and to address the lack of consumer demand for the current approach where social media networks are designed with privacy of data as the priority (Rubinstein, 2011). However, the risk for military organisations occurs when multiple Key Relations only remove one or two identifying elements from their online posts about a military event that when aggregated can provide a sufficient level of information detail for an adversary to act upon.

Whilst some of these considerations are not specific to Military Key Relations, there are suggested reasons unique to the military community for why Key Relations might choose to engage insecure online behaviours. One of these that participants discussed was the increased risk of Key Relations sharing information online about their military person when personnel are

deployed overseas, in sub-theme *Increased cyber risk overseas*. The opportunity for Military Key Relations to share sensitive information online increases when their military person is overseas because they have access to more detailed location and timing information that would be of interest to an adversary [P7]. This information is also more interesting for Key Relations than when personnel are at home “when I’m at home, it’s boring, I’m not doing much” (P6). This increased interest of information results in personnel providing their Key Relations with more information as personnel are more likely to want to share aspects of their day with their Key Relations than they would do at home, “a lot of people stationed overseas want to update family and friends about what they’ve been doing” (P14). It is common in society for family and friends to discuss aspects of their day with each other. However, the unique aspect of military operation details being classified, and the requirement to communicate updates over social media when situated away from their loved ones, increases the risk from being overseas for Key Relations having access to information that could present a risk to military cyber resilience.

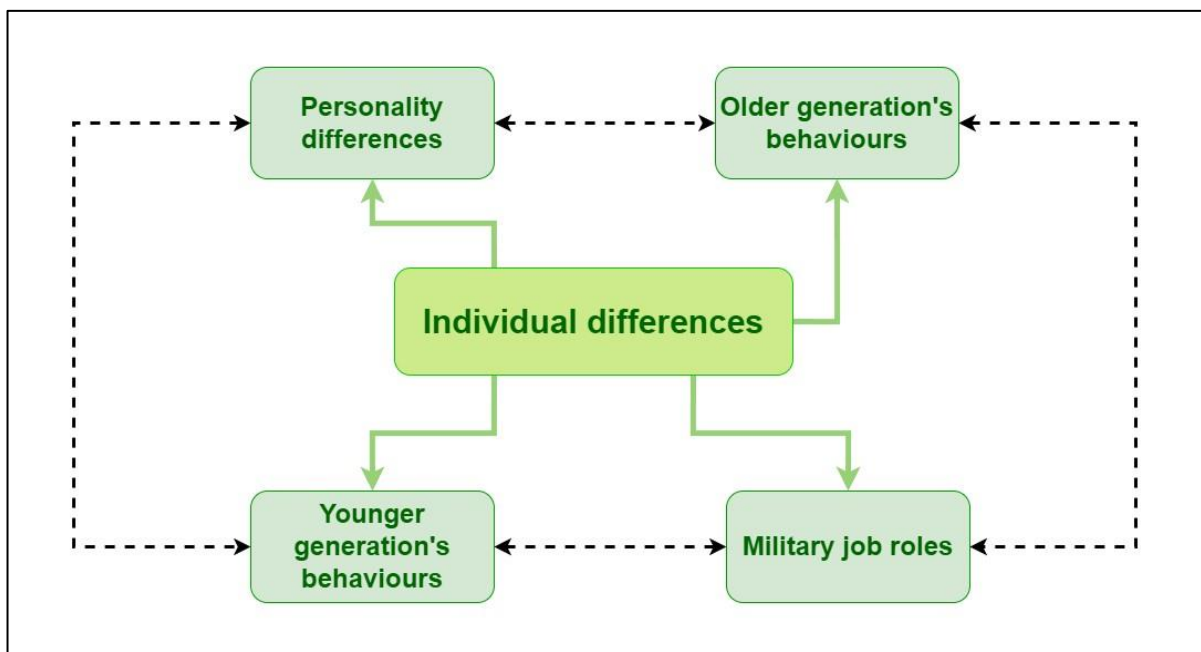
An additional suggestion unique to the military community for why Key Relations undertake insecure online behaviours is the role of pride in encouraging information sharing, “people feel very proud if they have children or spouses who serve in the military and so they might post something” (P10). The sub-theme *Pride influences online behaviour* focuses on participants’ experiences of Key Relations oversharing information online about personnel due to wanting to share their pride with their own social group. Pride is an egoistical emotion associated with self-control and that people experience when viewing their personal behaviours and achievements positively (Baek & Yoon, 2022). Key Relations may experience pride following their Key Relations’ success, particularly parents who may feel they had a role in preparing their child for life, “Mums and dads are so proud of their kids, they’ll be wanting to tell everyone what they’re up to” (P5). Pride over friends and relatives job role is not something that is unique for a military community, but the risk that comes with sharing the extent of an individual’s role within the military presents a unique risk due to the potential of becoming a target for a military adversary. Research exploring the role of pride in human behaviour identified that people who had experience pride were more likely to engage in indulgent behaviours such as a more indulgent food choice or frivolous expense choice (Wilcox et al. 2011). Hofstede (2011) identified indulgence versus restraint as a dimension of national culture, which plays a role in influencing national and societal behaviour. An indulgent society values human happiness, well-being and freedom and is common in Western societies. Comparatively, restraint societies such as in Asia and Eastern Europe value strict social norms (Hofstede, 2011). Zhang and Yang (2018) suggest that societies with an indulgence culture are less likely to consider information security issues, and are less likely comply with cybersecurity requirements if it involves restraining their behaviour. Potentially Key Relations who experience pride and may be more likely to engage in indulgent behaviours associated with riskier cybersecurity behaviours and less consideration of cybersecurity policy. Future cybersecurity initiatives with Military Key Relations should consider how Key Relations can show their pride for their military person and share that pride with others, in a way that keeps themselves and their military person safe online. All these sub-themes guide recommendations for cybersecurity education and awareness materials for Military Key Relations, as participants stressed the requirement of educating Key Relations on the importance of securing the information they have access to. Suggestions for how this should be done is explored further in Theme 6, **Cybersecurity materials recommendations**.

### 5.3.4. Main theme 4: Individual differences

When discussing key relation's online risk behaviours there were multiple individual differences that participants mentioned that they believe influence Key Relations' online behaviour and consequent cyber risk for themselves and military organisations. The main differences that participants highlighted was how different aged Key Relations behaved contrarily, with the younger generation and older generations presenting the most amount of risk, in sub-themes *Younger generation's behaviours* and *Older generation's behaviours*. Additionally participants mentioned the role of personality in online behaviour in sub-theme *Personality differences* and how personnel's job roles can influence their Key Relations' behaviours in *Military job roles*. Figure 5.6 visualises these sub-themes in a thematic map, and the relationship between them.

**Figure 5.6:**

*Sub-themes of Theme 4, **Individual differences**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.*



The first sub-theme *Younger generation's behaviours* highlights the online risk presented by younger Key Relations due to their vast and constant use of online communications platforms. This online behaviour is the norm for their generation, when compared with older generations (Ofcom, 2022). Whilst there was no clear definition of what participants meant by younger generations, the Key Relations spoken about were children, siblings and nieces and nephews. Participants discussed how it is natural for young people to want to voice their opinions, but the risk comes when this is across a plethora of platforms, and when it is information about their military person, "they've got social media platforms across the board [...] they have an opinion and they voice that opinion immediately" (P16). Participants had contradictory opinions about the role of age in online vulnerability. Some participants claimed the younger generation is less considerate of the risk when communicating online, "that generation I don't think they'd even double take to what they're posting or putting on" (P6). Whereas others claimed that younger generations are much more understanding of technology, the risks and how to mitigate against them due to the prevalence of technology throughout their lives, "brothers and sisters [...] have grown up around this sort of thing and are switched on but my mum and dad probably not" [P13].



When directing any future cyber initiatives to these Key Relations it is important to consider their experience with technology is vastly different when compared to older generations due to having grown up with access to the internet including widely available access to the internet during school.

Additionally, younger Key Relations may be less vulnerable on social media compared to the older generation as they prefer “closed community social media” (P4), compared to public facing social medias where they publicise their life. Again participants had contradictory opinions with some suggesting that the desire for younger generations to seek approval from others makes them vulnerable online, “the younger ones want instant access and gratification” (P16). Whilst this may vary from individual to individual, one participant discussed their concern about their children sharing information about their military role because “as a teenager it’s quite easy to be influenced” (P8). This potential to be influenced may result in Key Relations innocently sharing information that was discussed with the service person and the family. Vijayakumar and Pfeifer (2020) explain how information disclosure is a key part of adolescents social development. Self-disclosure helps build relationships with peers so that young people can move away from relying on their parents to receive more support from peers (Vijayakumar & Pfeifer, 2020). By disclosing information about themselves, young people can receive feedback from their peers which provides them with validation for their feelings thoughts and behaviours (Davis, 2012). This validation of emotions could be an even higher necessity for young Key Relations of serving personnel, as children experience a wide array of emotions related to the service person’s job. Fitzsimons and Krause-Parello (2009) Emotional Stages of Deployment Model describes this emotional cycle from a military child’s perspective throughout the Phases of deployment. The model begins with worry before their parent deploys, sadness and loneliness during deployment and then an increase in positive emotions when their parent is returning home. Sharing feelings and thoughts with others may provide Key Relations the validation required for their emotions but also the opportunity to develop close relationships that can offer additional support mediating the negative effects experienced due to their military person’s deployment (Meadows et al. 2017). However, the work on the psychological and developmental effects of deployment on children mostly explores the experiences of service children and so this effect might be different for young siblings, or nieces or nephews where the relationship dynamics might differ.

The existing research on the influence of age for engaging in cybersecurity best practice is inconsistent but reflects that different generations may engage in security behaviours in diverse ways. When discussing the sub-theme *Older generation’s behaviours*, participants’ main concerns are that older generations don’t keep up with the evolution of technology, and their use of social media is driven by their desire to communicate with their loved ones. For some in the older generation the deployment of their military person necessitates communicating online using new platforms they are not familiar with. This presents an additional risk to themselves but also their military person due to their previous lack of experience with technology [P8] and resistance to technology [P2]. This resistance to technology may stem from a lack of confidence. Research suggests the older population can lack confidence in online environments, sometimes unjustifiably, which influences their engagement with the internet both to make the most of the benefits, and to engage in safe behaviours online (Morrison et al. 2021). Research into how to engage the older population about digital literacy, online safety and how to improve their confidence online, found that participants benefited most from was learning about online safety and prevention. This involved explaining the benefits of using the internet, the online risks to be aware of, how to engage safely online, and their presence on the web (Zanchetta et al. 2022).

Older individuals found this education the most relevant for themselves when compared to information about society online and the benefits of using the internet for education were highlighted. Individuals also reported that having this initial insight into online risk and safety motivated them to learn more.

It is important to respect that individuals who are older have previous life knowledge and experience, even if their experience is not in technology. Incorporating older people's existing knowledge is important when helping them understand the progression of technology and applying new online skills to protect themselves and their military person online, "it's a fine line between telling the older generation we understand you've been around a long time, but it's making them understand the evolution and modernisation of everything" (P8). For example, when exploring password behaviours, Merdenyan and Petrie (2018) found that the older participants were more likely to write their passwords on paper to remember them, when compared to younger participants. Writing passwords down physically can encourage older participants to use stronger and more secure passwords as they don't need to memorise complex passwords. This unburdening of the mental capacity of password storage also helps the older generation use different passwords for different platforms. However, the importance of storing these passwords safely away from their devices should be highlighted (National Cybersecurity Centre, 2020). Accounting for generational differences encourages individuals to engage with secure behaviours but allows for materials to respect older generations knowledge levels and experience that may otherwise hinder engagement. The researcher reflects that whilst participants were not asked to provide their age, based on participants' career and life experiences, most participants would fall into the 30 – 60 years old age bracket. This places them outside of the generations they highlighted as presenting the most risk, which they identified as their parents, or in-laws. One participant early in their career mentioned their parents and their grandparents as exhibiting different online behaviours. Their mum posts a lot of information on Facebook to friends "on Facebook it reaches a larger audience for her" (P6), but grandparents preferring to share information offline due to their lack of trust in technology "grandparents I find that they are the most security wise people ever, they don't trust anything" [P6].

Participants discussed additional individual differences that potentially influence Key Relations online behaviour that interplay with generational difference to influence risk. The sub-theme *Personality differences* reflects participants experiences with their Key Relations personality types and their online behaviours. Some Key Relations appear naturally more inclined to be considerate of risk in all aspects of life, which is reflected in their online behaviours. For example one participant spoke about their wife being "tech savvy" (P9) and suggests this could be due to her job role in tech but explained prior to that role she was risk averse, suggesting being conscientious of risk is more of an aspect of her personality. This participant also suggested that personality may be the reason their father struggles with using technology as their father's previous experience in a hands-on career suited his personality, and he consequently finds the internet frustrating as it is not an easy physical fix [P9]. When exploring personality and the role it has in engagement with cybersecurity practices and behaviours, a lot of the research focuses on the widely used personality construct, the 'Big Five' (Cattell, 1956). There are suggestions that aspects of personality from the Big 5 can predict cybersecurity behaviours. Shappie et al. (2019) identified that high scores in personality constructs Conscientiousness, Openness and Agreeableness were positively related to self-report cybersecurity behaviours. These behaviours included using different passwords, backing up files and regularly updating anti-virus (Anwar et al. 2017). However, Shappie et al. (2019) used a participant group of college students and Berner et al. (2011) suggests that individual age and education play a more

significant role in predicting online behaviours than personality. When considering the findings supporting individual differences in the current thesis, the role of personality seems less important than age. This is an important consideration for the approach to any future cybersecurity initiatives for Military Key Relations as any education or training needs to be accessible by everyone regardless of their mindset, previous experience, and education level. When discussing existing approaches for military personnel's cybersecurity training, one participant highlighted the benefit of hands-on training such as cybersecurity themed escape rooms and board games, "we have an escape room [...] that's a really good tool [...] anything that gets people away from click through training or emails" (P14). These approaches can encourage people to physically engage more than online training or reading a pamphlet or magazine. Further recommendations for how to engage Military Key Relations in future cybersecurity initiatives are discussed in Theme 6, **Training and Education Recommendations**.

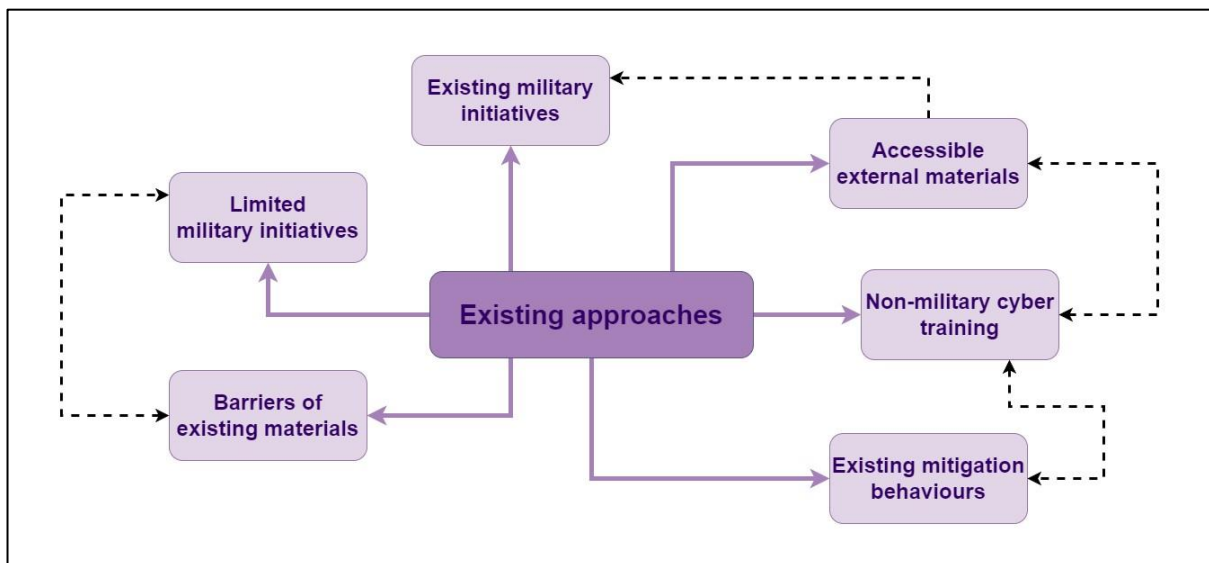
When identifying Military Key Relations' online risk, the influence of their military person's job role should be considered as not all Key Relations experience the same level of online threat, "the threat is certainly not uniform to all friends and family" (P17). Sub-theme *Military job roles* reflects how Key Relations of military personnel that are higher in command or commissioned to more specialised units are a more attractive target to a military adversary due to their potential access to more detailed information. There is the potential that Key Relations of individuals in these roles are already more aware than other Key Relations about the requirements for online safety behaviours due to the military person communicating requirements. Participant 6 spoke about a friend who is much more aware of the requirements of posting about their parent online due to them being in a high-risk military role. However, Key Relations receive much less cybersecurity training, education and awareness than military personnel as identified in theme 5, **Existing Approaches**. This reduced access to cybersecurity materials can make Key Relations an easier online target for adversaries. Consequently, this highlights the importance of providing Key Relations with cybersecurity materials to ensure the potential risk their online behaviours present to military cyber resilience is reduced.

### 5.3.5. Main theme 5: Existing approaches

To understand the existing approach from military organisations for Key Relations' cybersecurity, participants discussed their understanding of the current cybersecurity training, education or awareness initiatives for Key Relations. There was a mixed response with some identifying they were not aware of any cybersecurity materials for Key Relations, in the sub-theme *Limited military initiatives*. Others suggested Key Relations can access cybersecurity information through outreach days in sub-theme *Existing military initiatives*. This theme also discusses the alternative methods Key Relations learn about cybersecurity such as through their job or education in sub-theme *Non-military cyber training*, or through external organisations in *Accessible external materials*. The potential reasons why Key Relations may not be able to access or apply cyber materials are discussed in sub-theme *Barriers of existing materials*. Finally, this theme explores the behaviours personnel and Key Relations apply to keep them safe online in *Existing mitigation behaviours*. These sub-themes and their relationships are visualised in Figure 5.7.

**Figure 5.7:**

Sub-themes of Theme 5, **Existing approaches**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.



In sub-theme *Existing military initiatives* many participants highlighted that they did not have any knowledge of existing cybersecurity training, education or awareness materials specifically for Military Key Relations. One SME suggested there may be cybersecurity materials that exist for Military Key Relations that they are unaware of, but lacked confidence in the certainty that these materials exist, “I expect if you went on certain family facing portals there will be stuff that you can do” (P3). Participants explained that often Key Relations who reside on military bases with their military person may learn about cybersecurity behaviours and threats through messaging posted around the base, “we do advertise good personal security in military locations as well, which indirectly friends and family will come across” (P16). The same participant then reflected that this indirect messaging is only effective if Key Relations stop to read the information and have sufficient knowledge to understand and apply the information. Often the approach from military organisations is to rely on military personnel to relay relevant information learnt during their own cybersecurity training and education to their Key Relations. One participant discussed how sometimes personnel are provided with examples of the impact of Key Relations’ online behaviours on military cyber resilience to encourage personnel to communicate requirements to their Key Relations, “we have deliberately put in examples of friends and relatives doing things [...] in the hope they’d take that home and educate their friends and family” (P17). However, this also relies on personnel understanding who a Key Relation is. If personnel perceive their sphere of Key Relations as being narrower or different than the reality, then this information could be passed along to the incorrect people. Participants suggested that the reason cybersecurity materials and initiatives don’t currently exist for Key Relations is because even though military organisations recognise it as being important, it is less of a priority than cybersecurity materials for personnel, “nothing is not important in the security domain but there’s a level and degree of importance” (P15). There can be a challenge with directing resources across the entire extended military community due to insufficient resources, “we haven’t got enough people to do this” (P5). In this way, this sub-theme *Existing military initiatives*, is linked to the sub-theme *Barriers of existing materials*.

The sub-theme *Barriers of existing materials* highlights how resource limitations, and a priority of training military personnel reduces the opportunity for military organisations to provide Key Relations with cybersecurity materials. One participant spoke about how previously an external organisation helped provide engaging cybersecurity materials for Key Relations, but no longer exists due to resource restraints, “due to budget cuts during covid the annual contract went but they used to provide us [...] with monthly campaigns focussed for friends and families” (P12). The benefit of having an external organisation provide cybersecurity materials rather than military organisations is that Key Relations are able to access information without relying on their military person. Cybersecurity materials for personnel that could be distributed to Key Relations at a low classification is distributed on the Ministry of Defence’s internal network that requires an email domain associated with defence personnel, “so much messaging that goes out across defence just goes out to people with a MODNET device [...] it’s very difficult to get that message out there to family and friends that don’t have a MODNET device” (P14). The importance of accessibility in any future cybersecurity materials and initiatives for Key Relations is discussed further in Theme 6, **Training and Education Recommendations**.

Contrastingly, other participants highlighted they were aware of some existing ways of engaging with Key Relations about their online behaviour in relation to military organisations in the sub-theme *Existing military initiatives*. Existing engagement with Key Relations focuses on in-person events that civilians attend. For example, airshow events provide the opportunity for initial contact with Key Relations, and then encourage them to engage with future cybersecurity materials, “from having the conversations we can gauge where people are confident and where there are gaps in their knowledge” (P11). When discussing the format of the cybersecurity materials for Key Relations, participants explained how materials are tailored to the audience. Civilian briefs focus more on generic cyber hygiene behaviours such as secure passwords and locking down accounts [P11] and reducing the classification of the cyber threats discussed compared to what military personnel receive [P15]. The aim of these briefs is to encourage Key Relations to protect their own information online. By protecting their own information, this consequently protects their military person, without distilling fear or providing Key Relations with classified threat information they might inadvertently share, “on the civilian side we dial that down because we don’t want to put the fear of God into them” (P15). It is worthwhile to note that the participants who were aware of existing ways that military organisations engage with Key Relations about their cybersecurity were all subject matter experts, and so they are more likely to have an increased awareness about these materials due to their job requirements.

Two participants [P11, P12] highlighted a previous contract with Get Safe Online, an online website providing resources about cybersecurity in an accessible and factual manner (Get Safe Online, 2024). This provided materials specifically for military friends and relatives that they could access themselves, “one of the things we had with Get Safe Online was an outwardly facing webpage which meant dependents were able to access it as well” (P11). Whilst participants suggested there was currently no direct contract between Get Safe Online and military organisations to provide materials for Key Relations, multiple participants still highlighted the organisation as a useful resource tool for Key Relations in sub-theme *Accessible external materials*. This sub-theme delineates that whilst some participants were not aware of military provided cybersecurity materials or initiatives for Key Relations, they were aware of external organisations dedicated to protecting individuals online that they would direct their friends and relatives to. Get Safe Online was recommended for Key Relations due to being colourful and using animations [P13] as a good starting point, as they have existing information about online threats and protective online behaviours, “friends and family and can go and look

at their information leaflets on things like email phishing” (P10). The National Cybersecurity Centre (NCSC) was also suggested by multiple participants as being a useful resource for friends and families. One participant indicated NCSC would be their starting point when directing their Key Relations to cybersecurity materials due to them being accessible for individuals with a range of knowledge, “they’re worded in which way anyone can understand them right up to having a technical level of interest” (P13). The Ministry of Defence Cyber Confident team was highlighted as producing easy, digestible and eye-catching cybersecurity content [P14]. Whilst the discussion about the team responsible for the Cyber Confident Campaign mainly focussed on the content provided for military personnel, it is possible for Key Relations to access some of their materials. For example, the Cyber Sound Bytes podcast is available on public streaming platforms, which provides an overview of secure online behaviours and current cyber threats, with a focus on military personnel and their friends and relatives. Additionally in sub-theme *Non-military cyber training* participants highlighted that some Key Relations already receive cybersecurity training, education and awareness materials either in a professional capacity or at school. One participant commented that the cybersecurity training provided in schools may actually be more in-depth than what is provided for military personnel, “I can imagine a scenario where the parent has been told something about password security and goes home to tell the child and the child rolls their eyes and they already have a password manager downloaded” (P13). This reliance on cybersecurity training in education is important as generational differences in technological may limit both military personnel and civilian parents from educating their children on secure cyber behaviours due to not having that knowledge themselves. Especially as the findings from this theme, **Existing approaches**, highlights the reliance of personnel to educate their Key Relations about their online behaviour can affect the military person and military cyber resilience. Additionally, another avenue for older participants is learning about online risks, such as scams through word of mouth by talking to friends, as well as media outlets such as newspapers and television, “it’s osmosis nowadays isn’t it and just talking to their friends and through the news and things like that” (P3). This sub-theme links to theme 4, **Individual Differences**, as when addressing Key Relations contribution to cyber resilience, different experiences with cybersecurity materials and messaging can influence their knowledge levels and consequently their ability to engage with secure online behaviours. This should be considered when creating recommendations for future ways military organisations engage with Key Relations about their online safety behaviours, as materials should be accessible and engaging regardless of existing knowledge levels.

Sub-theme *Existing mitigation behaviours* explores how military personnel and their Key Relations have established rules for their technology and online behaviours to keep their information safe. Participants were asked for their opinion on physical cyber risks concerning Key Relations, such as vulnerabilities that might arise from sharing devices or networks. Most highlighted that there is little risk to military organisations from these behaviours as long as cybersecurity policy for remote working is followed, “I think that’s relatively low risk as long as you follow the policy on not doing work off work IT” (P7). Virtual Private Networks (VPNs) are a requirement for MOD issued devices [P3, P7, P16] and these devices should only be used for work purposes and not used by friends or relatives [P14]. When discussing these responses it is of note to highlight that participants were invited to participate by a gatekeeper providing an overview of the research. This means participants who displayed an interest might naturally be more interested in cybersecurity and more engaged with their role outside of the day-to-day requirements. Therefore, these results and the suggestion that remote working policies are followed might not be consistent for personnel across the forces. One participant noted

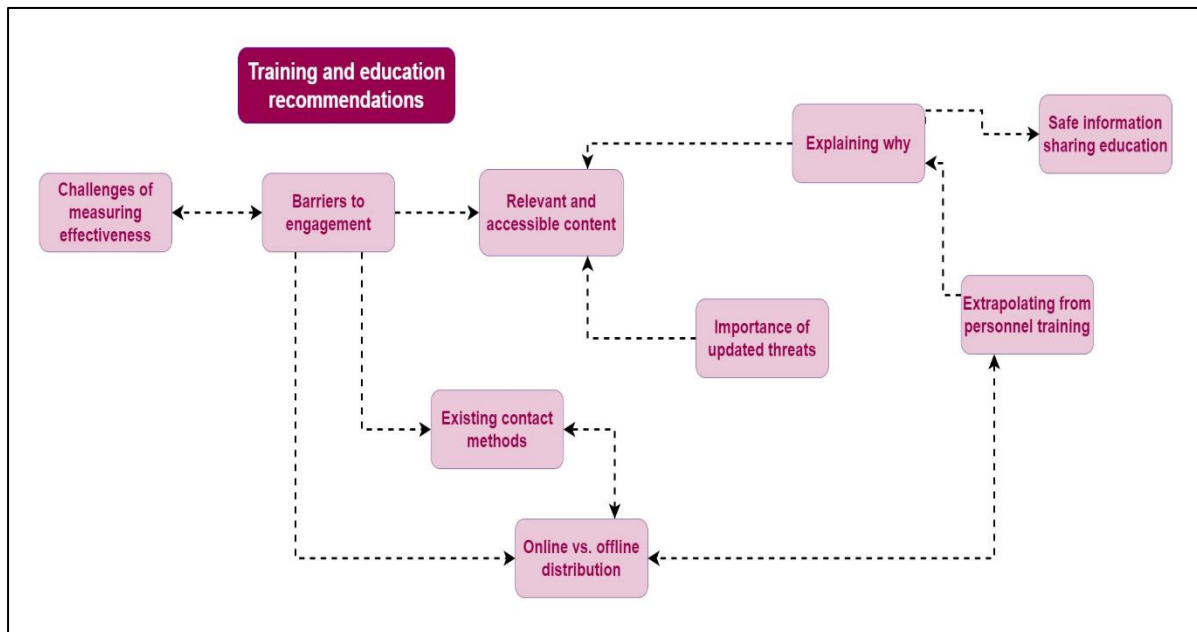
examples they were aware of where children of personnel had accessed work devices and joined meetings or messaged colleagues. There was concern this might increase as parents increasingly rely on technology to keep children occupied, “it will become an increasing risk as we become more dependent on technology that [...] people will share their IT with friends and family” (P14). Nikken (2019) identified that the use of technology to occupy or distract children can occur for a range of reasons, but factors can include parents that lack support and experience depressive symptoms. This is relevant for the military population due to many military personnel and their families experiencing more symptoms of mental illness than the general population (Gribble et al. 2019). Therefore, it should be a consideration that whilst military personnel can physically mitigate against cyber risks of sharing devices and networks, educating Key Relations on the cyber risks may further reduce the undesirable impact on military cyber resilience. This recommendation is relevant for other potential vulnerabilities occurring due to Key Relations’ online behaviour, such as information sharing online. One participant explained that to mitigate against this risk of information sharing from Key Relations, they limit the amount of information shared with Key Relations, “if I think it’s of a sensitive nature then I won’t tell them, I’ll just tell them I’m going away” (P8). This is possible for some Key Relations, such as extended family and friends. However, this becomes more challenging when family requires information about departure and arrival dates to manage family life such as childcare (Smith, 2015). One participant highlighted it is particularly difficult to obfuscate information to their spouse, “it’s almost unavoidable to talk to your spouse about all of these things” (P17). Theme 6, **Training and education recommendations**, builds upon the opinions discussed in this theme to provide recommendations for how future cybersecurity initiatives could be more effective at addressing Key Relations’ online vulnerabilities and reducing the risk to military cyber resilience.

### 5.3.6. Main theme 6: Training and education recommendations

As part of the interview questions participants were asked to provide their opinion on what cybersecurity materials could be provided for Key Relations of military personnel that can improve on the current approach. This theme, **Training and education recommendations**, provides an initial insight into how military organisations should create future cybersecurity materials for Key Relations, to ensure that Key Relations are engaging with any future initiatives. Participants provide suggestions for making cybersecurity material content accessible and appropriate for the extended military community in sub-theme *Relevant and accessible content*. Recommendations address concerns highlighted in previous themes in sub-themes *Safe information sharing education*, *Explaining why* and *Importance of updated threats*. Suggestions for how to deliver the materials are explored in sub-themes *Extrapolating from personnel training*, *Existing contact methods* and *Online vs. offline distribution*. Lastly, the theme discusses how to tackle potential challenges with future materials and initiative in sub-themes *Challenges of measuring effectiveness* and *Barriers to engagement*. Figure 5.8 depicts the directional relationship between these sub-themes.

**Figure 5.8:**

Sub-themes of Theme 6, **Training and education recommendations**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.



Theme 3, **Understanding online risk**, explored a lack of understanding from Key Relations may be vulnerable online. The theme addressed a lack of understanding about a variety of factors including how important their online information is to an adversary, the existing online risks, and how to apply online security behaviours that can protect themselves and their military person. This lack of understanding increases Key Relations’ vulnerability to a military adversary and increases the cyber risk for military organisations. When offering ways to decrease this vulnerability participants highlighted that an approach of enforcing individuals to not use social media is not realistic, “it is unrealistic to say don’t ever use it, however I think it is realistic to say be careful of what you put on there” (P1) as the progress of technology cannot be stopped [P11]. Therefore many participants suggested a method of reducing this vulnerability is to provide Key Relations with a basic education in cybersecurity, particularly in how to post online safely. This recommendation from participants is discussed in sub-theme *Safe information sharing education*. Participants highlighted that sometimes Key Relations are unaware of exactly what they can and can’t post about their military person online, and so providing them with this information clearly would be useful to reduce the chance of them making a mistake. However, Key Relations should also be educated on how they can still post online about their military person without posting information that is not allowed, such as having private and locked down profiles, and being vague with their information, “Don’t put on Facebook the exact dates I’m going home [...] make a Facebook post that counted down in weeks rather than days” (P7). By educating Key Relations about what information is safe to post online about their military person, this allows Key Relations to approach information sharing online with more consideration. Participant 15 suggested that when educating Key Relations about information sharing online they should be encouraged to consider the content of what they’re posting and whether it is necessary to share it online before they actually share it, which was reiterated by another participant “what we really want is for them to be very mindful of what they post” (P16).



Participants emphasised that if you want Key Relations to engage in secure online behaviours it is not sufficient in most cases to simply explain what online behaviours can present risk and how Key Relations can protect themselves online. Multiple participants reiterated that cybersecurity training, education and awareness materials should explain the reason why these behaviours are so important, in sub-theme *Explaining why*. Personal motivation has been suggested as an influential consideration for encouraging individuals to engage with secure online behaviours particularly if it aligns with their affective characteristics (Bada et al. 2015). For Military Key Relations, they are concerned with their military person's physical and mental wellbeing. Interview responses suggested framing why it is important for Key Relations to engage in cyber secure behaviours in the context of their military person is better than in the context of the Ministry of Defence [P15]. By framing the explanation in a way that aligns with Key Relations' main concern, the safety of their loved one, this may motivate Key Relations to engage with cybersecurity materials. One participant suggested that framing cyber risk in the context of why there is a risk to them as an individual military person may help mitigate risk behaviours displayed by their Key Relations "Explaining what the risk is to me by them posting something maybe photographs [...] explaining what the dangers are and the risks" (P12). However, there may be a generational difference in the necessity of explaining the underlying reasoning to engage in a secure behaviour. It was suggested that whilst the younger generations are less likely to adhere to cyber safety behaviours without knowing why, their parents would be happy with being told what to do to keep themselves safe without being told why, "she [Mum] probably wouldn't care she'd be like I don't understand, I just need to know what not to do and why isn't important to me" (P2). The participant suggested their reasoning for this opinion is because due to a lack of understanding their mother would lose interest a lot quicker. They did also comment on the human nature of wanting to know why, and how this differed for their child "my 4-year-old now is probably the best example of this, if you ask him to do anything he wants to know why" (P2). However, this is a perceived opinion of the participant's Key Relations and how they might potentially approach this information. Gathering perspectives from Key Relations themselves in Phase 3 of the research is important in determining the extent this would be true and is discussed in Chapter 5.

Explaining the reasoning behind engaging in secure online behaviours is something that was highlighted as beneficial when discussing military personnel's cybersecurity, and so could be beneficial for Key Relations also. The sub-theme *Extrapolating from personnel training* discusses points participants described as being successful in cyber training, education and awareness for military personnel that they believe could be beneficial for Key Relations. One recommendation was the use of gamification for cybersecurity messaging. Whilst opinions from participants towards gamification was mixed, when discussing the reception of gamification in cybersecurity from military personnel the consensus was that it has been beneficial in engaging everyone, regardless of their knowledge level, "it's a fairly low-level exercise where everyone can chip in and discuss so that's one way we've got around briefings being monotonous" (P13). An additional point from participants that has been beneficial with military personnel and could be extrapolated for Key Relations is the importance of making cybersecurity materials relevant to encourage engagement.

Participants recommended that cybersecurity materials should be relatable and easy to access for all Key Relations, regardless of their age, motivation or education level, to ensure all Key Relations engage with any future cybersecurity initiatives. The responses from participants about this relatability and accessibility is discussed in sub-theme *Relevant and accessible content*. Relevance explores how cybersecurity materials should explain specific risks and

threats for friends and relatives of military personnel. Accessibility focuses on the importance of not just the physical ability of individuals being able to access the information but also that everyone is able to understand and apply concepts regardless of their knowledge levels and ability. As explored in theme 4, **Individual differences**, the role of age, educational abilities and previous experience is influential in predicting online vulnerability and risk of Key Relations. Therefore, these factors should also be considered when creating cybersecurity materials that can be accessed by all Key Relations. One participant highlighted the importance of cybersecurity materials for Key Relations being broad and generic to encourage accessibility, especially when considering the age that children start using the internet for communication, “if people have children 8/9/10 years old just starting to access Facebook, down to that level is probably just as useful” (P7). As well as being accessible for everyone, participants highlighted the importance of cybersecurity materials being detailed enough for all types of Key Relations to understand and apply behaviours, “because it’s so broad, people won’t adhere to it so it has to be specific enough that people actually understand the applicability” (P4). When discussing how to make training realistic and relevant to all Key Relations, some participants gave examples. One participant detailed an example video they were shown of how engaging with social media accounts online can present risk. The participant explained the video showed a coffee shop advertising a free coffee for anyone who liked their Facebook page and when the individuals who liked the Facebook page were provided their free coffee, the cup contained all the information you could find out about them from their Facebook page. The participant remarked that examples like this remind people that cyber threats are realistic and attract people’s attention, “if you could do something that could capture people, I’m thinking about that example of writing on the Costa cup, that absolutely encaptured me” (P1). Some participants suggested that using fear to make example cyber threats realistic can be beneficial as fear drives individual to engage in secure behaviours, “ultimately fear is the main driver for getting people to do any of these things” (P17). However, participants had mixed opinions on the role of fear when providing realistic case studies, with some suggesting examples should be relevant enough that it shocks Key Relations, without scaring them [P4, P14]. Fear appeals have been suggested as effective for encouraging information security behaviours within previous research. Dupuis and Crossler (2019) found a higher perceived threat severity and threat likelihood established through implicit fear appeals was associated with higher mitigation behaviours against the threat. However, there is the suggestion that use of fear in materials aiming to encourage adoption of cyber secure behaviours is ineffective (Lawson et al. 2016), with the potential that content may become unrelatable for some individuals (Bada et al. 2015). With the results from participant interviews and the existing literature being inconsistent regarding the role of fear appeals in encouraging individuals to adopt cyber secure behaviours, this topic is explored and discussed further in Phases 3 in Chapter 6, following exploring the perspective of Military Key Relations themselves.

Another way identified of helping Key Relations engage with any future cybersecurity materials is monitoring trends in technology and threats to guarantee materials are up to date and addressing the current online risks and vulnerabilities. This recommendation is explored in sub-theme *Importance of updated threats* and is closely related to the previous sub-theme *Relevant and accessible content*, as updated information ensures materials are relevant to the audience. One participant explained that people are consistently presented with the same information about the online threats from a long time ago they disengage with the content, “it’s great we’ve learnt but what has happened in the last 6 months, what’s different today and the year before, because it gets a bit samey” (P4). As well as monitoring and updating threats relevant for Military Key Relations, participants also stated it is important to reflect changes in Key

Relations' behaviours online, to monitor for any emerging or increasingly prevalent vulnerabilities "it is about a shift in behaviours [...] we've got to find some way of monitoring it (P5). One way of monitoring how individuals behave online is for those creating cybersecurity materials to understand how to use the technology and online communication platforms as they progress. One SME discussed how when Tinder came out they used the app in a work capacity to monitor any vulnerable behaviours being exhibited by personnel, "if we see them popping up online on Tinder then they're not following the policies" (P11). This is direct monitoring of personnel's behaviours but through using the platform, these SMEs were able to understand what information can be posted on the platforms. By identifying this for any emerging platforms and technology, those creating cybersecurity materials can provide specific guidance for Key Relations' security behaviours.

Alongside recommendations for content of cybersecurity materials for Military Key Relations, participants highlighted the challenge of determining how to disseminate materials. Some participants suggested traditional methods like physical leaflets would be useful as they are easy to disseminate, "a pamphlet would be a nifty thing to have, it would be quick and easy and [...] they could say just quickly pass this pamphlet across to any family members and it gives them more information" (P6). Conversely others commented that as the internet is ubiquitous, using social media or other online formats would be more convenient, "social media maybe....actually what am I talking about it definitely needs to go out on those [...] it's so addictive" (P5). Some participants said that using established routes of contact between military organisations and military personnel's friends and relatives would be useful in reaching Key Relations already engaged with the military community. In sub-theme *Existing contact methods* participants discussed how using in-person events that Key Relations already attend provide a starting off point to begin engaging with Key Relations about their cybersecurity. For example military passing out days and inductions for families living on military bases provide an opportunity for conversations already framed in a military context, "just a little side note that obviously your people have joined a military branch and there is cybersecurity" (P6). Participants also highlighted existing organisations that contact Key Relations directly, including military family charities such as the Soldiers', Sailors' & Airmen's Families Association SSAFA [P5], an armed forces charity that assists military families with sheltered housing, support for bereavement and help with financial difficulties (SSAFA, 2024). Some of these charities even have existing online pages, such as websites and social media accounts, which could provide an avenue to deliver cybersecurity messaging [P15].

In sub-theme *Online vs. offline* the benefits and challenges of using both online distribution channels such as social media, websites and emails, as well as offline communication channels such as in-person seminars, magazines and leaflets are discussed. Participants suggested that online content about cybersecurity for the extended military community is convenient as Key Relations can access it in their own time, referring back to it when they need it. Online methods have the additional benefit that content can be more engaging such as short videos or animations, "a video or narrated animation [...] would be more applicable and they can look at it in their own time and they could share links" (P4). However, the use of online technology to distribute this cyber messaging may not be applicable for everyone. Some participants suggested that a younger generation would prefer online messaging, but the older generation would find a physical pamphlet beneficial to take away and read in their own time [P8]. One SME described their experience with Key Relations is that they use opportunities to contact military organisations if they have a query. Therefore a cybersecurity portal was proposed where Key Relations could submit concerns or flag potential threats or incorrect online

behaviours that may influence military organisations, “having that direct line between them and the wider defence community that’s the next step” (P15). This would be beneficial for military organisations to keep updated records of threats and provide outputs about cybersecurity incidents back to Key Relations.

The interview questions also asked participants to provide their opinion on any potential barriers they perceive for Key Relations engaging with any future cybersecurity training, education or awareness materials for cybersecurity. These are discussed in sub-theme *Barriers to engagement*. Participants stated the challenge of behaviour change when Key Relations consist of such a wide range of people with a variety of backgrounds, knowledge levels and motivations. To overcome this challenge one participant emphasised the importance of encouraging a shared experience of all being part of the military community “it’s just a complete mismatch of people shoved together [...] but one thing they all have in common is that they’re part of the military” (P13). Participants also spoke about various physical barriers including finding the time to complete any cybersecurity training [P3]. Additionally people are less likely to engage with materials that requires them to download a new app or create a new account for a platform, “even just things like having to create another log on, I have no interest in that” (P4). Whilst this sub-theme is standalone, it effects all other sub-themes explored in this theme as no recommendations are perfect, and all have their potential barriers to engagements, explored throughout the theme. It can be difficult to measure the effect barriers have on engagement with cybersecurity initiatives, with no agreed method to measure effectiveness of cybersecurity initiatives (Chaudhary et al. 2022). In the current thesis, participants highlighted how with any recommendations for cybersecurity initiatives it will be difficult to measure the level of engagement received by Key Relations, in sub-theme *Challenges of measuring effectiveness*. The audience of Military Key Relations is challenging as there is no way to ensure materials are reaching the entire community, or measuring which Key Relations attend cybersecurity programmes, “something like that would be great but there’s no way of tracking that or gaining attendance” (P13). Despite the challenges, participants were in agreement on the importance of measuring the effectiveness of cybersecurity initiatives. Metrics provide insight into the success of a cybersecurity initiative and can help direct future materials “metrics are really important to us as intelligence personnel [...] to see how effective it is but to see if there’s any patterns or anything we can draw from it” (P12). In this way, recommendations for future engagement with Military Key Relations about their cybersecurity should consider content and delivery but also methods of measuring effectiveness.

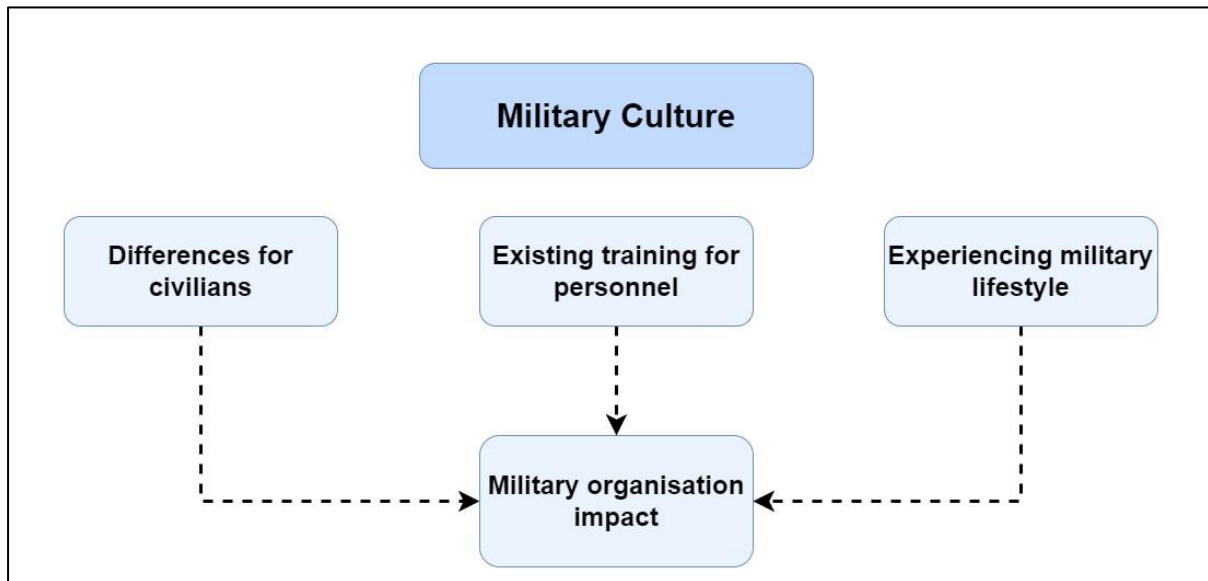
### 5.3.7. Main theme 7: Military Culture

Military Key Relations experience aspects of military culture such as deployment and relocation which ingrains military culture into the life of Key Relations, as well as military personnel [P2]. This experience of military culture creates a shared identity between Key Relations that arises from understanding what it is like to be a military family and incorporates values that are consistent with values held by service personnel including honesty, altruism, recognition of service and the importance of community (Manicini et al. 2018). Throughout the interviews in Phase 2 participants highlighted aspects of military culture that Key Relations have adopted due to being exposed to military lifestyle and experiences, which can influence how they behave online, including engaging with secure online behaviours. This theme, **Military Culture**, explores how military lifestyle, experiences and values play a role in key relation’s approach to cybersecurity, including an increased awareness of online risk through information sharing in sub-theme *Experiencing military lifestyle*. Sub-theme *Military organisation impact* discusses the

effect Key Relations’ online behaviour can have on military organisations’ cyber resilience in sub-theme. Sub-theme *Existing training for personnel* explores how cybersecurity is approach for military personnel and the sub-theme *Differences for civilians* highlights how there is a contrast between serving military personnel and civilians. Figure 5.9 visualises the directional relationship between these sub-themes.

**Figure 5.9.**

*Sub-themes of Theme 7, **Military culture**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.*



Sub-theme *Experiencing military lifestyle* explores the ways in which Key Relations may experience military lifestyle. This includes previous family life when growing up before becoming a military spouse [P1], living on a military patch [P4] and Key Relations being currently or previously employed within a military role [P4, P8, P11]. One participant reflected that the majority of their Key Relations have military experience and so all have a higher perception of the vulnerability that can occur through online behaviours that can be exploited by a military adversary, “I think I live in a bit of a bubble [...] friends most of them are military, so they’re all quite careful as well” (P3). This cybersecurity awareness may increase further for families where both parents have roles within the military, termed dual-military families. These families often have different decisions to single-military households when it comes to balancing work-family life. This includes deployment and location decisions, alongside childcare arrangements to ensure the family is not negatively impacted by career choices of the parents (Smith, 2015). One participant in the current thesis highlighted that being a dual-military household increases the discussions about cyber at home. They hope this exposure to discussions about cybersecurity will encourage children to be more considerate of what they’re posting online, “even when we’re not around they’d make the right sort of decisions in terms of not oversharing [...] because that’s what the message is coming from home” (P12). Some participants were unsure whether their Key Relations’ experience of military lifestyle and culture influences their approach to cybersecurity compared to the general population, “, it may be affected by the fact that my wife came from a military family [...] and so whether she’s average, I don’t know” (P1). Whereas others suggested that Key Relations who might only know one person in the military are less connected with military culture and engage in more online risk behaviours, “wider groups of friends and family

[...] are quite quick to post something saying their son or daughter is about to set sail [...] maybe those individuals have less military involvement except for a relative” (P12).

This difference in approach for those actively engaged with the military lifestyle and those with less experienced it outlined in the sub-theme *Differences for civilians*. This sub-theme reflects how participants’ opinions towards online behaviours and cybersecurity is different for military personnel and civilians, including Key Relations. For some Key Relations the consequence and impact for a military person and organisation is not as hard hitting and because this risk is not reinforced within civilian life. Key Relations may not understand the cyber risk that accompanies online information sharing, “if people aren’t military and have never been closely related to someone in the military, they don’t really understand the consequence of posting something” (P7). Participants highlighted how success on social media and the internet is a vital aspect of job performance for some civilian roles. This can create dissonance for Key Relations where sharing information online is second nature in their job whereas being a key relation of a military person requires them to be more considerate of what they post online, “what we can and can’t post will be completely different to say a magazine who’s got their own social media” (P8). This difference in approach towards online security behaviours between military personnel and civilians makes it challenging to educate Key Relations about the risks for both Key Relations and their military person in a way they would understand, “it’s really hard to explain that to people in a way that they just get it [...] it’s not malicious it’s just people being people” (P17). This way of thinking from civilians and Key Relations could be explained using the availability heuristic, which suggests the likelihood of a cyber event occurring is dependent on the individual’s ability to produce an example of where threat or risk has occurred previously (Benson & McAlaney, 2019). In this context, if Key Relations lack awareness of a previous example of a military friend or relative’s online behaviour influencing a military person or military organisation, they are more likely to perceive a lower probability that their online behaviour will influence military cyber resilience. The importance of working around this challenge, perhaps through incorporating recommendations from Theme 6, **Training and Education Recommendations**, is key. Participants highlighted that this knowledge and awareness difference for cybersecurity risks between military personnel and civilians makes Key Relations more vulnerable to being a target for military adversaries. Key Relations can be perceived by an adversary as being a weaker point within the extended military community, “it makes no difference who dispels the information online [...] a threat actor would target the weakest vector to get what they need” (P15).

The potential impact for military cyber resilience that occurs due to the online vulnerability of Military Key Relations is outlined in sub-theme *Military organisation impact*. Participants highlighted the potential risk of Military Key Relations sharing information online is becoming a target for military adversaries. This can increase the likelihood of Key Relations or military personnel being blackmailed by a threat actor, “threat actors can target military personnel, but they can also put leverage onto families and loved ones” (P16). However a number of participants also reinforced the idea that Key Relations can contribute to reputational damage for military organisations. This is due to Key Relations sharing apparently mundane information mentioned by their military person onwards to friends. This behaviour is particularly damaging if information is shared with media outlets [P2]. Information shared onwards to and by Key Relations is often shared in snippets of information which can be damaging when perceived by the general public, “anything that is posted online could be taken out of context” (P5). Information taken out of context carries potentially heavy reputational damage for both individuals and organisations. Participants gave examples of where individuals have lost their jobs due to information being shared through Key Relations. For example, a Captain being fired

during the covid-19 pandemic due to allowing a BBQ to happen [P5] which the media and public perceived as breaking lockdown and social distancing rules (Haynes, 2020). Additionally reputation damage that initially impacts one or multiple individual personnel can have consequent damaging effects for military organisations. When personnel and civilian safety is determined by a service person's ability to perform well in their job, personal distractions or concern over reputational damage can result in consequences to safety. Distraction is a frequently used principle in social engineering attacks (Stajano & Wilson, 2011), and vulnerability to cyber attacks increases further when an individual is experiencing a high cognitive workload (Jalali et al. 2020). Personnel focused on Key Relations' online behaviour, and the potential for reputation damage, may be more likely to experience inattention blindness. Inattention blindness occurs when an individual does not notice unexpected events of secondary task due to being preoccupied with a primary task (Mack & Rock, 1998). Cybersecurity is often considered a secondary task (Montanez et al. 2020). However, if a military person's first task changes from the physical and online security considerations of their job role to the consideration of the consequences of Key Relations' online behaviour, then this could result in personnel overlooking aspects of security. There is also the potential for information shared online by Key Relations to adapt into a physical attack from a military adversary. A key relation complaining about difficulties in communicating with their military person online exposes a unit is having communication issues thus creating a potential for the unit and its personnel of being the target of a physical attack from an adversary [P12].

As part of the interviews, there was one question which focussed on the participants' own experience of cybersecurity training, awareness, and education. This question and the associated prompts had multiple purposes including building rapport with participants, situating them in the mindset of cybersecurity and providing context for how they might knowledge share with friends and relatives. These questions also provided an opportunity to provide qualitative metrics directly to military organisations about personnel's opinion on cybersecurity, including their cyber risk and their opinions and application of training and education materials. The researcher would like to acknowledge due to the classification of these responses, not all information analysed as part of these questions have been included in the current thesis but have been included in direct outputs to military organisations. The responses included in this thesis have been outlined in the sub-theme *Existing training for personnel*. When discussing their own cybersecurity training, many participants highlighted that training can be unrelatable [P13] and is generic [P1, P9]. Participants suggested that those in specialised cyber roles mostly learn on the job and through their own research, "in terms of formal training the cyber 101 and then learning on the job really" (P11). This is a key point as theme 5, **Existing approaches**, identified that military organisations often rely on personnel to convey cyber risks and communicate recommended cybersecurity behaviours to their friends and relatives. This information cannot be shared if individuals are only provided with a basic understanding of cyber risk, and especially if risk is not framed within the context of Key Relations. Some participants did highlight the risk of Key Relations online behaviours is mentioned within their security training but that the information provided regarding Key Relations was minimal, "it does briefly touch on how your friends and family can let you down when it comes to things like social media" (P10). Participants provided recommendations for how personnel's cybersecurity training could be improved, including providing more specific threats and how to mitigate against them [P9]. Additionally personnel should be provided with education on how to make their Key Relations aware of the importance of the information about the military shared with them, "the only thing that could be added would be about overtly stating make sure you only tell people, your friends and family, that

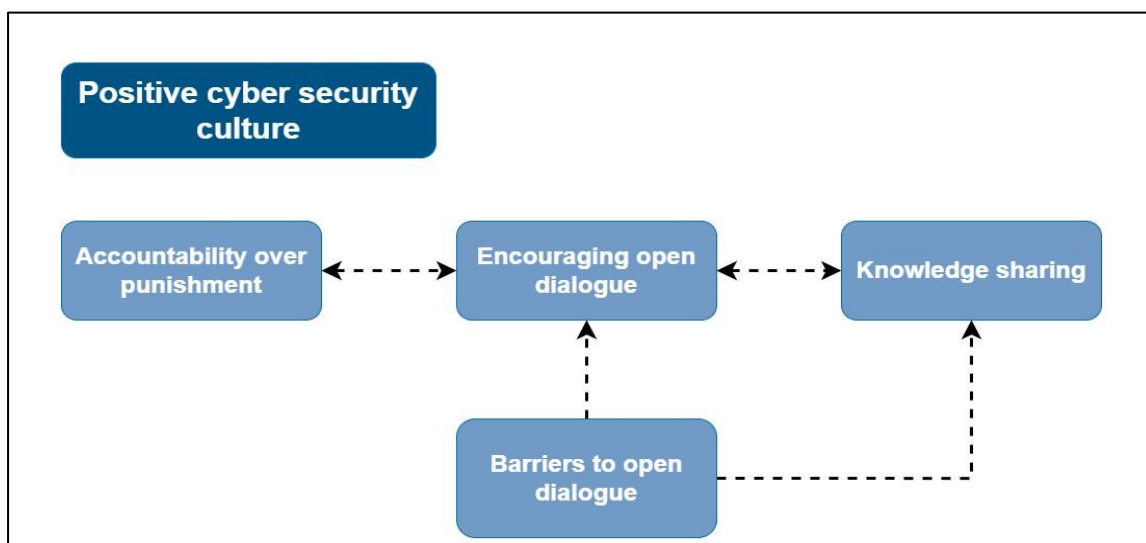
you trust and make sure you impress upon them the impact” (P7). By improving the cybersecurity training and education provided to military personnel, this allows personnel to be more confident to share this knowledge with their Key Relations in a more informal setting, which could influence the way in which Key Relations influence military cyber resilience.

### 5.3.8. Main theme 8: Positive Cybersecurity Culture

During the interviews participants were asked to provide their opinion on how military organisations should engage with Key Relations to encourage them to consider their online behaviours and adopt secure online behaviours to reduce cyber the vulnerability presented by Key Relations, where possible. A positive Cybersecurity Culture within the literature has been suggested as one that prioritises cyber resilience and considers individuals’ attitudes and values to encourage them to learn and apply strong cybersecurity practices (Gill, 2021). Many participants reflected this stance in their responses which encouraged organisations to move away from blame culture in sub-theme *Accountability over punishment*. Participants highlighted the benefit of open discussions between Key Relations and military personnel about cybersecurity behaviours in sub-themes *Encouraging open dialogue* and *Knowledge sharing*. The challenges that occur with open dialogue are also discussed in sub-theme *Barriers to open dialogue*. Figure 5.10 illustrates the relationship between these sub-themes, explaining the direction of these relationships.

**Figure 5.10:**

*Sub-themes of Theme 8, **Positive cyber security culture**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.*



Research into encouraging people to adopt secure online behaviours focuses on the importance of organisations approaching cybersecurity from accountability and educational standpoints where individuals can learn from their mistakes, rather than being punished for their mistakes (Gill, 2021; Elifoglu et al. 2018). Sub-theme *Accountability over punishment* discusses how participants believe that military organisations should focus on encouraging a culture of lesson learning from cybersecurity incidents rather than punishment. Additionally participants highlighted that this needs to be communicated to Key Relations to encourage their engagement with cybersecurity initiatives and application of secure online behaviours. Participants



suggested that they would not consider their Key Relations accountable for not knowing how to behave safely online, if they are not provided with the information, “I would not blame anyone in my family for not knowing” (P6). Participants suggested that a potential reward for Key Relations that engage in good cyber practice, or help others adopt secure online behaviours, could increase the likelihood that Key Relations will adopt these behaviours. It also rewards individuals for modelling secure behaviours, “they’re a shining light for cyber behaviours in the dependent community and that should be positively reinforced within the MOD” (P15). Safa and Solms (2016) suggest that organisation perceived as supportive towards cybersecurity and individuals’ behaviours are more likely have this support reciprocated back into the organisation. The use of rewards, whether this be a tangible reward or recognition of an individual, could help Key Relations move to feeling more supported by military organisations. Particularly as Key Relations can feel there is a lack of support and understanding of the role that Key Relations play in contributing to the extended military community (Sewart, 2022).

Part of encouraging a positive Cybersecurity Culture within the extended military community could be through military organisations encouraging *Knowledge sharing behaviours*. This sharing could be between Key Relations and their military person [P8], amongst different Key Relations [P6], and also between different military organisations [P15]. One participant spoke about a powerful knowledge sharing experience of overhearing their daughter sharing information about online safety with her friends, explaining that she understands the reason behind why her parents discourage her from engaging in certain online behaviours due to the potential risk, “there’s a reason why, and she’s explaining to her friends, which is really quite heartwarming and [...] quite powerful” (P12). This can be beneficial as role models for behaviour change are most effective when the audience can relate to them or if they have been through similar experiences (Strasser-Burke & Symonds, 2020), such as a close friend in the scenario outlined by Participant 12. The participant also claimed it reaffirms their daughter’s knowledge about cybersecurity, “to me means she’s taking it quite seriously and not just accepting what I’ve said she’s reaffirming her understanding” (P12). Research into sharing information security advice identified that the role of an individual’s attitude is pivotal, with a more positive individual attitude towards security behaviours increasing knowledge sharing within an organisation (Dang-Pham et al. 2017). This provides evidence for the benefit of building a positive Cybersecurity Culture for individuals within the extended military community that benefits the Ministry of Defence as a whole.

One way knowledge sharing can occur is through military personnel and their Key Relations having open, two-way discussions about cybersecurity, explored in sub-theme *Encouraging open dialogue*. Participants consider conversations with Key Relations about their online behaviours, potential online risks and risk mitigation behaviours, reduces the vulnerability of their Key Relations and the risk they present to military cyber resilience. Some participants highlighted how these discussions already occur as they perceive it a necessity to explain the requirements of their Key Relations online behaviours to avoid any potential risk to themselves or their military organisation, “I’d rather be open and honest with someone [...] if it saves a situation rather than beat around the bush [...] and something happens, and you wish you’d done it” [P8]. Examples of the content of the discussions include the military person’s requirements for location sharing online [P6], disinformation and misinformation online [P12] and privacy settings [P9]. One participant highlighted they think having these conversations as a family is beneficial as it encourages children adopt cyber secure practices that become second nature. Consequently this makes them much more conscious of their online presence than their friends, “we tend to speak a lot more about cybersecurity, so I think perhaps my children might be a bit

more cautious than perhaps some of their friends” (P10). This dialogue is even more beneficial if it is bi-directional. Opening up the conversation about cybersecurity allows Key Relations to ask their military person for advice and learn about online safety behaviours in a more informal way that they can then apply in any environment and decision-making situation [P2, P12]. Participants explain how Key Relations are generally receptive to these conversations, especially once it has been explained why this is so important for the safety of the participant and their colleagues due to their job role. One participant draws on an example of where they limit the amount of information they provide about deployment to their mother due to the concern she might share this information on. Once the participant had an open discussion about the reasoning why they choose to limit the information, their mother was able to understand, “she wishes she knew but I’ve told her exactly why I don’t and it’s fine because she knows and it’s easy to manage” (P7).

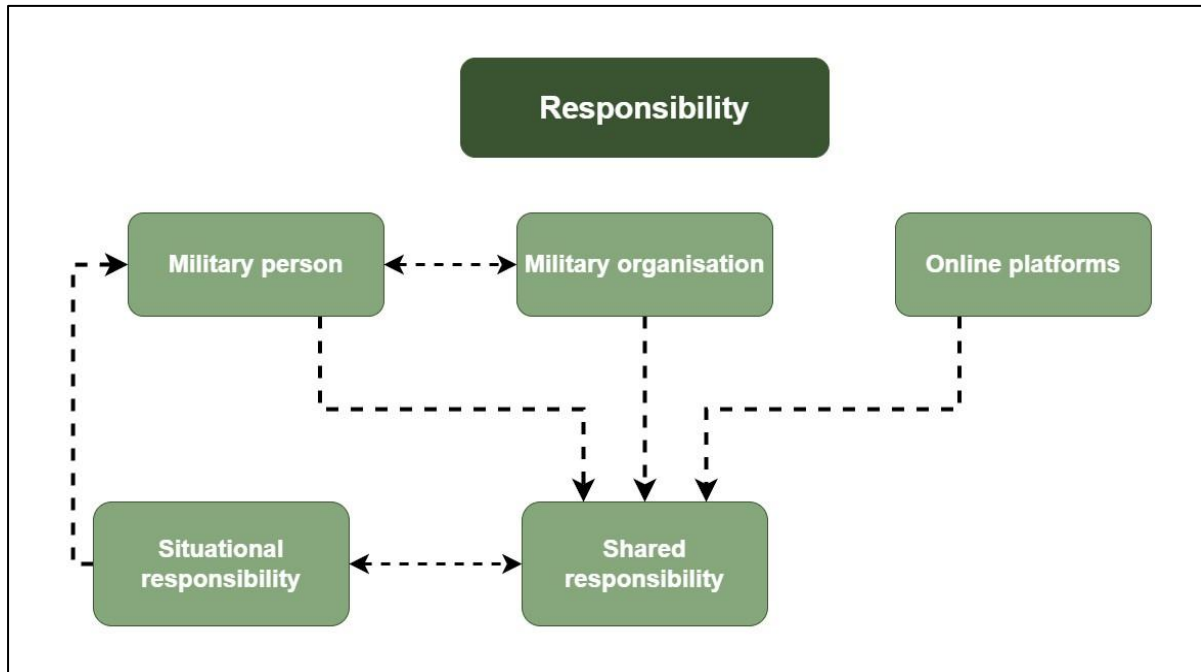
However, participants highlighted that conversations between personnel and their Key Relations may have its challenges in sub-theme *Barriers to open dialogue*. Some participants suggested that the perception of the military person training their Key Relations in cybersecurity, even informally through conversation, would be awkward and would strain relationships [P5, P9]. With the potential that some Key Relations would feel upset if they had posted something online with pure intentions and then their military person asked them to remove it, “I guess some parents you could imagine them getting a little bit hurt” (P6). Some participants also thought the reception of Key Relations about cybersecurity requirements in relation to military cyber resilience would be dependent on the individual’s personality. The suggestion is that those who spend a lot of time engaging with online technology would struggle to understand the military person’s perspective and would respond to the request with “I’ll do what I want” (P9). It may be beneficial for military organisations to provide military personnel with materials or information that they can pass along to their Key Relations. This can avoid the potential awkwardness of these conversations but also combat the challenge of personnel trying to explain risk without breaching sensitive information [P10] and using terminology suitable for a layperson.

### 5.3.9. Main theme 9: Responsibility

Responsibility is an aspect of Cybersecurity Culture which focuses on achieving accountability for online behaviour by making individuals aware of their role within security (Nel & Drevin, 2019). To explore the role of Cybersecurity Culture in understanding how Key Relations contribute to military cyber resilience, and to address aim 4 and the corresponding research question, participants were asked who they believe should be responsible for Key Relations online behaviour. There were a variety of approaches to responsibility discussed by participants and creating the theme **Responsibility** allowed for all these potential approaches to be explored in one theme. This theme identifies that Key Relations’ online behaviour should fall to various actors including personnel in sub-theme *Military person*, the various organisations in the Ministry of Defence in sub-theme *Military organisation*. Additionally there should be an increasing responsibility of the companies running online platforms themselves, explored in sub-theme *Online platforms*. Scenarios where responsibility might be conditional is also discussed in sub-themes *Shared responsibility* and *Situational responsibility*. Figure 12 depicts the relationship between these sub-themes, explaining the direction of these relationships.

**Figure 5.11:**

Sub-themes of Theme 9, **Responsibility**, and their relationships as indicated by the dotted lines. Arrows indicate the direction of the relationship.



Sub-theme *Military person* approached responsibility in two ways. One aspect suggests that military personnel receive cybersecurity training in their job to know what information is classified and what they can and cannot share with their Key Relations. Therefore it should be the military person's responsibility to not provide their Key Relations with sensitive information, "it's to me to have that knowledge, because I shouldn't be sharing anything with them that is unsharable"(P1). This suggestion for responsibility reduces the opportunity that Key Relations will share information online that would present a risk to military cyber resilience, if in the hands of a military adversary. Conversely, other participants note that it is not possible for military personnel to limit sharing everything with their Key Relations, especially when it involves personnel being away for a period of time. In this situation, military personnel should be responsible for ensuring that their Key Relations online behaviour does not present any cyber risk for military organisations. This can happen through explaining to their Key Relations how important the information is that they have access to, "it's just educating them and I think it's my responsibility for my children and my friends" (P8). Personnel should also be responsible for monitoring and addressing any online behaviours that Key Relations' exhibit that could present a cyber risk to military organisations, "I believe that's very much something I myself would need to monitor, or the person in the job role" (P6). One participant suggested that as the vulnerability of their spouse from a threat actor based on them being a military spouse this encourages them to educate their key relation on cybersecurity, "I think because there's more perceived threat if she did something wrong, it probably makes me want to educate her more and her want to know more" (P2).

However, this might only be achievable for personnel who's job role is focussed around technology and cybersecurity, as is the case for many of the participants who completed the interviews, but is not representative of the general military work force population. For those who

work in non-technical roles, they will have sufficient knowledge of online threats, and cyber secure behaviours for their job role, but may lack the confidence, ability and resource capacity to be able to communicate this knowledge to their friends and relatives. Therefore, it may be more beneficial to allocate responsibility to the organisations, explored in sub-theme *Military organisations*. This provides leaders within organisations the opportunity to demonstrate and model good cyber practice that can trickle down throughout the organisation, “culture [...] is set from the top [...] if you don’t have the right people setting the tone and not practicing what you preach then you can’t expect anything else” (P16). This behavioural change towards safer online behaviours within military organisations could be addressed through policy and strategy [P5]. Uchendu et al. (2021) suggests that having clear and well-communicated policy plays an important role in encouraging a positive Cybersecurity Culture within organisations. This sub-theme links closely to Theme 8, **Positive Cybersecurity Culture**. Multiple participants highlighted that ultimately the military organisation are the reason that personnel and their Key Relations are more vulnerable to being targeted by a military adversary. Therefore, they have a responsibility to protect their service people and their Key Relations, “I think the organisation has a responsibility to the sailors and their families [...] it’s a partnership” (P5). Therefore organisations should be responsible for providing Key Relations with the cybersecurity education and awareness to help reduce cyber risk, “if we do that right as an organisation, sailors will buy in and the families will buy in” (P5). As the military moves to a more civilianised workforce [P15], engaging with the wider military community addressed the necessity to align with civilian practices rather than having distinct military regulations.

As explored in Theme 3, **Understanding online risk**, there is a potential that Key Relations cannot adopt online security behaviours if the online platforms they use do not function in a way that encourages security. This is one reason why participants suggested that the developers and owners of social media platforms should have a role in responsibility for cybersecurity. This is highlighted in sub-theme *Online platforms*. Multiple participants reflected how they view social media platforms making changes to encourage safety on their platforms positively. For example as introducing time limits for children when using TikTok [P12] and providing an option to hide the ‘like’ count on Instagram posts [P14]. Participants perceived this as beneficial for reducing the potential risks of online platforms for children, “I think is a really responsible move so I would love to see more of that for children of a certain age” (P12). However, if viewing online security behaviours as the responsibility of the online platforms, these companies should ensure that any movements to a more secure system are still functional for end-users (Ambore et al. 2021).

As the previous sub-themes suggest, participants’ opinions on responsibility for friends and relatives online behaviours vary and reliance on different actors for different aspects of responsibility. Therefore responsibility may not be a concept that is belonging to one group of people, but instead shared amongst multiple actors. The sub-theme *Shared responsibility*, explores participants suggestions that sharing responsibility may be more beneficial due to there being a large number of people accessing military information that should protect it. Some participants suggested that responsibility should be divided between the Key Relations, the service person and the military organisation, “I think it’s a three-way split between the organisation, the person and the family, everyone is in this together” (P5). However, others suggested the responsibility should be shared by the military personnel and their friends and relatives. With Key Relations making a sustained effort to be more aware about how their online behaviour could influence military cyber resilience and military personnel providing them with guidance on how Key Relations can reduce their vulnerability online [P8, P14, P15]. One

participant suggested that even though military personnel and their Key Relations share responsibility, that the military person and their Key Relations should be approached as entire entities such as individual households or families, “make sure we consistently align them a bit more and not look at them as two separate parts as they come as a package” (P15). However, the role of the military person in responsibility for their Key Relations online behaviours may be limited during certain situations. For example when the military person is deployed they cannot consistently monitor their Key Relations online behaviours to ensure sensitive military information is not being posted, “when I’m not around, there will be a delay of oh grandad posted that 3 days ago and who knows who would have seen that now” (P6). This change in responsibility depending on the environment and the situation is described in sub-theme *Situational responsibility*. Additionally, participants suggested personnel that are in higher ranks or have more experience within the military, have more responsibility for their Key Relations’ online behaviours compared to those newer to the military. This is because these individuals are more aware of the requirements of the role, “I think that it’s probably a bit age dependent and rank dependent [...] I’ve been in long enough to now and my wife has been around long enough to know better” [P2].

This theme presents multiple approaches to responsibility for Military Key Relations’ online behaviours. Phase 3 explores the perspective of the Key Relations themselves and provides the opportunity for more insight into the role of responsibility in military cyber resilience, discussed in Chapter 6.

## 5.4. Results summary and implications for Phases 3 & 4

This section provides an overview of how the results address the research questions highlighted at the beginning of the chapter, and how the results will shape the creation of materials and the approach to the next Phases of the research, Phases 3 and 4.

[Research Question 1: Are the military friends and relatives who are identified as Key Relations the same individuals who currently receive cybersecurity training?](#)

Theme 1 explores the definition of Key Relations in more detail, with immediate family, extended family and close friends all being identified by participants as people they would consider as their Key Relations. This is consistent with Phase 1 which identified that military personnel would contact a range of Key Relations when they are deployed, discussed in Chapter 3. The definition of Key Relations created in this thesis based on the results from Phase 1 and 2 includes the friends and relations listed below and will be used when discussing the term Key Relations throughout the rest of the thesis, including Phases 3 and 4.

- Wife/Husband/Civil Partner
- Unmarried partner
- Short term partner (less than 1 year)
- Parent/Guardian
- Child
- Sibling
- Grandparent
- Extended family e.g. Cousin/Aunt/Uncle/Niece/Nephew
- Co-habiting friend/roommate
- Friend from school
- ‘Close’ or ‘Best’ friend

Whilst a range of friends and relatives are considered within this definition of Key Relations, Phase 1 identified that partners were the most frequently contacted when on deployment. Phase 2 expanded on this further, identifying that often it is unavoidable for military personnel to share operational details with their partner, increasing the likelihood that these individuals may share sensitive military information online. Within the interviews participants frequently discussed how their own roles within defensive cyber, as well as their partner's experience working in defence or cyber, contributes to more open discussion and an increased knowledge and awareness of the risks that can arise as a result of their online behaviours. This was reiterated within Theme 5, **Existing approaches**, with many participants discussing how military personnel are relied upon to disseminate their learning about cybersecurity information, to their Key Relations. During the interviews, there was sparse mention of direct outreach for cybersecurity training to Key Relations, with some receiving information during informal events, such as airshows, and if they live on military bases. This suggests that only those Key Relations who are already actively involved with the military community are receiving any formal cybersecurity training content from military organisations, rather than the range of Military Key Relations that personnel have identified in both Phases. This increases the online vulnerability for Military Key Relations and the subsequent risk that military information could be shared online and accessed by a military adversary. This thesis posits the Key Relations outlined above should receive cybersecurity materials that situates their online risk in the context of their military person, to reduce the vulnerability Key Relations' online behaviour could present to military cyber resilience. However, considering the challenges identified by participants with contacting Key Relations, there should be an interim priority to provide all military partners, including short-term partners and those not currently considered next of kin, with cybersecurity materials. This is due to the findings from Phases 1 and 2 suggesting personnel share the most detailed information with their partners, compared to other Key Relations.

One type of partner not included in this definition is an ex-partner. Whilst one participant mentioned an ex-spouse in their interview, when highlighting that they co-parent with this individual. Additionally, multiple participants mentioned in-laws when considering their Key Relations. Neither of these groups of Key Relations were included in the definition of Key Relations at this point due to the decision that accessing these individuals to invite them to participate in Phase 3 of the research would be challenging. [Section 7.2.1. The definition of Military Key Relations](#) discusses this in more detail, alongside recommendations for addressing including these types of relation in future research.

Research Question 2A: What types of online behaviours are friends and relations displaying?

As highlighted in theme 2, **Online risk behaviours**, participants frequently discussed the behaviour of Key Relations on social media. Key Relations' use of social media is consistent with the approach taken within current society, where information about our everyday lives is overshared on a variety of social media platforms. The findings from Phase 2 suggest there is a difference in behaviour that is influenced by age, as identified in Theme 4, **Individual differences**. The younger generations, use a much wider range of social media platforms, with more reports of them using apps like Snapchat, BeReal and TikTok. Compared to older generations, more participants mentioned Facebook and Instagram and those who have spent the majority of their life without social media, are more reluctant to engage with social media platforms. This provides further insight into the initial suggestion that age plays a role in influencing platform usage from Phase 1, as discussed in Chapter 3. This finding will be explored

further in Phase 3 of the research, to provide early insights in the behaviours of Key Relations from their own perspective. This is discussed further in Chapter 5.

Research Question 2B: How could these behaviours present a cybersecurity risk to military organisations?

The following section discusses the findings from Phase 2 which suggest how behaviours displayed by Key Relations may present an online risk and contribute to military cyber resilience. As highlighted above Key Relations frequently share information about themselves on social media. However, this behaviour on social media becomes a risk for military organisations when Key Relations share information online about their military person. This information sharing increases the likelihood that a military adversary may triangulate military information and the vulnerability of Key Relations to online manipulation from a threat actor with the desire to gain more information or to reach the military person. When discussing recommendations for how to reduce the cyber risk that Key Relations' behaviours may present to military cyber resilience, it is important to understand the reasons why Key Relations may choose to behave in this way. Theme 3, **Understanding online risk**, highlighted multiple reasons that Key Relations may share this information online, which vary from pride to a lack of understanding about technology and importance of information. The findings also highlighted generational differences within Key Relations in online risk behaviours. Many participants were concerned about their parents' safety online when the technology is so new to them, as it could increase the risk of them behaving in an insecure way online. Participants were also conscious of considering the influence of generation Alpha, where individuals have never known a time without social media, and how this might influence their approach to cybersecurity. Recommendations in this thesis for reducing Military Key Relations' online risk behaviours should be considered as a point of view consistent with society's current approach to technology, and that recommendations should be consistently reviewed and updated alongside the progression of technology. Additionally, throughout the interviews, there was some uncertainty from participants about the true extent of how their Key Relations behave online, particularly for individuals they spend less time with. This could mean that they don't have a full understanding of how their behaviours may increase a risk to cyber resilience. Therefore, it will be important to compare these findings to the perspective of Key Relations themselves in Phase 3 to provide a deeper understanding of Key Relations' online behaviours, to determine the extent behaviours may present a cybersecurity risk. Having an in-depth overview of potential risk behaviours can form the basis of recommendations to mitigate against potential online vulnerabilities and risk.

Research Question 3: Who should be responsible for Key Relations' online behaviour and their cybersecurity training, education and awareness?

Theme 9, **Responsibility**, explains how there was no definitive consensus from participants in Phase 2 about responsibility for military key relation's behaviour and their cybersecurity training, education and awareness. Some participants suggested a shared approach to responsibility between military organisation, military personnel and Military Key Relations, may be the best approach. Military organisations can provide cybersecurity resources to provide education and awareness for military personnel and their Key Relations to stay safe online, and military personnel can provide additional reinforcement of these materials at home and highlight the importance of securing the information they tell their Key Relations. However, this is only effective if Key Relations are able to understand and apply the information to their online behaviours. In this way, the next phase of the research (Phase 3) will focus on exploring

the difference between Key Relations' cybersecurity knowledge and understanding and whether their behaviour alters when considering information about their military person. This will be done in a survey to provide a clear definition of the two concepts to the Key Relations, and to identify whether they engage in different online safety behaviours when it comes to their military person's information compared to their own information. Based on findings from Phase 2, and to encourage engagement from Key Relations with any materials, it is important to gather key relation's opinions on responsibility when it comes to information about their military. Phase 4 will focus on asking Key Relations about their opinion on responsibility. Asking this question in a focus group setting allows for a deeper understanding for why Key Relations feel this way and provides the opportunity to discuss any potential barriers to a future approach.

Research Question 4: What should Key Relations be asked in Phases 3 & 4 to help guide creation of engaging cybersecurity initiatives?

As part of the interviews, participants were asked to provide their opinions on what future research should ask Military Key Relations to help encourage them to engage with future cybersecurity materials. Participants reflected the research should be asking Key Relations about their understanding of the extent their online behaviour influences their military person, as well as recommendations for specific cyber hygiene behaviours, such as secure passwords and making their profiles private, and how to frame materials. Many participants identified it would be useful to know whether Key Relations are aware of how they should be behaving online to protect their military person and their information. Additionally, participants suggested Key Relations should be asked whether they understand the reasons it is important to behave safely online and the potential consequences for their military person as a result of risky social media posts. This confirmed the importance in the approach of distinguishing between Key Relations' levels of cybersecurity knowledge and understanding for Key Relations, as highlighted when discussing research question 3 above. There is the potential that free-response questions about risk could be considered broad and may not be appropriate for individuals with limited cyber experience and knowledge. One SME provided a recommendation that the Key Relations should be provided with specific cybersecurity behaviours, such as use of multi-factor authentication and unique passwords and asked to select the extent they engage in these behaviours. This influenced the creation of some questions in Phase 3. Questions about cyber hygiene behaviours were originally a free response box and were altered so that participants could indicate the extent they engage in these security behaviours. This question form provides prompts for Key Relations and encourages responses to be reflective of Key Relations' engagement with cybersecurity behaviours rather than testing their ability to recall cybersecurity behaviours. The survey contains a mixture of quantitative and qualitative questions to provide participants the option to divulge further information about their online behaviours if they want to. It is important to inspire participants to engage fully with the research. One participant highlighted the benefit of framing cybersecurity materials in a positive manner and championing Key Relations that engage in secure cyber behaviours. This was taken into consideration when creating research materials for Phases 3 and 4, including the Participant Information Sheet and consent form. These documents highlighted how the research focuses on understanding how Key Relations can contribute to keeping their military person safe online, to encourage Key Relations to feel the research is a safe and trusted place to discuss their opinions and experiences.



## 5.5. Limitations and considerations for future research

Whilst not included as a main theme, multiple participants highlighted limitations with the sample when participating in the research. Due to the sample, it would be expected these individuals are more likely to engage in secure cyber behaviours due to some of them being experts within the cyber space, but also that those who engage with research are more likely to engage with other aspects of military life including engaging with and applying training principles. This point was highlighted by one participant within their interview, and an additional participant reflected on the role of rank and personal experiences both for individual personnel and their Key Relations and how this might influence in their uptake in cyber secure behaviours. The research also reflects on the participant sample as part of this, noting that the majority of participants are established in their career and that even those who were military representatives either had an aspect of their role that was cyber focussed or had an interest of hobby focussed on cybersecurity which might have made them more drawn to participate in the research.

For groups such as military personnel and experts within military organisations, there is the potential that question responses may have been distorted or responses may be reluctant due to suspicion towards researchers from mainstream society (Howitt, 2019), rather than within a military role either as a service person or civil servant. The potential effect of this was reduced by including an opening section at the beginning of the interviews which allowed the researcher to explain that whilst the research is being conducted by Bournemouth University, it is match funded by Dstl, but still emphasised the researcher is a civilian rather than a service person. For future research to address the limitation of reducing the influence of participant's concern of discussing their experiences with an academic researcher outside of the military, an interview-by-insiders approach could be adopted. Insider interviews involve a member of the same group, so a serving person or civil servant rather than an academic, to conduct the interview (Howitt, 2019). There are potential challenges with this approach due to the resource constraints of training individuals to run the interviews (Devotta et al. 2016), but they could offer the benefit of bringing a perspective an individual without any experience in this field, such as an academic without a military background, would not offer (Howitt, 2019). For this particular research problem, the resource limitations of training of an individual with previous experience only in the military, could be addressed by having an interviewer who has experience within both roles, for example a reservist. This is addressed in later Phases of the research, such as Phase 4 as both the focus group facilitator and participants will be civilians.

## 6.5. Key takeaway points from Phase 2

Findings from Phase 2 support the definition of Military Key Relations created in Phase 1, identifying that participants include a wide range of friends and relatives when asked who their closest relations are. When considering the risk to military cyber resilience, many participants highlighted that it is most difficult to not share operational information with their partners. This requirement in sharing sensitive information could create a vulnerability for cyber resilience when considering the potential online risk behaviours that Key Relations may engage in, particularly on social media. The findings from the interviews suggested a variety of reasons for why Key Relations may engage in online risk behaviours, with two themes suggesting that age may play a determining role Key Relations online risk behaviours.

Phase 2 provided insight into responsibility for Key Relations online behaviours when considering organisational cyber resilience in the military. Participants had varied opinions on a recommended approach for responsibility, with the findings overall indicating that effective

responsibility should be shared between the military person, their key relations and the military organisation. Whilst Phase 2 provides a more in-depth understanding of the experiences and behaviours explored in Phase 1, currently the suggested directions for future engagement with Key Relations about their cybersecurity only provides insight from serving personnel and SMEs. Exploring the perspectives of Key Relations in Phase 3 will provide further understanding into potential online risk behaviours friends and relatives engage in, and their opinions towards current and future cybersecurity initiatives to address any online risk behaviours.

## Chapter 6 - Phase 3: Exploring the Perspective of Military Key Relations in an Online Survey

The previous chapters discussed Phases 1 and 2, which explored the perspective of military personnel and subject matter experts in defensive cyber. Building on these findings, Phase 3 provides an insight into the perspective of Key Relations themselves. Phase 3 includes the perspective of individuals who are considered Key Relations based on the definition created using Phase 1 and Phase 2 findings. These individuals include Wife/Husband/Civil Partner, Unmarried partner, Short-term partner (less than 1 year), Parent/Guardian, Child (aged 16 years and older), Sibling, Grandparent, Extended family e.g. Cousin/Aunt/Uncle/Niece/Nephew, Co-habiting friend/roommate, Friend from school and 'Close' or 'Best' friend. One of the restrictions of Phases 1 and 2 of the research is that any potential understanding of why Key Relations may choose to behave a certain way online is an opinion or external observation from military personnel and subject matter experts. Exploring the experiences of Key Relations themselves allows for a deeper understanding of Key Relations' knowledge and comprehension of how and why their online behaviour can be influential for military organisations. The full aims and the respective research questions for Phase 3 are outlined below:

**Aim 1:** Explore how Key Relations report communicating with their military counterparts, including platform usage, frequency and topic discussed. These additional factors provide more insight into whether behaviours present a risk to military cyber resilience or are low risk, social interactions.

**Research question 1a:** *Will the type of relationship influence the communication frequency between Key Relations and their military person, with higher communication frequency for partners, parents, children, grandparents, and 'close' friends?*

**Research question 1b:** *Will platform usage alter with age, with younger participants using social media platforms more than older participants?*

**Research question 1c:** *Will there be different patterns in platform usage depending on the type of relationship?*

**Research question 1d:** *How does deployment situation and access limitations influence patterns in platform usage?*

**Research question 1e:** *Are topics discussed with personnel mainly non-work related, and does this differ from responses in Phase 1 from military personnel due to less pressure to conform to security standards set by military training?*

**Aim 2:** Gather perspectives on what Key Relations believe their online vulnerabilities to be for military organisations.

**Research question 2:** *Are there differences in level of understanding of vulnerability and how this might impact military organisations within Key Relations?*

**Aim 3:** Explore current experiences and opinions of cybersecurity training, education, and awareness materials for Key Relations provided by military organisations.

**Research question 3a:** *To what extent do Key Relations rely on their own cybersecurity knowledge and training, as opposed to that provided by military organisations, to keep information safe online?*

**Research question 3b:** *Do Key Relations receive cybersecurity awareness materials at times of operational significance such as deployment or relocation?*

**Research question 3c:** *How do barriers to participation such as relocation and fear of asking for help influence Key Relations' reluctance towards future cybersecurity initiatives?*

This phase uses a mixed-methods online survey to address three aims. The first aim intends to explore Key Relations online behaviours, from their perspective. Phase 1 provided an insight into the communication behaviours between military personnel and their Key Relations. Phase 2 provided further insight into the potential risk to military cyber resilience from Key Relations' online behaviours, from the perspective of military representatives from the Front-Line Commands, alongside subject matter experts (SMEs) in cyber education and awareness, and cyber incident reporting and monitoring in Defence. Exploring Key Relations' perspective alongside military personnel's and SMEs' perspectives will provide a thorough overview of online behaviours in the extended military community. This allows for any future cybersecurity initiatives encouraging Key Relations to behave securely online, which is relevant and addresses a wide range of authentic online behaviours. This provides the opportunity to create a Cybersecurity Culture that incorporates the need for military personnel and their Key Relations to communicate sufficiently and efficiently to maintain relationships, irrespective of location (Rea et al. 2015). Whilst simultaneously providing individuals with the knowledge of how to do this safely and protect their military person's information. The second aim explores Key Relations' understanding of how these online behaviours can impact military cyber resilience. Findings from Phase 2 suggest that some Key Relations do not demonstrate a good understanding of the importance of protecting military information and how an adversary can monitor a variety of online sources, including Military Key Relations, to seek this information. Phase 2 findings suggested that Key Relations whose military person provides them with this information will have a better awareness of the importance of their online behaviour. However, some personnel may not communicate this information to their Key Relations or may only communicate it to certain relations such as spouses and children. By asking Key Relations whether they understand the extent their online behaviour is important when considering the safety of military information, any potential gaps in understanding and potential vulnerabilities to online threats can be identified. The final aim explores Key Relations' opinions towards cybersecurity initiatives. Phase 2 findings suggested the current approach for Key Relations' cybersecurity is limited, though it can occur for those already engaged with the military community. However, it often relies on Key Relations accessing information in their own time, or their military person communicating cyber risk and safety knowledge to them. Additionally some researchers suggest that low motivation towards cybersecurity initiatives are ineffective if individuals believe cybersecurity is not relevant to them (Hadnagy, 2010). Other research suggests that even if individuals are motivated the cybersecurity awareness materials provided are disengaging inappropriate, and still rely heavily on users applying their own situational context (Bada et al. 2018). Exploring this further from the perspective of Key Relations provides an insight into where the gaps are in the current approach, and how to address them in the future.

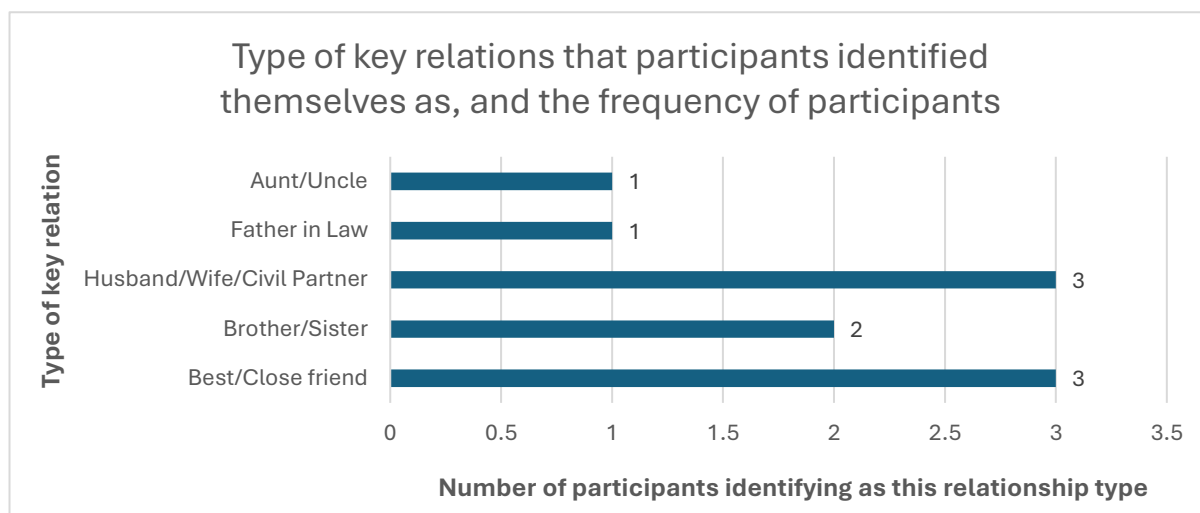
## 6.1. Phase 3 Pilot Study

### 6.1.1. Phase 3 Pilot Study: Method

A pilot study was conducted, with a participant sample of ten Military Key Relations. Two participant responses were removed due to being incomplete, indicating a withdrawal from the study. Nine participants identified as female, with one participant identifying as male. Participants had a mean age of 28.70 years ( $SD = 6.53$ , Minimum = 25, Maximum = 42). Participants identified themselves as a range of military close relations, as displayed in Figure 6.1 below, with six participants identifying their military person serves in the British Army and four in the Royal Air Force.

**Figure 6.1:**

*Type of Key Relations that participants identified themselves as, including the frequency of participants identifying themselves as this type of relation, for the pilot study sample.*



The pilot study participants completed an online mixed-methods survey. Participants completed the survey in a mean time of 15.03 minutes ( $SD = 6.53$ , Minimum = 7.48, Maximum = 29.92). Participants were provided with the Participant Information Sheet, and then the informed consent questions, both of which were embedded within the survey. The survey opened with demographic age and gender questions. Opening questions about their military person consisted of what branch of the military their military person serves in, and what the relationship type is between themselves and their military person. Participants were then asked to score the strength of the relationship on an 11-point scale, with 0 being 'Not a strong relationship' and 10 being 'A strong relationship'. The rest of the questions are presented in sub-sections in the same way that the participants were presented the questions.

#### *Online communication behaviours questions*

The next set of questions asked participants about their online communication behaviours. Participants were provided with a list of options and asked to select how often they contact their military person when on deployment. Additionally, participants were asked what platforms they prefer to use to communicate with their military person and why they choose certain communication methods. In this section, participants were also asked if there are any

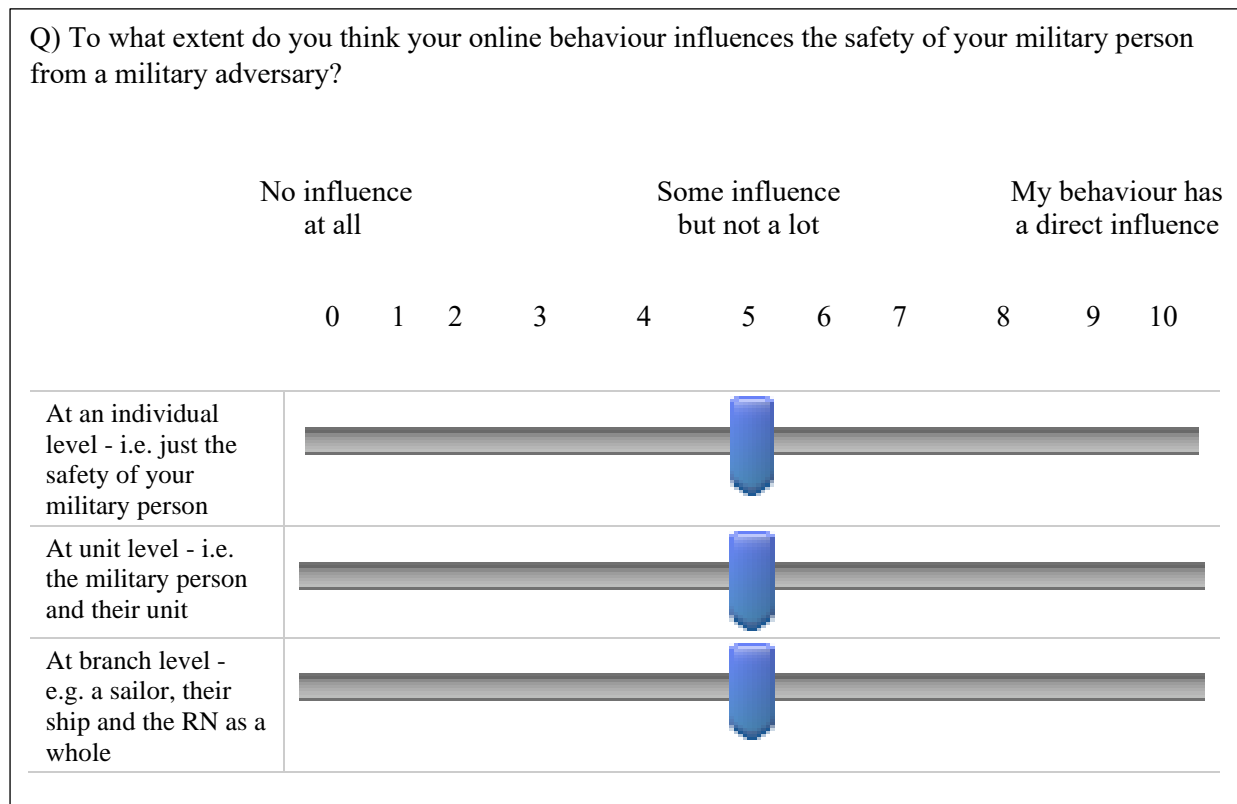
platforms they think are more secure than others, and why they might think this. Both of these were free-text response questions. These questions were influenced by findings from Phase 2 which identified that use of platforms such as WhatsApp is discouraged within the military community, with Signal recommended instead. In Phase 1 it was highlighted that no questions were asked about group chat communication, even though existing research (e.g. Matassi et al., 2019) indicates group chats are frequently used for communicating with friends and relatives. Therefore, the final question in this section asks if participants communicate using social media groups. For this question, if participants select 'yes' they are provided with questions that ask them to discuss more detail about these groups including who they communicate with and why they choose the format of groups. They are then also asked about access control and their awareness of any measures in place in the groups they are part of to monitor who is accessing the group. If participants answer 'no' to the question about whether they use social media groups for communication they are provided with a follow-up question about why they choose not to use social media groups.

### *Cybersecurity risk behaviours questions*

This section opened with questions where participants rated their confidence in their knowledge and understanding of cybersecurity risk behaviours. For these questions, participants were provided with a list of online behaviours and asked to rate on an 11-point Likert scale the level of cybersecurity risk associated with each behaviour, with zero being not confident and ten being very confident. Some of these behaviours include location sharing online, being tagged in a picture on social media and having an open or public profile. These risk behaviours are consistent with risk behaviours highlighted in Phase 2 as being a potential behaviour that Military Key Relations could engage in that could present a risk to military organisations. The next question provided participants with a list of cybersecurity behaviours, including installing anti-virus software, using different passwords and enabling two-factor authentication. Participants were asked whether they engage in each of these behaviours. After these questions, participants rated on a scale of 0-10 the extent to which these security behaviours are restrictive. To situate their online behaviours in the context of military cyber resilience, participants are then asked to rate on a scale of 0-10 the extent they think their online behaviour influences the safety of their military person at an individual level, unit level and branch level. Figure 6.2 demonstrates what these questions looked like for participants.

**Figure 6.2:**

*11-Point scale questions participants were asked in the pilot study about the extent they think their online behaviour influences their military person's safety at an individual, unit and branch level*



*Cybersecurity training, education and awareness questions*

The final set of questions focuses on cybersecurity training, education and awareness materials. Participants were asked if they had previously been invited or attended any cybersecurity training. If they select 'yes' a follow-up free response question asks participants to provide more detail about the content and provider of this training. If selecting 'no', participants are directed to the next question. This asks if they have received any cyber education and awareness materials via leaflet, email or online link. Again if participants select 'yes' for this question, they are asked to provide more detail about the content and provision. The final two questions focus on future initiatives and ask participants if they would attend an annual brief about online threats for Military Key Relations, and any barriers that would stop them from engaging with future cybersecurity initiatives. As this was a pilot study, to provide participants with the opportunity to direct any feedback to the researchers about the survey, a free response question was included that asked participants to state any concerns they had. This is included in Figure 6.3 below.

### Figure 6.3:

*Free response question pilot study participants were presented at the end of the survey to provide feedback on the survey.*

Thank you for completing the main survey questions! Your responses will provide data as part of a pilot study to ensure the survey makes sense and participants feel they can respond to the questions appropriately.

The text box below provides you the opportunity to explain any points where you were unsure of what was being asked of you during this survey. This might include questions where the question wording was unclear or where it was unsure how you were meant to respond, or anything else.

Providing this information can help us make sure the survey questions are clear for future participants.

---

### 6.1.2. Phase 3 Pilot Study: Results and Discussion

Overall participants gave their relationships with their military person a mean strength score of 9.00 (SD = 1.33, Minimum = 7.00, Maximum = 10.00). When asked how often participants would contact their military person, the most frequent response was 'Everyday', with 50% of participants stating this. Two participants said, 'Once a week' and 'Once a month', and one participant responded, '2 to 3 times a month'. When asked about their preferred platform to use when communicating with their military person, participants most frequently identified that 'Facetime' was their preferred communication platform, with three participants stating this. Whilst all participants responded in some way to this question, four participants responded in a way that was difficult for the researchers to interpret what the respondent had intended to communicate. For example, one participant rated four platforms '3', and four platforms '7'. The researchers could interpret this as the participant saying for these platforms those they rated as '3' are equally preferential yet are more preferential than the platforms they rated as '7'. However, this cannot be confirmed. Due to four participants responding in a manner that was not as intended, this question was altered for the main study. This change is discussed in the section below, [Alterations made following feedback and results](#). When participants were asked what their most important consideration was for deciding how to communicate with their military person there was a range of responses. Those mentioned more than once included 'Convenience', 'Security', 'Use of the Internet' and 'Familiarity' with the platform for both parties. No issues were apparent with this question, with participants responding as expected. The main study will explore additional effects such as the influence of relationship type and age on the results for these questions. However, due to the aim of the pilot study being to ensure the survey is suitable for the population and that participants can understand the questions, the pilot study will not report the influence of these additional factors.

When participants were asked if they thought any communication platforms were more secure than others, 70% highlighted they thought WhatsApp was more secure than other platforms. When asked for an explanation for this response, three participants highlighted end-



to-end encryption, though one participant demonstrated uncertainty 'I think the chats are encrypted' (PS2). One participant highlighted how WhatsApp promotes their platform as being more secure, and one participant suggested that WhatsApp and Facetime as the most commonly used apps they are more secure. Participants responded to these questions as expected. Two participants did not respond to the follow-up question when asked why they had responded the previous platform was more secure. However, one participant responded 'No' to the first question when asked if they thought there were any platforms more secure than others, requiring no additional explanation. The second participant explained their choice when asked in the initial question if there were any communication platforms they thought were more secure, stating that their primary method of communication is a phone call, so security is less of a concern.

Participants were also asked about their use of social media groups. Whilst the questions up to this point were adapted from the Phase 1 survey, this group of questions were the first addressing gaps from Phase 1. Seven participants identified that they do use group chats to communicate with their military friends or relatives. This was on a variety of platforms including WhatsApp, Instagram, Facebook Messenger and Snapchat. When asked follow-up questions about access and control monitoring questions in these groups one participant identified they're an administrator for Facebook Groups for military personnel and families. This participant explained individual credentials are checked to confirm people are genuine before being admitted to a group. Two other participants reiterated this. Two participants confirmed that of the one group they are a member of, there are measures in place to control group access. However, two participants indicated they were unsure if these measures were in place, and three participants suggested this only exists for some of the groups they are part of. Those who responded 'No' that they don't use social media groups in this capacity answered the follow-up question to explain why. Participants stated it is not a requirement for them due to only knowing one military person, or because they want to communicate with people individually.

The following questions focussed on cybersecurity risk behaviours and began with the 11-point scale question about confidence in 'knowledge' and 'understanding' of cyber risk and security behaviours. Participants rated their confidence in their 'knowledge' with a mean score of 6.60 (SD = 2.17, Minimum = 3.00, Maximum = 10.00). Participants rated their confidence in their 'understanding' with a mean score of 6.00 (SD = 2.45, Minimum = 3.00, Maximum = 10.00). In the main study, additional patterns will be explored, for example, whether those self-reporting lower confidence in knowledge and understanding also identified uncertainty in other questions. However, the results from the pilot study are sufficient to indicate the questions can provide this insight. When provided with a list of online behaviours and asked to select the extent participants consider this a cyber risk behaviour, participants answered in a way that suggested they were considering the choices. For example, generally, participants rated the levels of risk for different location behaviours as similar to each other, except for perceiving higher risk for picture tagging behaviours and then also geolocation and privacy settings behaviours. This was a similar pattern when participants were provided with a list of cyber secure behaviours and asked to select which ones they engage in. When asked about whether participants make any changes to their online behaviour when considering their military person, one participant responded, 'As above'. Due to the previous two questions being the behaviour listing questions, the participant may have intended this to mean their behaviour does not change, however, their intention is unclear. The question wording already provides an option for if there is no change in participant behaviour, and seven participants responded with "no change". The decision was taken that altering the question was not required.

The final group of questions focused on training, education and awareness materials. Two participants indicated they had been previously invited to cybersecurity training and three had previously received cyber education and awareness materials from a military organisation. Of those who said they had not and may be reluctant to engage with future materials, the most frequent barrier mentioned was time constraints. These results provide evidence that the questions are clear to participants and that are suitable are providing insight that can be built upon.

### 6.1.3. Phase 3 Pilot Study: Alterations made following feedback and results

At the end of the survey, participants were informed they had participated in the pilot study. An explanation was provided that the study aimed to ensure the questions were appropriate and made sense to participants. At this point, participants had the opportunity to provide feedback on the survey, particularly for any questions where the question wording was unclear. Only one participant responded to this question, with “None.” However, the researcher identified an issue with how participants responded to one of the questions, visualised in Figure 6.4. As highlighted above, for the question asking participants to rank their preferred communication method, there were inconsistencies in participant responses. Two participants left this question partially complete, and two participants did not rank the platforms in a clear numbering system. It is not possible to understand the reasoning for these responses, as none of these participants commented on this question in the feedback. To reduce the chance of participants misunderstanding what the question asks them to do in the main study, this question was split into two separate questions. The first new question asks participants to select all communication platforms they use to communicate with their military question, see Figure 6.5. Then a separate question asks them to rank which platforms they prefer to use, see Figure 6.6. Aside from this, no other changes were made following the pilot study survey.

**Figure 6.4:**

*Pilot study survey question asking participants about their preferred communication platforms*

When communicating with this individual, what is your preferred method of communication?

Please rank from most preferred **(1)** to least preferred **(15)**.

For platforms which you do not use, please enter 0 next to them.

\_\_\_ Facebook

\_\_\_ Text message/SMS

\_\_\_ Email

\_\_\_ Phone call

\_\_\_ Instagram

\_\_\_ Snapchat

\_\_\_ Twitter

\_\_\_ Telegram

\_\_\_ WhatsApp

\_\_\_ Facetime

\_\_\_ Skype

\_\_\_ BeReal

\_\_\_ Discord

\_\_\_ LinkedIn

\_\_\_ Dating App (e.g. Tinder/Bumble/Hinge)

\_\_\_ Other (please state)

**Figure 6.5:**

*New question in the main study adapted from the pilot study question in Figure 1*

When you want to speak **to this individual**, how do you communicate with them? Please select all methods below that apply, regardless of how often you use this method.

Facebook

Text message/SMS

Email

Phone call

Instagram

Snapchat

Twitter

Telegram

WhatsApp

Facetime

Skype

BeReal

**Figure 6.6:**

*New question in the main study adapted from the pilot study question in Figure 1*

When communicating **with this individual**, what is your **preferred** method of communication?

Please rank your most preferred using **(1)** and your least preferred **(15)**.

For platforms that you do not use, please enter 0 next to them.

\_\_\_ Facebook

\_\_\_ Text message/SMS

\_\_\_ Email

\_\_\_ Phone call

\_\_\_ Instagram

\_\_\_ Snapchat

\_\_\_ Twitter

\_\_\_ Telegram

\_\_\_ WhatsApp

\_\_\_ Facetime

\_\_\_ Skype

\_\_\_ BeReal

\_\_\_ Discord

\_\_\_ LinkedIn

\_\_\_ Dating App (e.g. Tinder/Bumble/Hinge)

\_\_\_ Other (please state)

## 6.2. Phase 3 Main Study: Method

### 6.2.1. Participants

In total 64 participants attempted the survey, however 31 responses were removed due to being incomplete. Participants were informed that if they wished to withdraw from the study they should close the browser window before clicking 'submit' on the survey. Therefore, any incomplete responses were considered withdrawn from the study and responses were removed. The 33 remaining participants are included as the participant sample for this study. The participants had a mean age of 37.97 years (SD = 11.98, Minimum = 22.00, Maximum, 64.00). Thirty participants identified as female, and three participants identified as male.

Participants were recruited via opportunity sampling, as participants were invited to participate via an advert (see [Appendix E](#)). This advert was distributed via multiple methods including via the Dstl Military Advisors and posted in service families community centres in Portsmouth. The research also attempted to reach a wide range of Military Key Relations that may not actively engage in services provided by Military organisations by disseminating the study advert in Facebook groups for Military Key Relations. To gain access to the Facebook groups in a credible way, I reached out to administrators of multiple Facebook Groups including for UK spouses, and one specifically for men who are partners of serving personnel. However, none of the administrators replied to indicate interest in disseminating the advert. There is the potential that this was due to contacting these individuals on an account which was created purely for the purpose of this study, and whilst steps were taken to provide credibility, the lack of information on the account may have been concerning for individuals who were contacted. However, they may also just not have been interested in the research.

During the process of gaining favourable opinion from the ethics panels as part of this research a target participant sample size was identified for this phase of the research. The sample size for Phase 3 considered the challenges that were identified during recruitment of participants in Phase 1. The target for participant sample size for Phase 3 was a minimum of 30 and a maximum of 384. A minimum of 30 participants aligns with Phase 1 and is sufficient to provide insight on an exploratory topic, but also aligns with previous research that used surveys in this area, such as a Bittner (2014) who had a sample size of 30 participants. The maximum participant number is reflective of the number of participants required to test statistical significance. This was calculated using the Qualtrics sample size calculator considering there is approximately 121,600 children from armed forces families (Ministry of Defence, 2022), and that each Key Relations sub-group has a similar population size. Considering a 95% confidence interval, and 5% margin of error (Coolican, 2019), this would create an ideal sample size of 384 participants. A sample size of 31 in this Phase meets the minimum requirement of sample size and reflects the challenges experienced during recruitment of participants. Lessons learned from these recruitment challenges are discussed in [Section 7.3. Evaluation of the Research](#).

### 6.2.2. Materials

An online survey questionnaire was created and distributed on the survey platform Qualtrics, a copy of the survey can be found in [Appendix C](#). The survey opened with the Participant Information Sheet and then the informed consent questions, embedded into the survey. Opening demographic questions asked participants about their age and gender identification. Participants were also asked initial questions about their military person. This

included a question about what branch of the military their military person serves in. Participants were provided with a list of relationship types, based on the definition of Key Relations identified in the previous Phases, and were asked to select which relationship type best suited their military person. There was also an 'Other' option if none of the provided relationship types adequately reflected their description. Participants were also asked to rate on an 11-point scale the perceived strength of their relationship with this person, with 0 being 'not a strong relationship' and 10 being 'a strong relationship.'

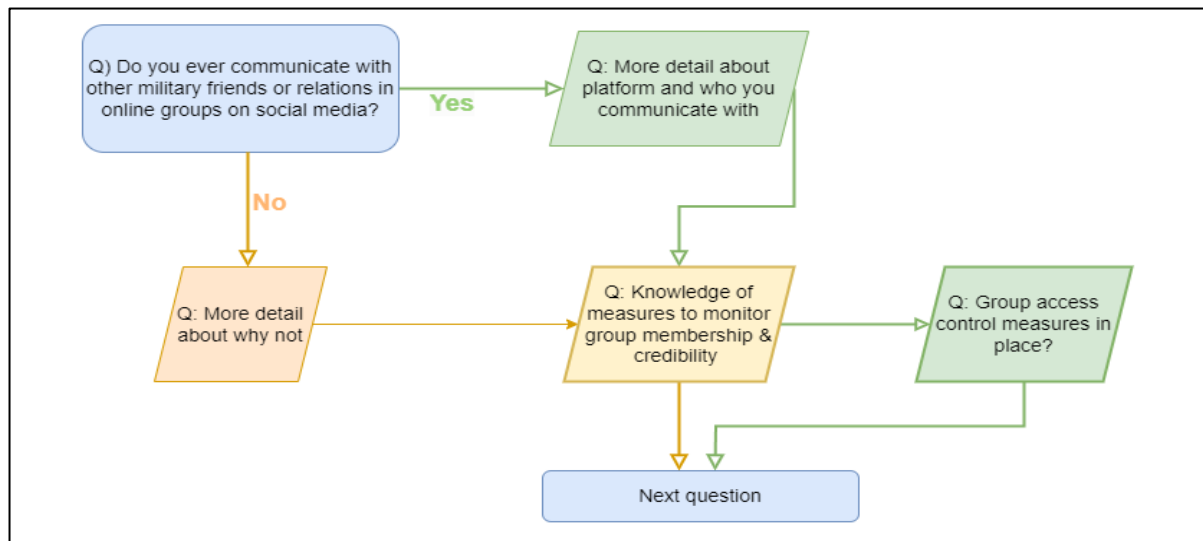
#### *Online communication behaviours questions*

The next block of questions focuses on communication frequency and platform considerations. The first four of these questions were adapted from the Phase 1 survey with military personnel. These questions asked participants about how frequently they contact their military person when they are deployed. Participants were provided with a list of options that align with a typical deployment length of 6 months, up to 12 months (Keeling et al. 2015). These options were: 'Once a year', 'Twice a year', 'Once a month', '2 to 3 times a month', 'Once a week', and 'Everyday (when possible)'. Participants were then provided with a list of communication methods and asked to select all the methods they use to contact their military person. This question is the adapted question from the pilot study visualised in Figure 5.5. Following this question was the second question adapted from the pilot study, visualised in Figure 5.6. This question provided participants with the same list of communication methods as the previous question and asked participants to rank their preferred communication methods, with 1 being their most preferred. To understand participants' decisions for these questions in further detail, a follow-up free-text response question asked participants to explain what the most important consideration is for them when deciding how to communicate with their military person. As the study aims to explore Military Key Relations' perception of their online vulnerability and how they might influence cyber resilience, the following questions centred on cybersecurity and communication platform usage. The first of these questions asked participants to state any platforms they think are more secure, based on their opinion and knowledge of online safety. To explore the justification behind the responses to this question, a follow-up free-text response question asked participants to briefly explain why they consider the platforms they identified, if any, to be more secure.

Following the analysis of Phase 1 results, Chapter 4 discussed how the survey had not addressed the use of group chats in communication. Therefore, questions in this question block explored Key Relations' online behaviour when communicating in social media groups. Firstly, participants were asked if they communicate with military friends or relations in online social media groups, Figure 6.7 outlines the follow-up questions depending on how participants respond.

**Figure 6.7:**

*The question flow for questions and follow-up questions asking about participants' use of social media group*



If participants responded 'Yes' they were asked a follow-up question to provide more detail about the platforms they use and who they communicate with. Participants who responded 'No' were provided a follow-up question asking them to explain why they choose not to communicate in online social media groups. To explore Key Relations' understanding and knowledge of cybersecurity, all participants were then asked to state any methods they were aware of that could monitor membership and member credibility when using social media groups. To understand if any methods are applied to these groups, participants who responded 'Yes' to the initial question were asked whether the groups they communicate in apply any measures to control group access. Participants were provided with a range of options. Half focusing on if participants are only a member of one group, and the others reflecting if participants are members of multiple groups.

#### *Cybersecurity risk behaviours questions*

The next block of questions focused on Key Relations' online risk behaviours. The researchers wanted to explore if there was evidence that supports the suggestion from Phase 2 participants that sometimes Key Relations may engage in online security behaviours without fully understanding why it was important, and the benefits of these behaviours. Therefore the next two questions asked participants to rate their confidence in their 'knowledge' and then their 'understanding' of cybersecurity risk and behaviours they can engage in for protection. Participants were provided with an explanation that the question on 'knowledge' was asking them about what they do, whereas the 'understanding' question focused on the why they do something. Participants were asked to rate their confidence on a 11-point scale, with zero being not confident, and ten being very confident. The next question explored Key Relations' understanding of cyber risk behaviours in more detail. Participants were given a list of online behaviours such as location sharing, use of geolocation settings, and having a public profile, and asked to select the amount of cybersecurity risk associated with each behaviour. The options provided ranged from 'No risk', 'Some risk', 'A little risk, and 'Extensive risk' and participants could also select 'Unsure' or 'N/A I don't use this platform'. The full list of behaviours can be seen in Question 19, in [Appendix C](#). In a similar question, participants were provided with a list of

cybersecurity behaviours including installing anti-virus software, enabling two-factor authentication, and not sharing passwords with others. The question asked participants to indicate which behaviours they engaged in to keep themselves and their information safe online. Participants could simply select 'Yes' or 'No', but they also could identify they were 'Uncertain if up to date or set up,' that they 'sometimes' engaged in these behaviours, or 'N/A – I don't have this device or platform'. The full list of behaviours can be seen in Question 20, in [Appendix C](#). To situation cybersecurity in the context of their military person and military cyber resilience participants were asked to describe any changes in their online behaviour they might make to keep their military person's information safe. To explore potential reasons for Key Relations not to engage in online security behaviours, participants were asked a question that encouraged them to consider if online safety behaviours are restrictive. Question responses were on a 11-point scale with zero being 'I can behave how I would like, whilst still being safe online', five being 'Online safety is restrictive on some behaviours' and ten being 'Engaging in online safety behaviours is restrictive'. Finally, this question block asked participants to consider the extent they think their online behaviour influences the safety of their military person from a military adversary. Participants were asked to score this on a 11-point scale, with zero being 'no influence at all' and ten being 'my behaviour has a direct influence. Participants were asked about this when considering the individual military person, the military person and their unit, and the military person and their branch.

#### *Cybersecurity training, education and awareness questions*

The final block of questions explored cybersecurity training, awareness and education for Military Key Relations. The first question asked participants if they had ever been invited to or attended cybersecurity training from a military organisation, participants were provided with the option to respond, 'Yes' or 'No'. Participants who responded 'Yes' were presented with a follow-up free-text response question asking for more detail on the nature of the training and who provided it. Those who responded 'No' were presented with the next question. This question asked if participants had previously received any education or awareness materials from a military organisation, participants were provided with the option to respond, 'Yes' or 'No'. Again, if participants selected 'Yes' they were presented with a follow-up free-text response question asking for more detail about the content of these materials and who provided it. If participants selected 'No' they were presented the next question. This next question asked participants if they would attend an annual briefing provided by a military organisation about online threats and safety behaviours to help protect their military person. Participants could respond 'Yes', 'No', or 'Perhaps, depending on other factors'. Those who responded 'No' were presented a follow-up free-text response question which asked for more detail about why they would not be interested. This was not presented to participants who responded 'Perhaps' as the final question addresses potential barriers. This final question asked participants to state any barriers that would prevent them from engaging with cybersecurity initiatives. This was a free response question and participants were provided with some examples of potential barriers to provide clarity on what was meant by the term barriers. Once participants had completed all the questions they were provided with the link to a separate Qualtrics survey where they could provide contact information if they were interested in future research on this topic or enter into the Amazon voucher prize draw.

### 6.2.3. Procedure

Participants were directed to the study from a link, as a URL and a QR code in the study adverts. Researcher contact details were also included on there should any participants wish to take part but be hesitant to follow a link or scan a QR code, however no participants chose to contact the researcher in this way. The links directed individuals who were interested to the survey, where they could read the Participant Information Sheet and then complete the survey, if interested. Participants completed the survey on Qualtrics with a mean completion time of 54.93 minutes ( $SD = 245.903$ ). The reason for a much higher completion time for these participants than the pilot study participants ( $M = 15.03$  minutes,  $SD = 6.53$ ), could be due to one participant taking 1424.47 minutes to complete the survey. This is potentially due to them starting the survey and coming back to it at a later date, though it is not possible to confirm. When removing this participant, the mean survey completion time was 12.14 minutes ( $SD = 4.93$ ).

### 6.2.4. Ethical Considerations

The Participant Information Sheet and Informed Consent Form were embedded at the beginning of the online survey distributed on Qualtrics (see [Appendix C](#)). Individuals were asked to read through the information sheet and consent form and then take 24 hours to consider whether they wished to take part in the study. At the time of seeking ethical approval for this phase, this thinking time was the recommendation from the Dstl Scientific Advisory Committee (SAC) and Ministry of Defence Research Ethics Committee (MODREC). Informed consent to participate in the survey was provided by participants via tick boxes on the landing page of the survey. In the information sheet participants were informed they could withdraw at any time from the survey by closing the browser, and that there is no requirement to answer the survey questions if they do not want to. However, participants were advised that once the survey responses had been submitted they would not be able to withdraw their responses, due to the survey being anonymised. The Participant Information Sheet also explained that the participants' decision to (not) participate in the research would not influence service members' careers, and anonymity was highlighted.

Anonymity was an important consideration for this study. To ensure anonymity where possible, personal information collected from participants was limited to age and gender. Additionally, limited information about their military person was collected to reduce the chance that someone could identify the participant or their military person from the responses. Participants were notified of this in the Participant Information Sheet, and it was explained individuals would not be attributable in any publications. Participants were prompted to remove any identifiable information from free response questions but were informed that any identifiable information accidentally included would be redacted during analysis. As compensation for completing the survey, participants could enter into a prize draw to win one of four £25 Amazon vouchers. To contact the individuals who had won one of the Amazon vouchers, the contact information was required. Therefore a separate Qualtrics survey was created so that participants could be entered into the Amazon voucher prize draw, and provide a contact email address, without the possibility of linking their personal information to their survey responses. This survey was also used if individuals wished to express an interest in hearing more about future research and to provide contact details for researchers to provide information the future studies as part of the wider programme of work outside of the PhD thesis.



The survey was summarised with a debrief section. This provided individuals with directions to support services, including military-specific services for military friends and relatives as well as personnel themselves. The participants were also provided the contact details of the lead researcher and the contact details of the volunteer advocate for the research. Whilst the survey did not directly ask questions that would cause participant distress, there is the potential that questions may evoke sensitive or upsetting emotions and memories for the participants. Therefore, ensuring a range of appropriate support services for participants, with the option to speak to military-specific services, was important. This phase of the study received favourable opinion from the Dstl Scientific Advisory Committee (SAC) and the Ministry of Defence Research Ethics Committee (MODREC): 2256/MODREC/23. Evidence of this is included in [Appendix J](#). Bournemouth University Ethics Committee also provided ethical approval for Phase 1 of the research, evidence of this is included in [Appendix K](#).

### 6.2.5. Data Analysis

The results produced quantitative and qualitative data. Quantitative responses were analysed using frequency analysis, which consisted of the frequency of participants who responded in a particular way, as well as the percentage of participants who responded in this way. For questions which required selecting a number on a scale of zero (low strength/low confidence etc.) to ten (high strength/very confident etc.). For these questions, the mean score was calculated. For example, the mean confidence score for all participants when asked about their confidence in their knowledge of cyber risk and cybersecurity behaviours. Qualitative responses from the survey were analysed using Qualitative content analysis. Inductive category development created categories from the qualitative responses, and sub-groups were formed based on the grouping of these categories. Independent coding was applied during the analysis and was particularly evident when creating these sub-categories for the free response questions to ensure categories accurately represented the participant data and were grouped appropriately. The data was analysed using JASP, version 0.15.0.0. Microsoft Excel was used to analyse responses when JASP was not compatible. For example, when analysing the free-response questions. Excel was used during qualitative content analysis to create categories from the responses, and then track the frequency of these categories and any overlap to form the creation of groups from the original categories.

## 6.3: Phase 3 Main Study - Results

This section provides the results for the survey questions outlined in the method section above. This section begins with an overview of the relationship types, strength and communication frequency. The most frequent relationship type that participants reported was that their military person was a 'Husband, Wife or Civil Partner', with a large percentage of the participants' military person serving in the 'Royal Navy'. Overall, participants gave the relationship with their military person a mean strength score of 9.49, with the highest possible score being 10. This section also highlights the most frequent communication regularity between participants and their military person was 'Everyday (when possible)'. Whilst the mean strength score did not differ vastly between relationship types, this section provides an overview of the interaction between relationship strength score and communication regularity. This section also provides results for participants' platform usage when communicating with their military person. Overall WhatsApp was the most frequently used and the most frequently preferred platform. Justifications participants provided for their platform choices varied but most frequently considered their military person's access when on deployment. Differences in platform usage

for relationship type and age ranges are reported. WhatsApp was also the most frequently mentioned platform when participants were asked which platform is most secure. Justifications provided for these responses mainly focussed on end-to-end encryption.

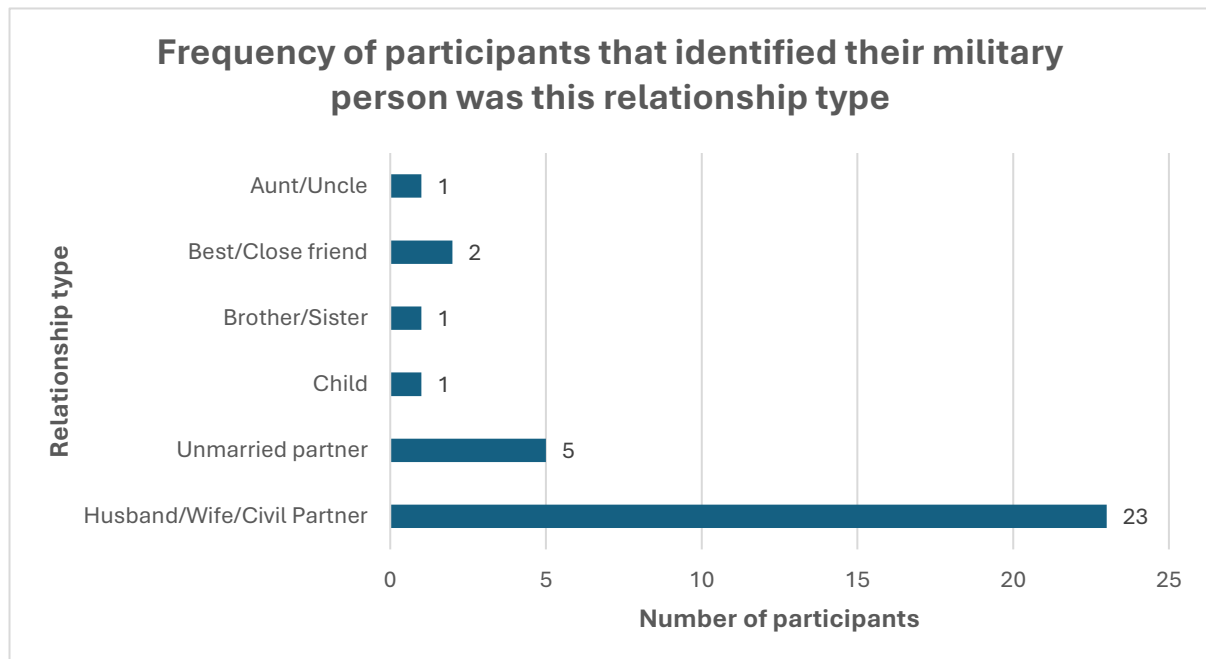
To address a gap in the survey from Phase 1, findings for how participants use group communication platforms are included in this section. Participants tended to use Facebook when communicating with online groups, who were mostly other Military Key Relations or families that live in the same military patch, which is an area of military housing provided on a military base for married servicemen and servicewomen. This section highlights the methods reported by participants that they're aware of for checking group member credibility and monitoring group access. Participants confidence scores of knowledge and understanding of cybersecurity and cyber risk behaviours are reported. With participants reporting a higher mean score for their understanding of cybersecurity and cyber risk behaviours. When considering specific risk behaviours, participants clearly indicated location sharing behaviours carry an extensive risk, whereas there was more uncertainty over tagging others and being tagged in online images. In the context of military organisations sub-section, responses for how participants alter their online behaviour when considering their military are presented. These mainly consist of ensuring no operational information is shared, though did vary, with some participants explaining they don't share anything at all about this individual online. The final sub-section states the findings for the questions on cybersecurity training, education and awareness. The results indicate only a small percentage of participants have previously received cybersecurity training or education and awareness materials from military organisations. However, a much larger percentage reported that they would be interested in attending future cybersecurity initiatives for Military Key Relations, if offered. Barriers to participants attending future cybersecurity initiatives are also discussed.

### 6.3.1. Relationships with military personnel: Types, strength and communication regularity

Participants identified six different relationship types that described their relationship with their military person. The most frequent relationship type that participants reported was a 'Husband, Wife or Civil Partner'. Figure 6.8 visualises the participants were a range of Military Key Relations, and how many participants self-identified their military person as being each relationship type. Participants identified that their military personnel served a range of military branches, with multiple individuals from each military branch. The highest frequency was for the Royal Navy, with 22 participants identifying their military person as serving for this military branch or 66.67% of participants. Five participants identified their military person serves in the Royal Air Force, four participants reported their military person serves in the Army and two participants stated their military person is in a civilian role within the military.

**Figure 6.8:**

*The frequency of participants that identified their military person was this relationship type.*



Across all participants and relationship types, participants scored the relationship strength with their military person with a mean score of 9.49 (SD = 1.03, Minimum = 6.00, Maximum = 10.00). There was very little difference in mean relationship strength scores across the different types of relations. Individuals whose military person was a 'Brother or Sister', a 'Child' and an 'Aunt or Uncle' all rated this relationship a score of 10.00. Those who identified their military person as a 'Husband, Wife or Civil Partner' gave a mean relationship score of 9.57 (SD = 0.90, Minimum = 7.00, Maximum = 10.00). The lowest mean scores provided by participants were still high. The lowest mean scores were for an 'Unmarried partner' at 9.00 (SD = 1.73, Minimum = 6.00, Maximum = 10.00) and a 'Best or close friend', also with a mean score of 9.00 (SD = 1.41, Minimum = 8.00, Maximum = 10.00).

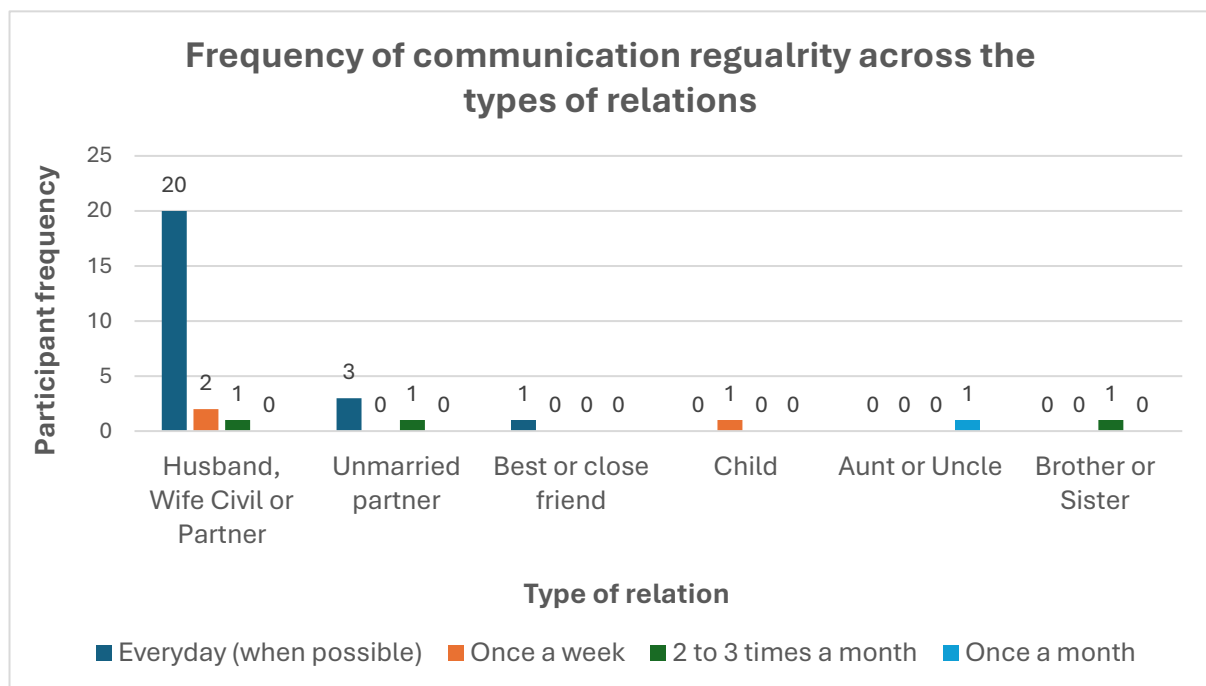
When asked about how regularly participants would contact their military person when they are deployed, the most frequent response was 'Everyday (when possible)'. Table 6.1 visualises the percentage frequency for these responses, demonstrating the large percentage that stated they would contact their military person 'Everyday (when possible)', but also the percentage split of how the rest of the participants responded. Zero participants identified that they would contact their military person 'Once a year' or 'Twice a year', and two participants did not answer this question. When split by relationship type, those who reported their military person was a 'Husband, Wife or Civil Partner', 'Unmarried Partner', or 'Best Friend' had a modal communication regularity of Everyday (when possible). The modal communication for 'Child' was 'Once a week'. The modal communication regularity for 'Brother or Sister' was '2 to 3 times a month' and it was 'Once a month' for an 'Aunt or Uncle'.



Figure 6.10 visualises the frequency for communication regularity across the types of relations. Due to the small sample size, and the high percentage of participants identifying their military person as a ‘Husband, wife or civil partner’ it is not possible to determine if there is a pattern of type of relation influencing communication regularity. The role of sample size is reviewed further in section [6.4. Phase 3 – Discussion](#).

**Figure 6.10:**

*Bar chart displaying the number of participants who would contact their military relation at this communication regularity, split by type of relation.*

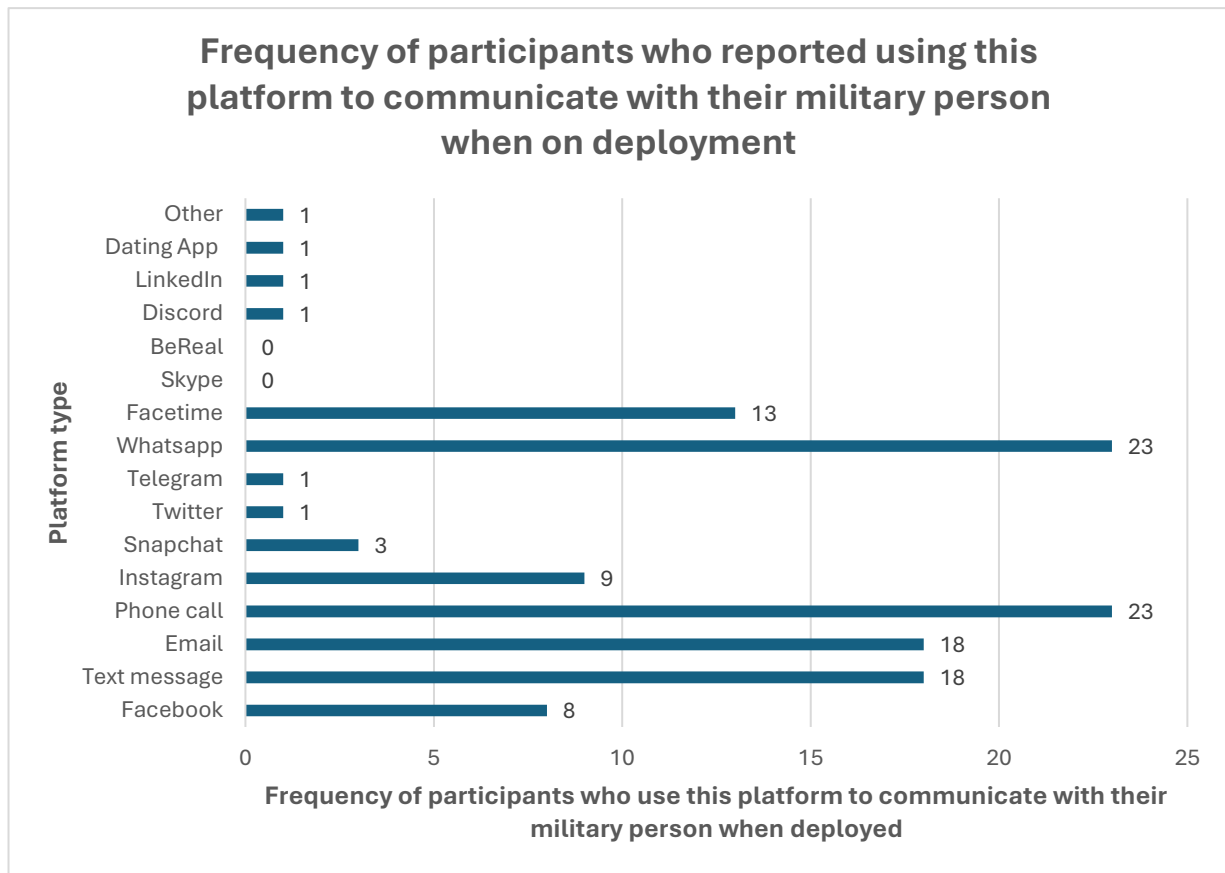


### 6.3.2. Communication platform preferences and safety considerations

When participants were asked about their communication platform preferences when communicating with their military, the most frequently used platforms were ‘WhatsApp’ and ‘Phone Call’. Figure 5.11 visualises the frequency of participants who reported using each type of communication platform to communicate with their military person on deployment. As the data in the Figures demonstrates the total number of responses is more than the total number of participants, which is due to participants being provided the option to select more than one platform. Figure 6.12 visualises the popularity of WhatsApp, Phone Call, Email, and Texting, whilst social media platforms such as Facebook Snapchat, and Twitter were much less popular. One alternative platform was included when participants were asked about any other additional platforms they use to communicate with their military person that had not already been included, visualised as ‘Other’ in Figure 6.11. This was ‘Familygram’, which is a service used by personnel serving on Submarines in the Royal Navy where other methods of communication are not viable. It allows friends and relatives to provide personnel with non-serious and joyful information in a one-way short form method (Royal Navy, 2024).

**Figure 6.11:**

Graph depicting how many participants reported using each communication platform to communicate with their military person when on deployment.



Participants were also asked about what platforms they most and least preferred to use when communicating with their military person. 'WhatsApp' was reported most frequently by participants as their most preferred platform, as visualised in Figure 6.12. However, there was a range of most preferred platforms, including other social media platforms 'Snapchat' and 'Facebook'. Two individuals ranked multiple platforms as their most preferred to communicate with their military person. Both of these individuals reported their most preferred were 'WhatsApp', 'Text messages', 'Email' and 'Phone call' were equally their most preferred. One of these participants also included 'Facetime' as an equally most preferred platform.

**Figure 6.12.**

Graph depicting how many participants reported each communication platform as their most preferred platform to communicate with their military person when on deployment.

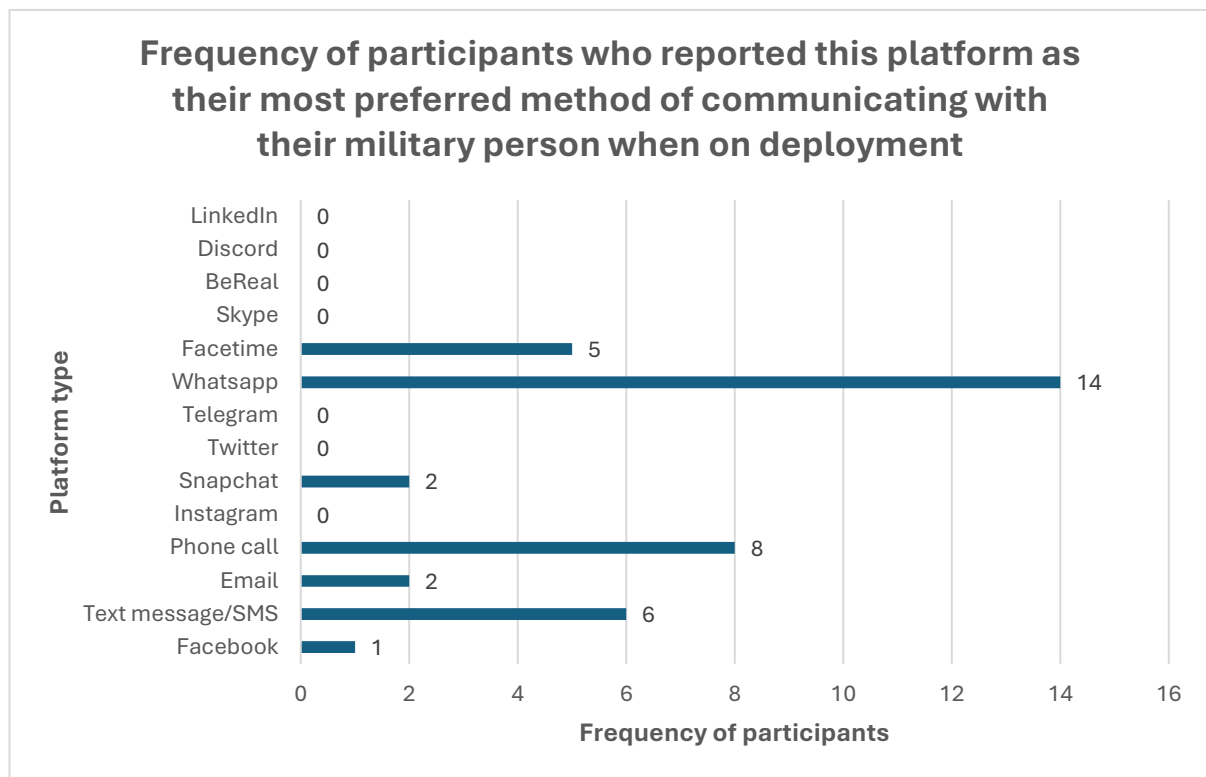
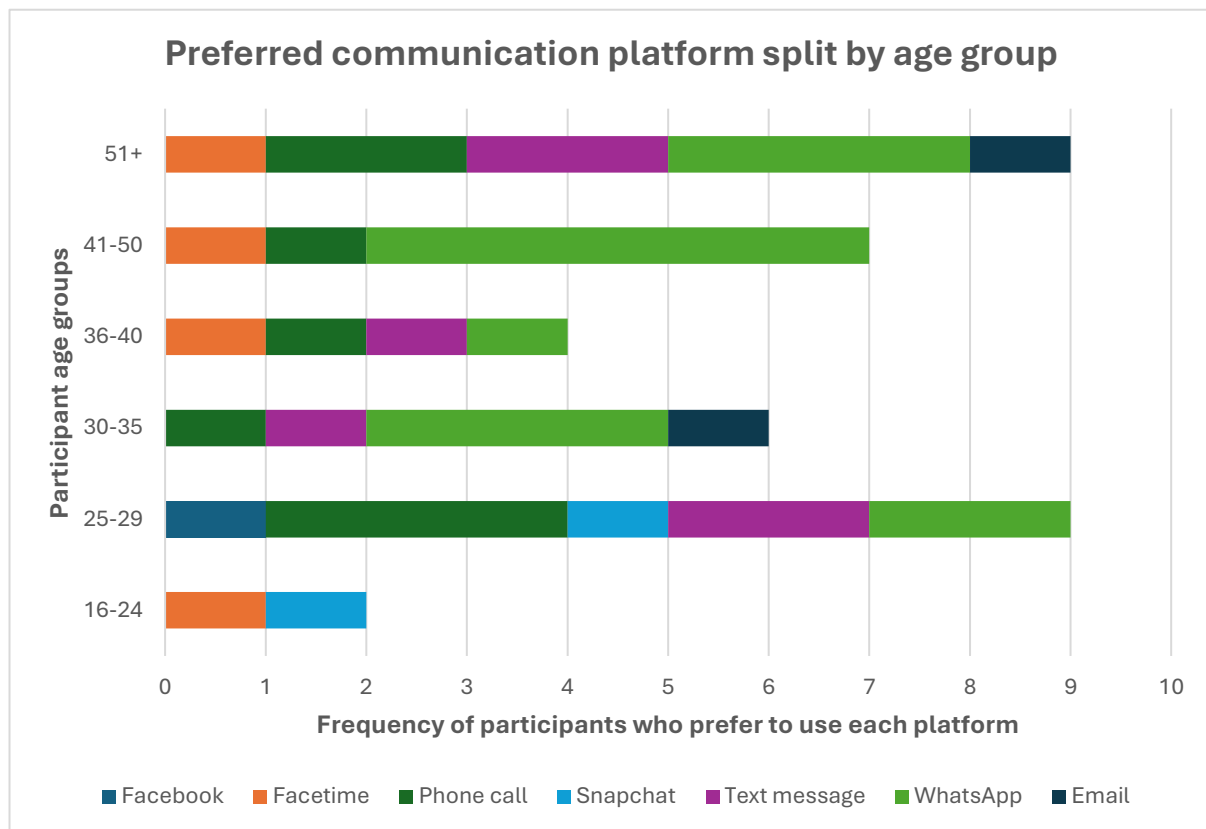


Figure 6.13 provides an overview of the results for preferred platform use when age of participants is considered. Age group splits aligned with the same age groups created in Phase 1. As Figure 6.13 shows there was no distinct pattern of age influencing platform preference for Key Relations communicating with their military person. For example, whilst only 4 participants reported using Facetime to communicate with their military person, these individuals were across a range of age groups. With 1 participant being in both the youngest age group and 1 participant being in the oldest age group. This was similar across most of platform types included in the Figure, except for Snapchat. The data demonstrates that for the rest of these platforms, even though there may not have been 1 participant from each of the age groups who reported this platform as being their preferred choice, the participants that it was their preferred platform were not towards either end of the age scale of the participant group. The only platform that did demonstrate a potential influence of age was Snapchat. Of the two participants who said participant was their preferred platform to use when communicating with their military person, one participant was in the 16–24 years-old age group, and the other was in the 25–29 years-old age group. No participants older than 27 said Snapchat was their preferred communication platform.

**Figure 6.13:**

Graph showing number of participants who's preferred communication platform is Facebook, Facetime, Phone Call, Snapchat, Text Message, WhatsApp or Email, for each age group.



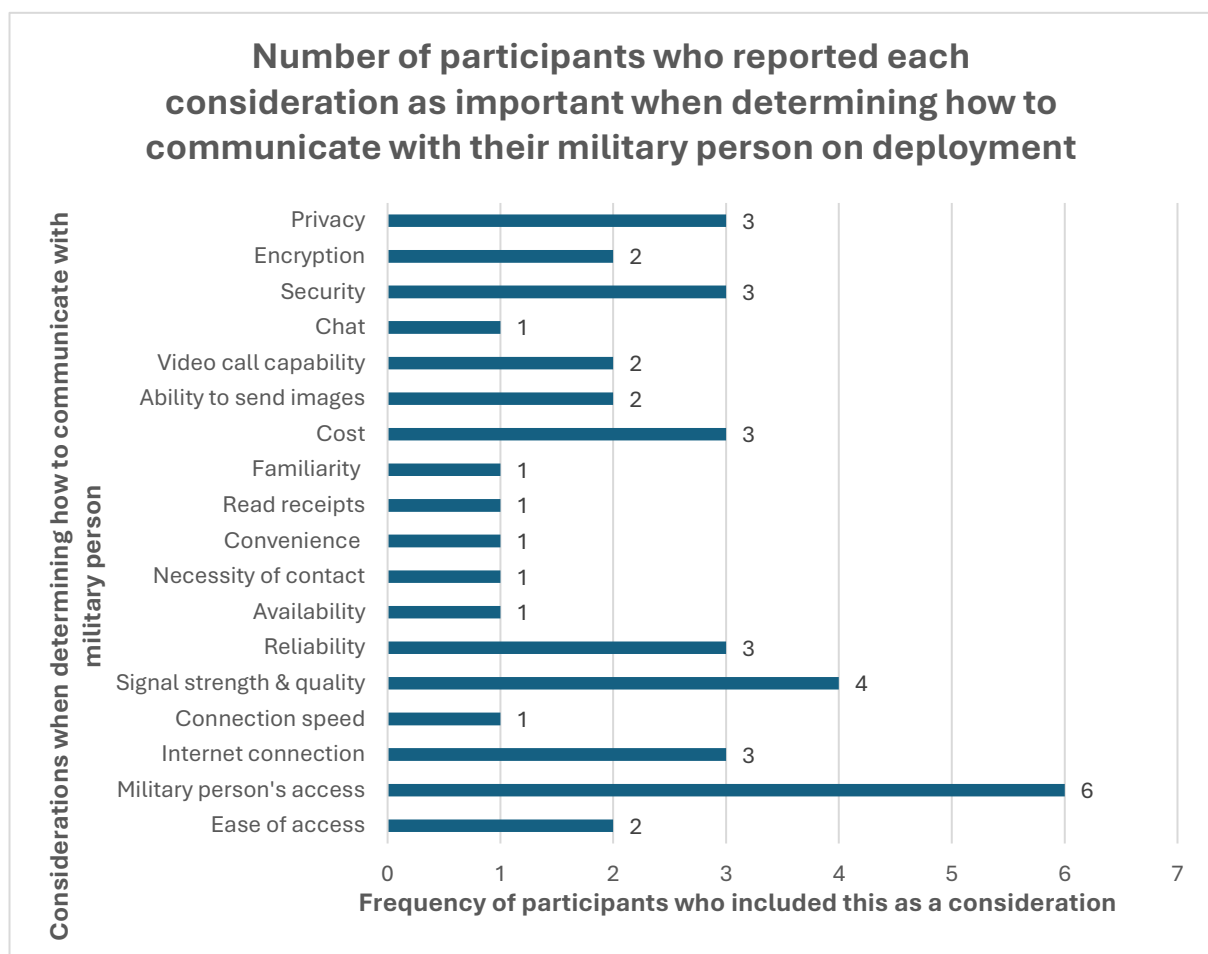
Participants were then presented the opportunity to provide context for their previous answers when asked what their most important consideration is when deciding what platform to use to communicate with their military person. This was a free response question that provided qualitative data, rather than numerical. In total 18 categories were created from participant responses. Figure 6.14 includes the full list of categories that were created as well as the frequency of participants who mentioned this category as a consideration. Figure 6.15 demonstrates that 'Military person's access' was the most frequently reported consideration by participants. This encompassed multiple considerations, including the ability to access the method through military platforms and the access personnel have due to their job requirements. For example, one participant highlighted that as their military person is a submariner, their options are limited when they're underwater. A separate category remained for participant responses where it was unclear whether they meant access for themselves or their military person, termed 'Ease of access'. Whilst the responses were categorised and analysed with frequency analysis, some responses also provide important context as a standalone response. For example, the participant who stated 'Facebook' as their most preferred communication platform in the previous question explained in this free response question that due to the strength of the internet connection Facebook messages are more likely to be received and sent than WhatsApp messages. However, another participant explained that they preferred to use WhatsApp over other platforms because they prefer to video call.



As depicted in Figure 6.14 multiple participants highlighted security as a consideration when choosing what platform to use to communicate with their military person. Three of these responses simply stated that ‘security’ was a consideration, without providing additional information such as specific aspects of security or how they determine whether platforms are secure. However, two participants highlighted that ‘Encrypted communication’ was their only consideration when deciding what platform to use. Of these two participants that mentioned encryption as the most important consideration for platform decisions, one reported their most preferred platform was ‘WhatsApp’ and the other reported ‘Snapchat’ as their most preferred platform when communicating with their military person on deployment.

**Figure 6.14:**

*Graph showing the categories of considerations participants mentioned as being most important when deciding how to communicate with their military person, and the number of participants who mentioned each one.*

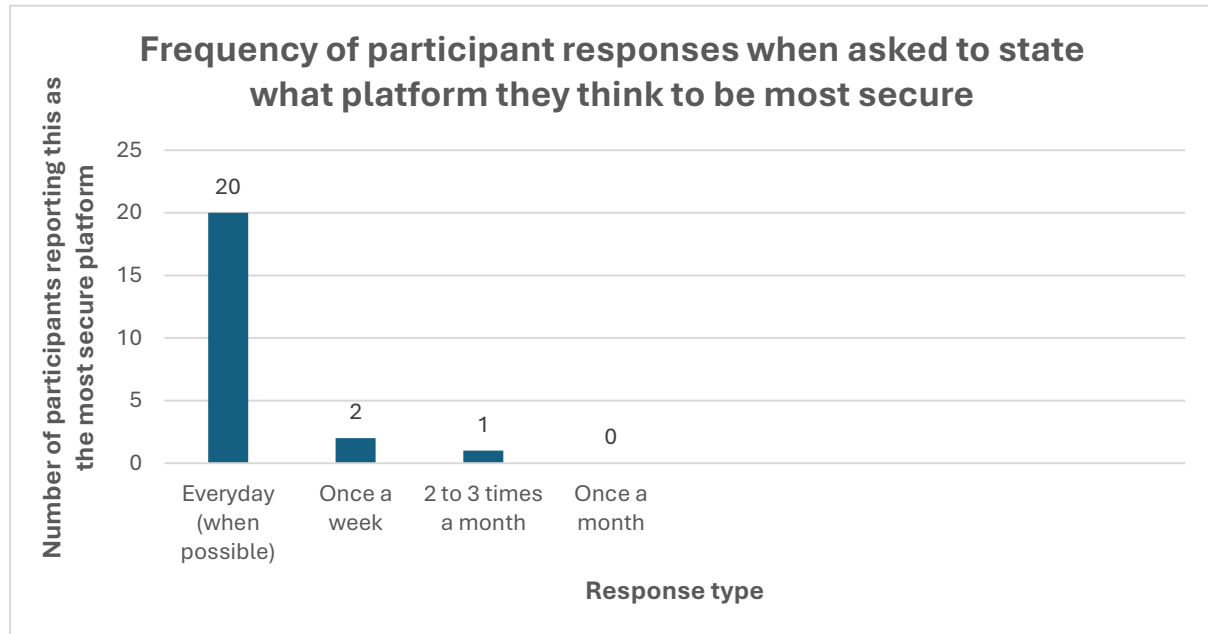


The next question participants were asked focussed specifically on security of online platforms and asked them to identify any platforms they believe to be more secure than others. Three participants responded definitively ‘No’, suggesting they do not believe the platforms to differ in security. Two participants stated uncertainty in their responses, with one stating they perceive that from the military organisation’s perspective none would be secure. Overall, 20 participants reported that they believed WhatsApp to be the most secure platform. Of this 20 that stated WhatsApp as being the most secure, 70% mentioned encryption when asked to justify why they consider this platform more secure. Other justifications included popularity of the

application as well as the ability to set up multi-factor authentication on their devices using biometric authentication methods.

**Figure 6.15:**

*Graph showing how many participants thought these platforms are the most secure*



For participants responding email as the most secure platforms, both participants highlighted this was due to the existing connection with the military organisation, including monitoring of emails from the Navy. Contrastingly one participant explained they thought Facetime was more secure due to having no text so it can't be monitored, screenshot or copied. Three participants reported that they believed Signal to be the most secure platform, with all three justifying their choice by explaining their military person's organisation had recommended the use of this platform over others. Despite Signal being recommended as the platform to use when communicating with military personnel on deployment by military organisations, all three of these participants stated a different platform as their most preferred to use to communicate with their military person. These platforms were Facetime, WhatsApp and Text message, with only one of these participants stating they used Signal at all. None of these participants stated security as their most important consideration when deciding what platform to use to communicate with their military person. Instead they mentioned considerations of cost, signal quality and military person's access.

### 6.3.3. Communication via group messaging

Of the 33 participants who completed the survey, 26 participants responded 'Yes' when asked if they communicate with military friends or relatives in online social media groups. These participants were asked a follow up question to provide more detail about the format of these group chats including platforms used and who is involved. The most frequently mentioned platform was Facebook, with 18 participants stating they use this platform for group communication. Not all participants specified what type of group this was, but at least 1 participant mentioned the use of group pages, community group pages and Facebook messenger groups. Participants frequently mentioned the use of Facebook groups to

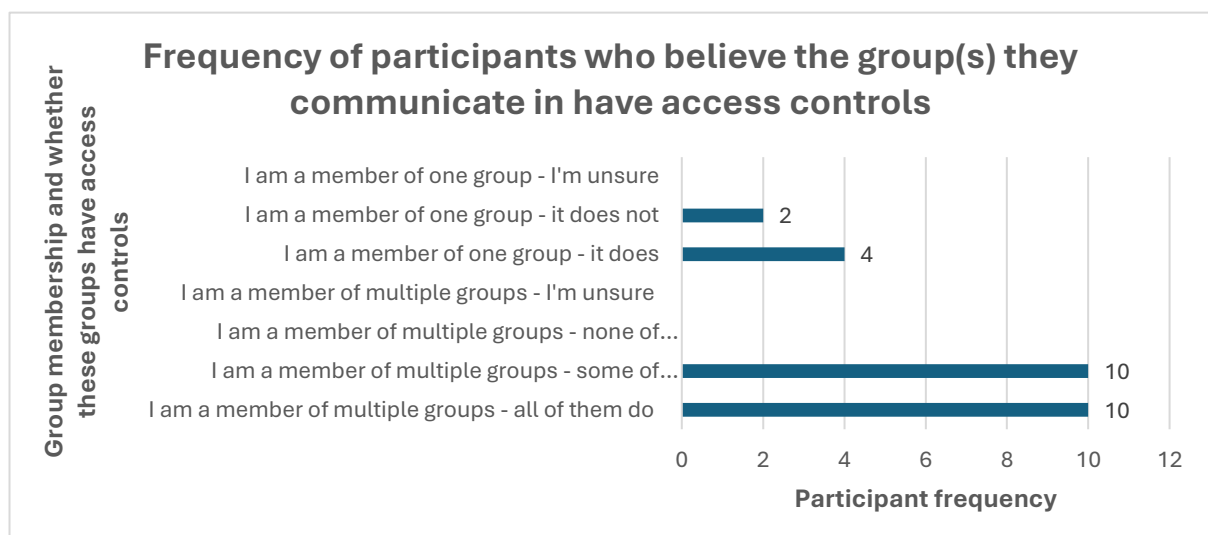
communicate with others in the extended military community. This could be other military partners and spouses, or other families that live on the local military patch. Other social media platforms that participants mentioned have set ups for military families include Instagram and WhatsApp. WhatsApp and Instagram, as well as Snapchat were also platforms participants highlighted as being used to communicate with military friends in a personalised group setting, without being part of a group specifically directed to and created for Military Key Relations. One participant mentioned they were part of a Royal Navy specific online forum that is set up for military families, that allows group communication. The seven participants who responded 'No' when asked if they communicated using group chats were asked to provide more detail about this response. One individual highlighted that they do not use social media groups in any capacity, whether that's in the context of their military person or not. Other responses included a lack of time, simply a lack of necessity to use groups, and the preference to communicate individually.

All participants were asked to detail their knowledge of any measures to monitor group membership and credibility. Twelve participants responded 'None' to indicate they are not aware of any measures that exist for membership monitoring and credibility checking. One participant identified they were an administrator for military family and personnel Facebook and explained they check member credentials to ensure individuals are genuine. This was reiterated by multiple other participants who stated that groups require new members to answer questions to prove their connection to the military or the specific unit or base. Additionally, multiple participants highlighted that some groups only accept membership from new individuals if they have been invited or referred to the group by another existing group member. Responses indicated the level of credibility and admission checks can depend on the information that is included in the group. For example, one participant explained that due to ship movements being posted in one of the groups they are a member of, you can only join the group if you are referred by a friend. For the more personalised groups, such as a small friendship or family circle, participants described that no new members are invited due to the nature of the group.

As Figure 6.16 visualises more participants are members of multiple social media groups, than just one of these groups. This Figure also indicates that at least 12 participants are members of 1 or more groups that do not have measures in place to control access to the group.

**Figure 6.16:**

*Graph showing how many participants are part of one or multiple online groups, and the extent they believe the group(s) monitor access to the group*

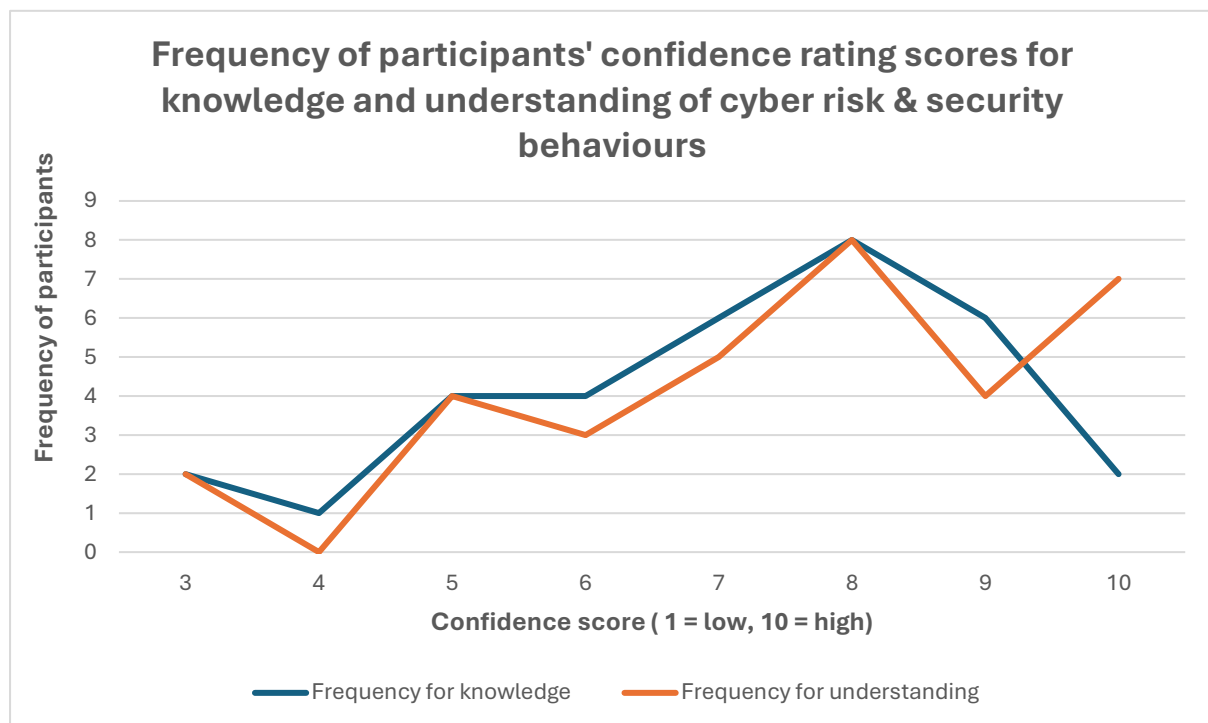


### 6.3.4. Understanding risk behaviours

To provide a baseline for participants' perception of their knowledge and understanding of cyber risk and cybersecurity behaviour they were asked to rate their confidence in both of these concepts, on a scale of 1 (low confidence) to 10 (high confidence). When considering the ratings in confidence for knowledge of cyber risk and security behaviours, participants responded with a mean score of 7.09 (SD = 1.86, Minimum = 3.00, Maximum = 10.00). Participants gave themselves a similar mean score for confidence in their understanding of cyber risk and security behaviours, with a mean score of 9.55 (SD = 2.00, Minimum = 3.00, Maximum = 10.00).

**Figure 6.17:**

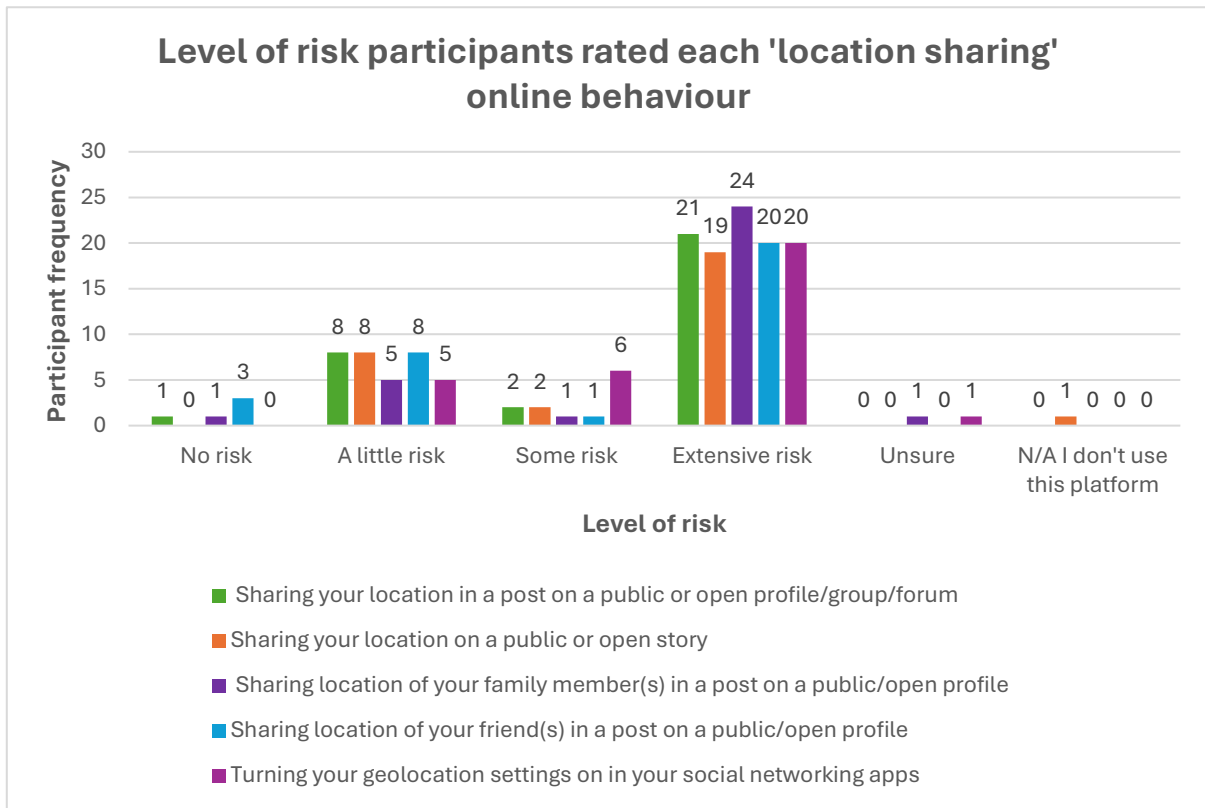
*Graph showing the frequency of scores participants rated their confidence in knowledge and understanding of cyber risk and security behaviours.*



To explore participants' understanding of online risk behaviours in more detail they were provided with a list of potential online risk behaviours and asked to select the extent they believe this behaviour presents a cybersecurity risk. The list of these behaviours can be divided into sub-categories of behaviours including 'Location sharing behaviours and 'Picture tagging behaviours'. As Figure 6.18 shows when considering 'Location sharing behaviours' both of themselves and others, the pattern in the findings suggests that participants considered this an online behaviour associated with a higher level of cyber risk. Comparatively, when asked about 'Picture tagging behaviours' there was a wider dispersion of the level of risk that participants associated with these behaviours, as visualised in Figure 5.18. There was also a higher number of participants who reported uncertainty over the level of risk these behaviours hold. There is a pattern in the findings where behaviours that clearly state information is shared on an open or public platform are associated with greater cyber risk.

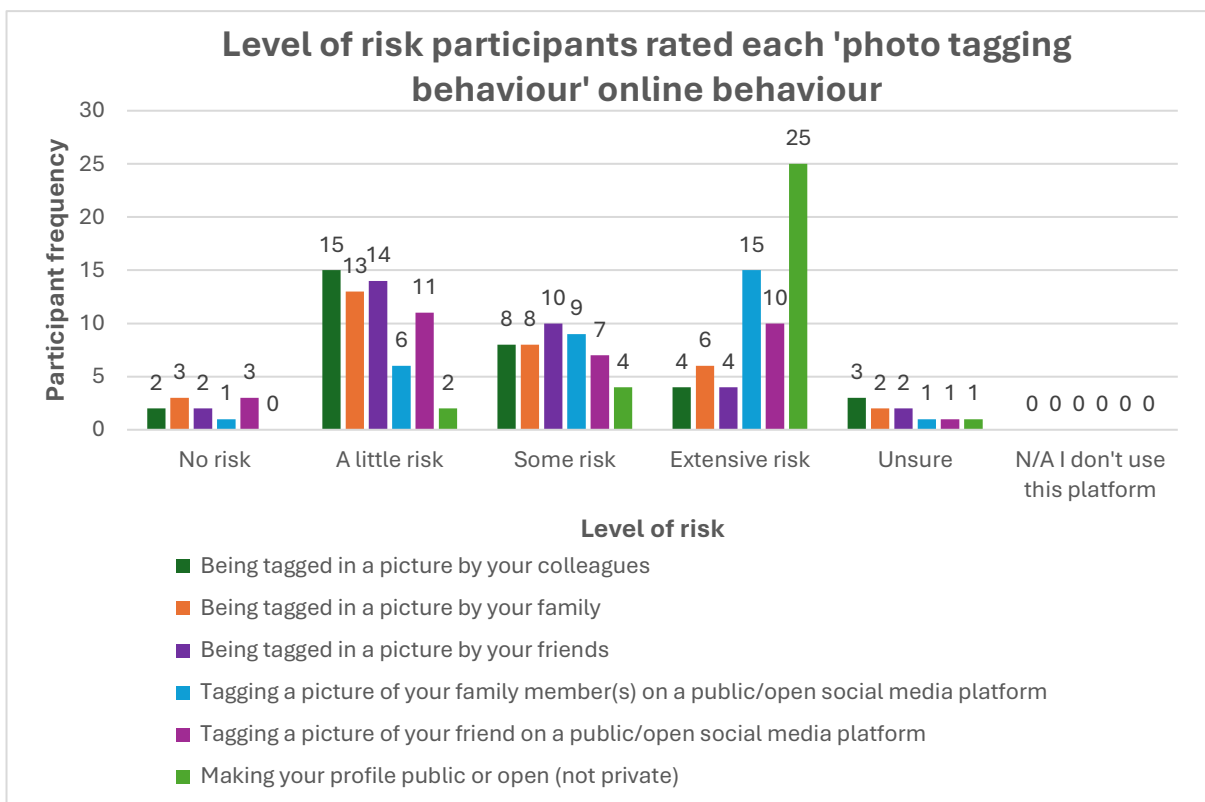
**Figure 6.18:**

Number of participants who rated online 'location behaviours' no risk to extensive risk.



**Figure 6.19:**

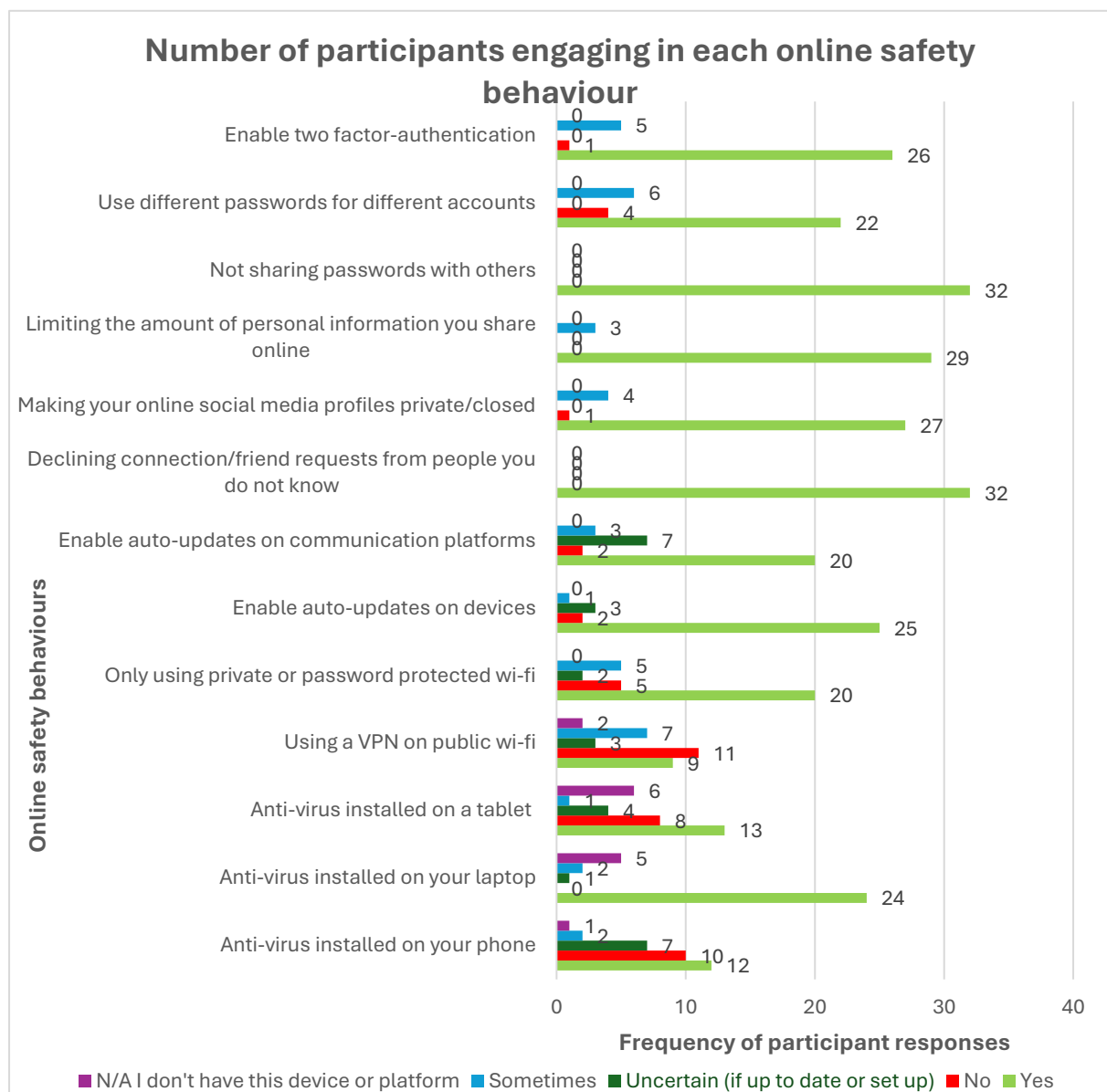
Number of participants who rated online 'location behaviours' no risk to extensive risk.



The next group of questions explored online safety behaviours by providing participants with a list of behaviours and asking them to state the extent to which they apply these behaviours. As Figure 6.19 shows there were some behaviours that participants are not consistently engaging with including using a VPN on public wi-fi and installing anti-virus on their phone or a tablet. Comparatively, double the number of participants said they have anti-virus installed on their laptop. The two behaviours with the highest frequency of participants reporting uncertainty about were installing anti-virus on their phone and enabling auto-updates on communication platforms. Participants reported engaging in most online information sharing safety behaviours. Including not interacting with people they don't know, limiting the amount of information they share online, and making their social media profiles private. Nearly all participants responded they don't share their passwords with others, however a much lower number confirmed they do use different passwords for different accounts. Those that did not confirm this reported they do this sometimes, or not at all.

**Figure 6.20:**

*List of online safety behaviours provided to participants and the frequency of participants who engage in each online safety behaviour*



To begin to gain an insight into participants opinion towards cyber secure behaviours they were asked to rate the extent they think engaging in these behaviours is restrictive on their online behaviour. They were asked to select this on a scale from 1 to 10, with 1 being 'I can behave how I would like, whilst still being safe online, and 10 being 'Engaging in online safety behaviours is restrictive'. Participants responded with a mean score of 4.90 (SD = 2.78, Minimum = 0.00, Maximum = 10.00).

### 6.3.5. Online behaviours in the context of military organisations

The initial question in this section of the survey asked participants to describe any changes they make to their online behaviour when considering the security and safety of their military person and their information. This was a free response question with qualitative data being collected. Nine participants responded that they think they do not make any changes to their behaviour when considering their military person and their information. Overall participants stated it was important to reduce the amount of information that connects their friend or relative to the military. Some responses simply stated no information is shared about their friend or relative at all. Whilst others were more specific in detailing they do not share military related information. Frequently mentioned details that individuals ensure not to share online included pictures of their military person in uniform, deployment location, and service number. Some participants provided justifications for why they limit this information, with one explaining triangulation of information can present a risk, and another explaining the information presents a security risk if the information is not common knowledge. One participant explained they judge the amount of information it is acceptable to share based on press releases from the Navy. Participants also explained any decisions about what is shared online are made by discussing it with their military person first to understand what is appropriate and what they are happy to be shared about their military connection. This included accepting friend requests from mutual connections, personal information such as the military person's rank and, operational information. One participant who identified their military person is their 'Husband, Wife or Civil Partner' highlighted this behaviour extends to their children, as well as their military person. They stated that as well as not highlighting their connection to the military online, pictures of their children in school uniform or on the public school account are not posted either.

Participants were asked to consider the extent their online behaviour influences the safety of their military person from a threat actor. This was asked when considering three different aspects, their military person as an individual, their military person and their unit, and the military person and their military branch as a whole. Participants were asked to rate this on a 10-point scale, with zero being 'No influence at all' and ten being 'My behaviour has a direct influence'. Participants scored all three of these individual aspects of their military person's security from a military adversary similarly. The highest mean score was for considerations of their influence on the safety of their military person at an individual level, with a mean score of 5.78 (SD = 3.13, Minimum = 0.00, Maximum = 10.00). Participants gave only a slightly lower score when considering their military person at a branch level, with a mean score of 5.63 (SD = 3.52, Minimum = 0.00, Maximum = 10.00). The marginally lowest score was for considerations of their military person at a unit level with a mean score of 5.53 (SD = 3.49, Minimum = 0.00, Maximum = 10.00).

### 6.3.6. Training, Education and Awareness

Two participants responded 'Yes' that they had been invited or attended any previous cybersecurity training from a military organisation. When asked to detail this training in the follow up question, one participant identified they also work within the Ministry of Defence and so receives mandatory cybersecurity training. The second participant explained they receive annual cybersecurity training with the Royal Air Force (RAF). This second individual did not state whether this was as part of their own job role or as part of a friends and relatives cybersecurity training initiative.

A higher number of individuals identified they have previously received cybersecurity education and awareness materials from a military organisation, with seven participants responding 'Yes'. Three individuals explained they had received this information as part of their career when working in Defence. Another way one participant received this information is the Deployment Welfare Package, which is a support package provided to personnel deployed overseas to help maintain the physical and mental well-being of personnel, and their friends and relatives. Additionally one participant explained they received general Operations Security (OPSEC) information, from HIVE, a service set up to provide information and welfare support to the extended military community.

When asked if they would attend a cybersecurity briefing specifically for friends and relatives of military persons, 16 responses 'Yes' they would, two responded 'No' they wouldn't and 14 responded 'Perhaps, depending on other factors'. Those that responded 'No' were provided with a follow-up question asking why this is something they would not be interested in. One participant explained training "wouldn't influence" them as they make a judgement on what is safe to share, and the other explained they were "aware" of their own security. Those that responded 'Perhaps, depending on other factors' were not provided this follow up question due to the final question presented to all participants asking them to state any barriers to engagement with future cybersecurity initiatives. The most frequently mentioned barriers by participants were 'Time' and 'Childcare'. Ten participants cited a lack of time as being a barrier to engagement with future initiatives, especially when balancing their own career and looking after children, which is even more strained when their partner is deployed. Nine participants said 'Childcare' was a concern, with multiple participants stating they had just had a baby or are relocated away from family making childcare more challenging. Another frequently mentioned barrier was 'Work commitments', with one participant highlighting that existing military events don't currently consider partners working a full-time job Monday to Friday. One participant provided a potential solution as they explained how they would prefer the information be presented on a website so they could engage with information at their own pace when they have the time and could revisit the information as required. Two participants considered how the format of the training could potentially be a barrier. With one stating they wouldn't want themselves or their military person to be punished if they are not able to attend, and another highlighting how engagement would be dependent on the person delivering the training as they would not like to be patronised. Five participants stated they did not think there were any barriers with one participant stating, "when there's a will, there's a way!".



## 6.4. Phase 3 - Discussion

**Aim 1: Explore how Key Relations report communicating with their military counterparts, including platform usage and frequency.**

The first aim had five research questions which were:

- **Research question 1a:** *Will the type of relationship influence the communication frequency between Key Relations and their military person, with higher communication frequency for partners, parents, children, grandparents, and 'close' friends?*
- **Research question 1b:** *Will platform usage alter with age, with younger participants using social media platforms more than older participants?*
- **Research question 1c:** *Will there be different patterns in platform usage depending on the type of relationship?*
- **Research question 1d:** *How does deployment situation and access limitations influence patterns in platform usage?*
- **Research question 1e:** *Are topics discussed with personnel mainly non-work related, and does this differ from responses in Phase 1 from military personnel due to less pressure to conform to security standards set by military training?*

Addressing research question 1a, it was found that participants who identified their military person as being a 'Husband, Wife or Civil Partner', 'Unmarried Partner', or 'Best Friend' had a modal response for communication regularity of 'Everyday (when possible)'. For the category of 'Child' the modal communication was 'Once a week', which was less than the other types of relationship. However, there was only one participant who identified their military person as this type of relation. For the participant who identified their military person as being a 'Brother or sister', they responded they would contact this person '2 to 3 times a month'. Whilst a brother or sister is not traditionally a next of kin or a dependent, the connection between siblings can still be strong.

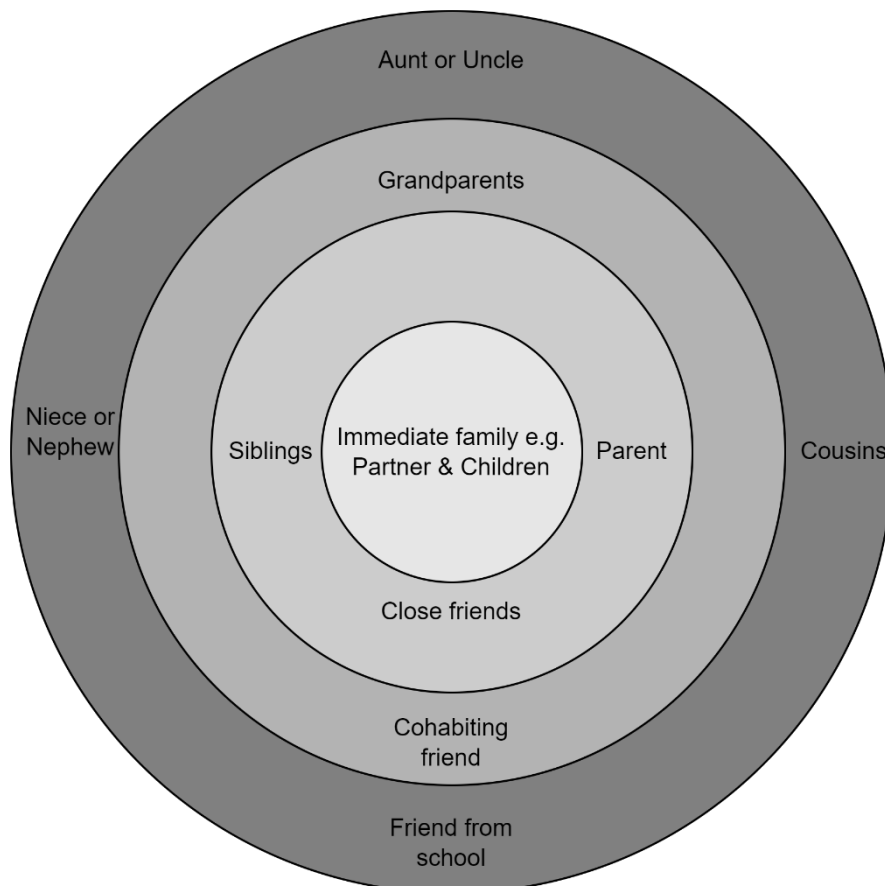
When considering the influence of relationship strength for this survey, those with a mean strength relationship score of less than 10 were a 'Husband, Wife or Civil Partner', 'Unmarried Partner', or 'Best Friend'. Whilst participants would contact these individuals more regularly, the strength of the relationship for 'Brother or Sister', 'Child', and 'Aunt or Uncle' were still very high. Thus providing further support that these individuals should be included in the definition of Military Key Relations and when considering future cybersecurity initiatives. Based on the findings from Phase 3, as well as Phases 1 and 2, Figure 6.21 provides a visual overview for the levels of distance for Key Relations. The Figure mainly bases distance of relations on the percentage of people who mentioned these types of Key Relations in Phases 1 and 2, and the percentage of participants who were this type of relation in Phase 3. However, it also takes into account relationship strength scores and communication regularity responses from all three Phases.

Nonetheless, research question 1a cannot be fully explored due to the participant sample not including the full range of relationships, including the most distant relations. The current sample mainly consists of Husbands, wives and civil partners, and so even for those relations that were included in the findings, it would be beneficial to have more context to fully understand this potential influence of relationship type on communication regularity. There were

no participants who identified their military person as being a 'Parent' or 'Grandparent', and this could have been due to participants needing to be older than 16 years old to take part in the survey. This reduces the chance participants would have grandparents still serving in the military. Particularly when the average age of becoming a grandparent is 63 in the UK (Office for National Statistics, 2019), and the normal retirement age for service personnel is 55 years old (Ministry of Defence, 2013). The influence of age does not necessarily provide an explanation for the lack of participants with a 'Parent' as their military person. An alternative explanation could be due to recruitment methods for the survey. The survey was distributed via Facebook groups for military families, as well as community centres for military personnel. Both of these methods may not naturally attract individuals who are 16 as support may be found in other areas, such as school. The survey was also distributed by Dstl Military Advisors to personnel who were asked to forward it on to their Key Relations if they deemed it appropriate. Parents can be reluctant to encourage their children to participate in research for reasons such as there being no direct benefit to the child, a general lack of trust in research and the potential risks to their child (Nathe et al. 2023). Therefore, when deciding who to share the study with, military personnel may have made the decision to not share it with their children due to these concerns, amongst others and shared it with a partner on the basis they would be able to make a more considered decision about their own participation. This explanation has credibility due to the high proportion of participants in the survey being a 'Husband, Wife or Civil Partner' or an 'Unmarried Partner' and the lack of participants being more distant relatives and friends.

**Figure 6.21:**

*Diagram depicting the level of 'closeness' to military personnel each key relation type has. The further out the circle level, the more distant a relation is to the military person.*



Research questions 1b, 1c and 1d for Aim 1 dealt with variations in platform usage. The aim of exploring platform usage was to identify any risk behaviours that could be presented on these platforms and where to direct future cybersecurity initiatives to address potential risk behaviours. Overall WhatsApp was the most frequently used platform, and also the most preferred platform to be used by participants, when not considering any additional factors. This is consistent with Phase 1, which also found WhatsApp to be the most frequently preferred platform when military personnel communicate with their Key Relations. As well as WhatsApp being the most frequently used platform for Key Relations to communicate with their military person, many participants mentioned how they use social media platforms Facebook, WhatsApp, and Instagram for group communication. Whilst some identified it was with their friendship group their military person was a part of, the majority of participants used these groups to communicate with other military partners, and other families living on military patches. Group communication appears to create a sense of community within the extended military community, which aligns with previous research on Military Key Relations. This research identified that interacting with other military families can be beneficial in reducing the negative effects of challenges that Military Key Relations experience such as relocation and separation from their military person (Rea et al. 2015; Meadows et al. 2017).

One consideration for the responses from this thesis is the question wording, and how participants interpreted what the questions asked them to do. As discussed in [Section 6.1.3.](#), two questions were altered to make the intention of the question clearer. These questions were split with one exploring what platforms participants use to communicate with their military person, and the other question aiming to understand which platforms they prefer to use. Despite participants being asked to score platforms they do not use to communicate with their military person a “0”, in the preference ranking question, some still rated these platforms, despite not reporting they used the platform in the previous question. It is not possible to understand why participants responded in the way they did, if the question responses contradict themselves. Therefore the questions were analysed separately, as intended, and the results presented separately, with the acknowledgement this question should be further refined in future research. This could be asked in the focus groups that could be conducted as part of the wider programme of research, outside of the PhD project, following submission of the thesis.

When looking at additional factors, research question 1b predicted: *Patterns in platform usage will depend on age, with younger participants using social media platforms more than older participants.* There is some support that platform usage is influenced by age when looking at Snapchat usage. Snapchat is the only platform with a pattern where those who used the platform were of a younger age. Of those aged 16-24, 100% of participants use snapchat, and of the 25-29-year-old group, 50% use snapchat. However, it is important to note that there were only two participants in the 16-24 years old age group compared with nine in the 25-29 years old age group. No participants in any of the other age groups reported using snapchat. For two participants they identified their most preferred platform when communicating with their military person would be ‘Snapchat’. These participants were 22 and 27 years old, with their military people being a ‘Husband, Wife or Civil Partner’ and ‘Unmarried partner’, respectively. Aside from Snapchat, there were no other clear patterns in the data that suggest age influenced what communication platforms people Military Key Relations prefer to use. However, when looking at general usage of communication platforms, the age group of participants aged 51 years old and over consistently did not use social media platforms other than WhatsApp. 100% of this age group did not use Facebook, Instagram, Snapchat and Twitter. Comparatively, within the other age groups, this pattern was not as clear, with varying percentages of participants using each

platform. This is consistent with trends in existing research that state as individuals get older, the smaller percentage of those individuals report using social media sites (Auxier and Anderson, 2021). However, Auxier et al. (2021) also suggest that the use of Facebook was used a similar amount regardless of age, which is inconsistent with the findings from the current study. This current thesis mainly focussed on the use of communication platforms when communicating with their military person, with some participants discussing communication with the extended military community in the group communication question. However, the survey did not include any questions which asked participants about their platform usage when engaging with online platforms. As the findings from Phase 2 identified, online risk behaviours presented by Military Key Relations may occur as a result of sharing a social media post, a story, or sharing images, and not solely when communicating with their military person. Whilst this survey begins to explore cyber risk behaviours when engaging in these information sharing behaviours in questions further on in the survey, these are not detailed enough to provide insight into behaviours on specific platforms. For example, no participants in this survey responded they communicate with their military person on BeReal. However, the nature of BeReal focuses on sharing images to your entire network, and so there is the potential that Key Relations may inadvertently share sensitive military information, without being in direct communication with their military person. The use of platforms in a variety of contexts is something that should be explored in future research. This will ensure future cybersecurity initiatives are relevant to Military Key Relations by addressing the specific online behaviours they engage in.

Addressing research question 1c: *Research question 1c: Patterns in platform usage will depend on relationship type. Children and parents will be more likely to video or voice call rather than message.* It is difficult to determine if the results demonstrate a clear pattern of relationship type influencing platform choice, due to the number of participants mainly identifying their military person as a 'Husband, Wife or Civil Partner'. The one participant who identified their military person as a 'Child' did identify their preferred method of communicating with this individual would be using WhatsApp. As WhatsApp has the capability to both video and voice call, this does provide support for research question 1c.

Due to my experience as an academic researcher rather than working or living in a military environment, participants were invited to participate in the research by an external researcher. This potentially limits the rapport a researcher can build with participants (Chavez, 2008), as individuals within the military community have shared experiences and understanding of military life (Kirke, 2012). Additionally, a researcher who is an "insider" may find it easier to access existing spaces (Chavez, 2008), particularly within the military community to provide more insight on where to direct recruitment materials to a wide range of individuals. Future work would benefit from exploring this topic further from an insider's perspective by someone recognised in a military role, to access a wider range of participants to explore a wider range of experiences and opinions and provide further insight into this area.

There is support for the research question 1d, that situational factors such as deployment access, will influence patterns in platform usage. Qualitative responses provided in the question that asked participants about what their most important consideration was when deciding how to communicate with their military person, supports research question 1d. 'Military person's access' was the most frequent category of response for this question. This addressed how the situation of their military person's deployment influenced the level of access they had to certain platforms or networks. One participant highlighted that due to the nature of their military person's role as a submariner, they communicate via 'Familygram' which allows them to send

messages whilst the submarine is underwater. Multiple other considerations reported by participants indirectly consider the role of the military person's deployment situation. These include 'Signal strength and quality', 'Cost' and 'Internet connection'. All of these considerations may be affected by where and how long the military person is deployed for. Whilst factors such as the ability to send images or video call, was important for participants, the overarching consideration was how to effectively make contact with their military person in a way that is not restricted by the requirements of a military deployment. This priority of considerations may explain why relationship type did not appear to influence platform usage, as all Military Key Relations prioritise communicating with their military person, in whatever way they can. This is consistent with findings from Phase 1, when military personnel were asked the same question, but from the opposite perspective of being deployed and contacting those at home. The most frequent consideration from participants was 'Ease of use'. This suggests military personnel and their Key Relations balance each other's requirements to ensure effective communication. In the context of military cyber resilience, this prioritisation of military personnel wanting to make it easy for their Key Relations to contact them may result in them using methods of communication they know are less secure but are effective when considering other challenges such as internet access or cost. In Phase 2, participants highlighted that military personnel are discouraged to use WhatsApp due to the security vulnerabilities of the platform. However, findings from Phase 1 and Phase 3 provide evidence that the most frequent and the most preferred communication platform for military personnel and Military Key Relations to communicate with each other, is WhatsApp.

As highlighted these questions aimed to explore any potential online risk behaviours of Military Key Relations in their communication habits. It is important for organisations with a strong Cybersecurity Culture to incorporate the requirements of stakeholders in the organisation so that individuals do not circumvent cybersecurity policy to facilitate their communication goals. Uchendu et al. (2021) identified that management support is one of the key factors in building and maintaining a positive Cybersecurity Culture in an organisation. Individuals who feel supported by an organisation are reciprocal in their commitment to the organisation (Safa & Solms, 2016). So ensuring that Military Key Relations, as well as military personnel, are considered when creating cybersecurity policy and distributing materials in future cybersecurity initiatives is important for fostering cyber resilient military organisations.

## Aim 2: Gather perspectives on what Key Relations believe their online vulnerabilities to be for military organisations.

Aim two consisted of one research question:

- **Research question 2:** *Are there differences in level of understanding of vulnerability and how this might impact military organisations within Key Relations?*

Two questions focussed specifically on participants' knowledge and understanding of cyber risk and security behaviours. The responses from these questions do support research question 2, in that participants provided a range of scores on their confidence in these areas. The lowest confidence score participants gave themselves was a 3, of which two participants rated this for both knowledge and understanding. This is much lower than the mean scores for both understanding and knowledge, at 7.09 and 9.55 respectively. However, there were six participants who rated the confidence in their knowledge a 10, and seven who rated the confidence in their understanding a 10. The variability between the mean scores for knowledge

at 9.55 and understanding at 7.09 suggests that whilst participants may believe that their knowledge is not as in-depth as it could be, participants are confident in understanding what they do know. This further justifies the requirement for providing Military Key Relations the opportunity to access Cybersecurity materials to ensure they are aware of the potential risk of their online behaviours, and how they can protect important information by engaging in cybersecurity behaviours.

The level of understanding Military Key Relations have may also be dependent on the type of behaviour being discussed. When provided with a list of potential risk behaviours, participants showed more discrepancy in their responses about 'picture tagging behaviours' such as being tagged in a picture or tagging others in a picture, compared to 'information sharing behaviours', which they mostly classified as having a high risk. Participants also reported more uncertainty in 'photo tagging behaviours'. This may have been due to questions not specifically mentioning the military, and so resulting in uncertainty. When participants were asked specifically about altering their behaviours to ensure the safety of their military person and their information, participants frequently mentioned they do not share pictures of their military person in uniform. This supports research question 2 as it suggests that participants do consider how sharing a picture of the military person in uniform could present a vulnerability that influences the military person and their organisation.

Findings from the survey provide evidence suggesting Military Key Relations are also conscious of their online vulnerability when communicating with their military person. When participants were asked what their most important consideration is when deciding how to communicate with their military person, eight participants mentioned something about privacy or security. As highlighted in the Chapter 1 and Chapter 4, distinguishing privacy and security is important. As privacy focuses more on determining who should have access to information (Bambauer, 2013), participants who mentioned privacy could have been intending to convey various points. For example, it may have been they desire privacy from the military organisation not viewing their communication, or privacy from other military personnel. However, they could also have meant privacy from potential bad actors, which strays more into security. Three participants distinctly mentioned 'Security' as a consideration but did not go into any more detail about what aspects of security they are particularly conscious of. As the beginning of the survey clearly discussed the aims of the research and was titled to reflect the research was exploring cybersecurity participants could have been displaying demand characteristics when responding to this question. Whilst this can be challenging to avoid, a future study as part of this research aims to explore these topics in more detail with Military Key Relations, in a focus group context. In a focus group, researchers will be able to ask follow-up questions about what participants mean when they say 'Security' or 'Privacy' to determine the extent Military Key Relations understand these concepts.

Two participants did provide a slightly more in-depth answer when asked what their main consideration was by mentioning 'Encrypted communication' and 'End-to-end encryption'. This was also the most frequent response in the following question which asked participants to explain why they think certain communication platforms are more secure than others. The majority of participants in this instance identified they were talking about 'WhatsApp' when considering the security of encrypted communication. WhatsApp and other social media platforms, such as iMessage, introduced end-to-end encryption to mitigate the scrutiny of the privacy of these platforms (Chase et al. 2019). Whilst WhatsApp is generally recommended as one of the more secure communication platforms when considering the introduction of this end-

to-end encryption for users (Wankhede, 2024). Research into the platform suggests users often do not use encryption verification methods set up by WhatsApp and explains the encryption may still be susceptible to security threats such as Man-in-the-Middle attacks (Chase et al. 2019). MITM attacks occur when an attacker intercepts the communication between two endpoints, such as a laptop user and a Wi-Fi router, and modifies or replaces the data being sent between the two endpoints (Bhushan et al. 2017). Whilst this may not be as much of a security concern for the everyday user, these vulnerabilities may be one reason military organisations discourage the use of WhatsApp by personnel and their Key Relations. As highlighted in Phase 2 in discussions with subject matter experts and military personnel, Signal is recommended over WhatsApp by the Ministry of Defence due to its security. Three participants in the survey did identify Signal as being the most secure platform, with these individuals highlighting their military person's organisation had recommended the use of Signal as part of the Security Operating Procedure. This provides support for Research question 2, in that participants have an understanding of how they should behave online in relation to the impact on military organisations. However, only one of these participants reported actually using Signal to communicate with their military person, and still reported that their most preferred platform to communicate with their military person would be WhatsApp. This suggests that even though Military Key Relations may have the knowledge and understanding of how their online vulnerability contributes to military cyber resilience, and consequently how to reduce the risk they present, they still may not engage in safer online behaviours. A branch of the theory of planned behaviour (Ajzen et al., 2011), the knowledge-attitude-behavioural (KAB) model suggests that as individuals' knowledge of cybersecurity behaviours increases, their attitude towards these behaviours also improves, resulting in adoption of cybersecurity behaviours (Parsons et al. 2017). However, the knowing-doing gap suggests that even though individuals may possess knowledge about secure online behaviours, they may not always engage with them (Gundu et al. 2019). The survey in the current thesis did not explore attitudes and therefore it is not possible to determine whether this played a role in the behavioural decisions of participants. However, as discussed in Aim 1, multiple factors come into consideration when Key Relations and their military personnel are deciding how to communicate with each other. The participant who identified Signal as the most secure platform and stated they prefer to use WhatsApp, despite using Signal sometimes, reported 'Cost' as their most important consideration when deciding what platform to use. Sasse et al. (2001) identified that if security measures conflict with the users' goals and requirements for effective communication, then security is demoted to a secondary consideration. This is supported by survey results indicating that some participants find engaging in security behaviours being restrictive on their online behaviour. Whilst only one participant gave a rating of 10 to indicate they find security behaviours too restrictive, the most frequent response from participants was a rating of 5, 'Online safety is restrictive on some behaviours'. These findings link to a Phase 2 sub-theme: *Barriers to engaging in secure behaviours*. This sub-theme highlighted participants' experiences of Key Relations reverting to insecure behaviours online, particularly using less secure platforms if the functionality of the recommended secure platform hinders their ability to communicate effectively with their military person.

In future research with Military Key Relations questions should focus on attempting to understand the goals and requirements of Military Key Relations, to comprehend why individuals choose to use WhatsApp over other similar applications such as Signal. This then would provide those creating cybersecurity policy, as well as future cybersecurity training, education and awareness initiatives the insight to address potential risk behaviours from Military Key Relations.

Incorporating Key Relations' requirements, whilst still addressing risk behaviours, can encourage Military Key Relations to adopt secure online behaviours (Pollini et al. 2021), and reduce the potential exposure to cybersecurity risk for military organisations. Leenen and van Vuuren (2019) explain how the gap between Cybersecurity Culture and military culture can become challenging when cyber experts are brought into a military context. Adopting an Interactive Management approach in future research in this area may be beneficial in addressing the requirements of stakeholders for this particular challenge of addressing the role of the extended military community in military cyber resilience. Research can facilitate a discussion between stakeholders including cybersecurity professionals, military representatives and Military Key Relations, to address the problem in a way that is beneficial to all stakeholders (Ward et al. 2017). The use of different approaches also addresses the concern highlighted that research into Cybersecurity Culture often uses surveys and questionnaires, with a requirement for more dynamic methods (Uchendu et al. 2021).

In further support of Research question 2, the results from the survey do begin to suggest some participants have a more in-depth understanding than others about how their online behaviour impacts their military person. When asked about any changes participants make to their behaviour, some were more detailed than others. For example, using the phrase "triangulation" and outlining they do not share specific topics online about their military person such as location, military uniform pictures and other operational information. Others simply stated they do not share anything military-related about their military person, or that they do not share anything about this individual online at all. Considering the mean scores provided by participants when asked to rate the extent their online behaviour influences their military person at an individual, unit and branch level (5.78, 5.53 and 5.63 respectively). This suggests on average participants believe their online behaviour to have an influence on the safety of their military person and the military organisation in some way. Only two participants responded they do not believe their behaviour has an impact at all on their military person's unit and branch. One participant also scored zero to indicate they do not believe their behaviour influences their military person as an individual. Despite these two participants, these findings suggest the majority of Military Key Relations know that their behaviour impacts military cyber resilience.

As explored throughout the thesis, a key element of Cybersecurity Culture being considered is the role of responsibility, particularly in combination with accountability. Responsibility in Cybersecurity Culture involves ensuring all stakeholders are aware of their role within the organisation (Nel & Drevin, 2019). For this thesis, that includes the Military Key Relations. Often within cybersecurity individuals do not perceive responsibility for cybersecurity and information safety the priority of anyone except cybersecurity specialists. However, this can often result in individuals not understanding the influence their behaviour has and leaving an organisation vulnerable to cybersecurity threats (Ramachandran et al. 2012). To ensure that military organisations reduce potential vulnerabilities to organisational cyber resilience, cybersecurity and information security should be approached holistically, and include Military Key Relations. As identified in Phase 2, Military Key Relations have the potential to behave in a way online that could be targeted by a military adversary, and negatively impact military organisational cyber resilience. Future cybersecurity initiatives should explain to Military Key Relations the extent their behaviour influences the safety of their military person as an individual, but also other aspects of the military whole force, in a way that prioritises the safety of their serving person. This awareness of responsibility can contribute to a Cybersecurity Culture in a way that positively influences military cyber resilience.



### Aim 3: Explore current experiences and opinions of cybersecurity training, education, and awareness materials for Key Relations provided by military organisations.

Aim three has three separate research questions, these are:

- **Research question 3a:** *To what extent do Key Relations rely on their own cybersecurity knowledge and training, as opposed to that provided by military organisations, to keep information safe online?*
- **Research question 3b:** *Do Key Relations receive cybersecurity awareness materials at times of operational significance such as deployment or relocation?*
- **Research question 3c:** *How do barriers to participation such as relocation and fear of asking for help influence Key Relations' reluctance towards future cybersecurity initiatives?*

The first one, *Research question 3a*, focussed on Military Key Relations' existing cybersecurity knowledge. This research question addressed the reliance from Military Key Relations on their own cybersecurity knowledge from everyday life, or from training in their own careers, rather than as a military key relation. Findings from the survey provide for support Research question 3a as only two participants identified they receive cybersecurity training from a military organisation, and one of these highlighted this was a result of being employed by the Ministry of Defence. The other participant explained they receive annual cybersecurity training with the RAF but did not explain why they receive that. Therefore, there is the potential they also are attending annual training as a part of a job within the RAF. As identified in Phase 2 of the research, ensuring Military Key Relations are aware of all the military information that should not be shared online is important, as it may not be second nature to all Key Relations. Even Military Key Relations who receive cybersecurity training in their own careers may not receive all the information required to keep their military person's information safe online. It is in the best interest of military organisations to reduce any potential cybersecurity vulnerabilities in the extended military community due to the impact. Consequences of a successful attack from an adversary due to information shared online can include ineffective or intercepted communication channels, weapon or other system failures, and data corruption (Defense Science Board, 2013). A negative impact on all of these factors within an operational context may ultimately result in a loss of life. Therefore, ensuring that all Military Key Relations are provided the opportunity to access cybersecurity materials in a military context is important in reducing any potential vulnerabilities from Key Relations' online behaviours.

In the survey, 48.49% of participants highlighted they would attend an annual cybersecurity brief provided to Military Key Relations by a military organisation. With 42.42% saying they might attend depending on other factors. This provides initial evidence to suggest that investment in providing Military Key Relations with cybersecurity materials, would be well received, as long as it is provided in an effective manner. Future cybersecurity initiatives for Military Key Relations should consider barriers to participation such as lack of time, as well as childcare responsibilities. In academia there is the suggestion that planning more family-friends events such as providing financial support for childcare or arranging this onsite would be beneficial in increasing attendance at academic events such as conferences (Calisi, 2018). This research explains this would be beneficial for women, but also for single-parent families, which is relevant for many of the extended military community. For military families, this may also

provide the socialisation opportunity for children to receive support from peers with shared experiences of being a military child that reduce the negative effects of the military lifestyle, such as relocation (Meadows et al. 2017). Additionally, participants were concerned about the impact to their military person and ensuring that any decision to participate or not would not reflect negatively on their military person. This aligns with barriers to participation from Military Key Relations explored in previous research, where Key Relations are concerned about their behaviour impacting their military person due to informally carrying the military rank of this individual (Drummet et al. 2003).

Two participants responded they would not attend training, and justified this response by explaining they thought their current cybersecurity knowledge was sufficient. Whilst this may be accurate, there is also the potential these participants are displaying optimism bias. Wherein, they have underestimated the risk of their online behaviours, and are overconfident in their abilities to be able to deal with a cyber incident should one occur (Alnifie & Kim, 2023). Whilst it is not possible to enforce Military Key Relations to engage with cybersecurity initiatives, future cybersecurity initiatives should invite all Military Key Relations to engage in a way that demonstrates it is beneficial for themselves, and for the safety of their military person.

The second research question for Aim 3, *Research question 3b*, predicted: *Some relatives receive cybersecurity awareness materials because of military personnel deployment or military relocation, but not at other times*. This research question is partly supported as only seven participants reported receiving cybersecurity education and awareness materials from military organisations, and one of these was as part of a Deployment Welfare Package. However, this research question is not entirely supported as participants also reported receiving this information from military services such as HIVE information centres. Military Key Relations, as well as personnel are able to access information from HIVEs at any time, and they provide a range of information including about schooling and housing, as well as information about relocation and deployment (The British Army, 2024).

These findings demonstrate the current approach to cybersecurity training, education and awareness for Military Key Relations is limited. This research identified how the definition of Key Relations should be broader to ensure future initiatives are accessed by the appropriate audience. Furthermore, the findings demonstrate that even dependents such as spouses, are not consistently receiving cybersecurity materials. The limitations of the current approach potentially increases the opportunity Key Relations may inadvertently engage in risk behaviours detrimental to military cyber resilience. The recommendation from this phase is for military organisations to provide Military Key Relations the option to access cybersecurity materials. These materials should focus on identifying the military information that should not be shared online and providing basic cybersecurity education on how to best protect themselves online. Any future initiatives should also consider the potential barriers to Key Relations engaging with materials. Recommendations to circumvent these barriers include providing this information online, in a format that means Key Relations are able to access it in their own time and refer back to it when possible. Additionally, any information that cannot be shared online should be disseminated at events that provide childcare, and at a variety of times to consider those who work full-time jobs or have other family care commitments.

## 6.5. Key takeaway points from Phase 3

The findings from Phase 3 continue to support the definition of Military Key Relations as outlined in Phases 1 and 2. However, Phase 3 expands on this definition to suggest that there

may be varying levels of distance for Key Relations as demonstrated in Figure 5.22. Whilst the perception of closeness between Military personnel and Military Key Relations may vary between type of relation, the level of importance in including the friends and relatives listed as Key Relations when considering military cyber resilience does not vary. Findings suggest that relationship strength and communication regularity may be influential in determining distance between military person and their type of relation. Therefore, there is the potential that online vulnerability from Military Key Relations through sharing sensitive operational information online, may be presented by any of these Military Key Relations, regardless of distance of relationship. Whilst this Phase did not demonstrate any clear influence of age and relationship type on platform usage behaviour of Key Relations, it does appear that Military Key Relations consider their military persons' deployment situation, such as access to the internet, when deciding how to communicate.

This Phase provided evidence to suggest that uncertainty exists for some Military Key Relations over cyber risk and security behaviours, though most are aware that their online behaviour does influence their military person and the military organisation to some extent. The potential lack of confidence in Military Key Relations' understanding of online risk and cybersecurity behaviours may be due to the fact that the majority have not had any form of cybersecurity training, education or awareness provided to them by a military organisation. The findings present evidence that a gap does exist in providing Military Key Relations sufficient insight into why and how they can protect military information when online. The findings also indicate that if this gap is addressed through a cybersecurity initiative for Military Key Relations, they would engage as long as it considers potential barriers such as childcare, their own work schedules, and the location.

Whilst this survey provides an initial insight into the experiences and opinions of Military Key Relations themselves, future work would benefit from engaging with a larger population sample of Key Relations, across a wider variety of types of relation. This will help provide further understanding as to whether patterns identified in this Phase, are still apparent when considering different perspectives, in addition to focus groups, to understand why responses were given.

# Chapter 7: Discussion

## 7.1. Chapter Introduction

This thesis aimed to answer the research problem: How do Friends and Relatives contribute to Cyber Resilience within Military Organisations? Considering the role of Military Key Relations in cyber resilience is important due to the potential vulnerability that their online behaviours could present to national security. Whilst keeping information safe online is important for most organisations, within a military context, the risk of sharing confidential information online has potential implications for personnel safety. Sensitive information in the hands of a threat actor can affect the operational success which in some situations could result in fatalities. However, there is a gap in the literature which does not currently consider the extent Military Key Relations impact military cyber resilience. This includes exploring the online behaviours that could result in an online vulnerability and exploring the extent of their knowledge and understanding of online safety, in a military context.

This research problem and the gap in the literature were addressed in this thesis through three separate but interrelated studies, Phase 1, Phase 2 and Phase 3. The previous chapters of this thesis have outlined the results of each Phase and addressed the individual aims and research questions of each Phase individually, bringing in findings from other Phases where appropriate. Phase 1, as discussed in Chapter 4 explored the opinions of military personnel through an online survey. This phase created an initial definition of Military Key Relations, identifying that friends and extended family members should be considered alongside dependents. In Chapter 5, Phase 2 explored the perspectives of military personnel in more depth, alongside the opinions of subject matter experts in cyber education & awareness and cyber incident reporting & monitoring in defence, with semi-structured interviews. These interviews provided further insight into potential online behaviours that Key Relations could engage in that could present a risk to military cyber resilience, mainly focussing on sharing operational information such as location, dates and times. Additionally, the themes from the thematic analysis identified limited existing cybersecurity training, education and awareness provided to Key Relations to ensure they are not engaging in those cyber risk behaviours. In Chapter 6, Phase 3 provided an insight into these themes from the insight of Military Key Relations, through an online survey. This phase confirmed that whilst Key Relations have a varied understanding of cybersecurity risk and safety behaviours, many are not provided with the cybersecurity materials to ensure their online behaviours are not detrimental to military cyber resilience.

This Chapter discusses how the overall thesis Aim and four Objectives, as outlined in Chapter 1, are addressed by the findings from the research Phases. A summary of how the research objectives are addressed through research findings are presented in Table 7.1. Section [7.2. Main Research Findings](#), then discusses these findings in more detail with key takeaways from across all Phases of the research project and all chapters of the thesis. The contribution of the research and application of the findings within military organisations is discussed, as well as how the findings can be applied to any organisation or industry working with sensitive information. Limitations of the current research project addresses challenges of being an independent researcher working with a military population and with the design of the research, providing justifications for future suggestions of research in this area. This Chapter, and the thesis is summarised with a conclusion for the research project, outlining next steps for the wider programme of work this PhD thesis sits in.

**Table 7.1:**

*A summary of the four research objectives as outlined in Chapter 1 and how they have been addressed through findings from Phases 1, 2 and 3 of the research project outlined in this thesis.*

	<b>Research Objective</b>	<b>Findings</b>	<b>Contribution to knowledge statement</b>
<b>Objective One</b>	To create a definition explaining which military friends and relatives should be considered Military Key Relations	A range of friends and relatives should be included in the definition of Military Key Relations. This includes ‘Next of Kin’ relationships, which are included in much of the existing research on military friends and relatives (e.g. Clever & Segal, 2013). But this thesis posits a broader definition that specifically should include extended family and short-term relationships. Additionally, whilst much of the research that addresses gaps in this area still focuses on military families (e.g. Gribble et al. 2020) this research project highlighted multiple types of friendships should also be included in the definition of Military Key Relations.	The research provides a clear and specific list of military friends and relatives that should be considered Military Key Relations. This definition can be referred to when identifying which individuals military organisations should engage with, both within the context of cybersecurity, as well as other scenarios, for example healthcare.
<b>Objective Two</b>	To investigate the online behaviours that Military Key Relations engage in, and identify any behaviours that could create a cyber risk for military organisations	Military Key Relations use a variety of communication platforms, with WhatsApp being frequently preferred. Potential risk behaviours could arise in communication if Military Key Relations are unaware of the importance of military information and share sensitive operational information such as location, timings and dates. As well as personal information that could make themselves and their military person a specific target for a threat actor.	The research provides an outline of information sharing behaviours that may impact military cyber resilience, as well as potential explanations for behaviours. This provides a direction for addressing Key Relations online risk behaviours.
<b>Objective Three</b>	To explore current approaches to cybersecurity training, education and awareness for Military Key Relations and how adequately these approaches address potential online risk behaviours.	There is limited direct engagement about cybersecurity with the extended Military Key Relations community. Those actively involved with a military organisation either in their own career or due to living in housing provided to married serving men and women on a military base, may receive cybersecurity materials. However, most have not been invited to attend cybersecurity training or been provided with cybersecurity education and awareness materials for a military context. Many rely on their own knowledge, or their military person to relay information to them.	The research highlighted gaps in the current approach for cybersecurity training, education and awareness for military Key Relations, and areas that could be improved in the future.

<p><b>Objective Four</b></p>	<p>To determine who should be responsible for ensuring Military Key Relations behaviour is not detrimental to Military organisation's cyber resilience and determine accountability for the consequences of Military Key Relations online risk behaviours.</p>	<p>The responsibility for Military Key Relations' online behaviour and how it contributes to military cyber resilience is shared between the Key Relations, the military personnel and the organisations themselves. This is a co-dependent relationship as personnel cannot provide their Key Relations with the information if they are not provided with it themselves, and military organisations and personnel cannot disseminate the information if Key Relations are not engaged. Accountability is more nuanced. The importance of ensuring a culture knowledge sharing and learning from mistakes should be encouraged rather than punishment or disciplinary measures.</p>	<p>By identifying the responsibility for Key Relations online behaviours is shared between the organisation, military personnel and Key Relations this provides a clear direction for who needs to receive cybersecurity training, education &amp; awareness materials to ensure Key Relations keep information safe online. The understanding of knowledge sharing over punishment can help guide military organisations to build a positive cyber security culture.</p>
------------------------------	--	--	---

## 7.2. Main research findings

### 7.2.1. The definition of Military Key Relations

The current approach to defining Military Key Relations by the Ministry of Defence takes a broad approach, explaining that diverse relationships and situations should be considered (Ministry of Defence, 2023). Whilst the presumed intention is to be inclusive of all situations, this presents challenges for those responsible for engaging with the extended military community as there is inconsistent guidance for how to direct information to personnel's friends and relatives. This could include a deployment welfare package, or a cybersecurity campaign. Therefore, this thesis has created a definition that references specific friends and relatives based on the findings from Phases 1, 2 and 3. The definition of Military Key Relations from this research includes the following friends and relatives:

- Wife, Husband or Civil Partner
- Unmarried partner
- Short-term partner (less than 1 year)
- Parent or Guardian
- Child
- Sibling
- Grandparent
- Extended family e.g. Cousin/Aunt/Uncle/Niece/Nephew
- Co-habiting friend or roommate
- Friend from school
- 'Close' or 'Best' friend

Gribble et al. (2020) claim that research involving the extended military community does not often consider short-term relationships. The findings from this research suggest that short term relationships, defined as a relationship of less than one year, are considered a Key Relation by military personnel. However, this does not diminish that the type of relation with the largest percentage of personnel saying they would contact this person on deployment, was a 'Husband, Wife or Civil Partner'. In Phase 3, the type of relation with the largest percentage of participants was a 'Husband, Wife or Civil Partner'. In the findings from Phase 1, the three types of relation which had the highest percentage of participants responding, 'Yes' they would contact this relation type on deployment was 'Husband, Wife or Civil Partner', 'Child' and 'Parent or Guardian'. This demonstrates that whilst the definition of Military Key Relations should expand to include extended relationships, dependent and next of kin relationships are still considered a part of a military person's close network.

Research into support for military personnel following trauma exposure highlighted how friends can mediate the negative effects trauma exposure has on mental health (McCabe et al. 2020). However, in the literature search there was no research identified that the definition of Military Key Relations includes friendships. This creates a gap in the research into this definition as Rözer et al. (2016) identify how primary contacts with an active role in our lives, those who we feel the closest to and intimate towards, can be friends as well as relatives. As the findings from Phase 1 in the current thesis identified, individuals may even consider their friends as their

family, if they are not in contact with or do not have any family members who are an active part of their life.

Whilst the findings demonstrated that relationship strength and communication frequency can vary between type of relation, the results did not suggest that this influenced whether or not a military person would consider this type of relation a Key Relation in their network. Military Key Relations that were originally included in Phase 1 that are not included in the final definition were removed due to an insufficient percentage of personnel identifying they would contact this person on deployment in Phase 1 or because no participant reported this relation type as a Key Relation in Phase 2. Additionally, a work colleague was not included in the definition of Military Key Relation in this thesis, as they would already have access to cybersecurity materials provided by a military organisation. However, Phase 1 in Chapter 4, discussed how colleagues can be important in providing support for military personnel. Additionally, Phase 2 identified types of relations including ex-partners and in-laws that have not been included in this definition of Military Key Relations. Only one participant mentioned an ex-partner in discussions around Key Relations, and the participant only briefly mentioned this relation, with a lack of context about their opinion in the dynamic of this individual contributing to cyber resilience. Comparatively, multiple participants in the interviews mentioned in-laws when considering their friends and relatives. Due to the potential difficulty of accessing both ex-partners and in-laws to explore their perspectives in Phase 3, there is insufficient data from this research project to justify including them in the definition of Key Relations. However, to ensure vulnerabilities in cyber resilience are reduced, future research should explore the dynamic of these types of relation in more detail, to determine how their online behaviour might contribute to organisational cyber resilience.

### 7.2.2. Potential behaviours influencing military cyber resilience

When looking at online communication behaviours between military personnel and Military Key Relations, findings from Phase 1 and Phase 3 identified that WhatsApp was the most preferred platform for these individuals to use to communicate with each other. This is of interest when considering that findings from Phase 2 highlighted that the use of WhatsApp is discouraged by the Ministry of Defence. During interviews, participants explained that they are encouraged to use Signal when communicating with their loved ones on deployment. Participants in Phase 2 also explained how military organisations advise personnel to encourage their loved ones to use Signal when communicating with personnel when they are deployed. However, any social media application has the ability to present a vulnerability to military cyber resilience if cybersecurity behaviours are not employed. Military Key Relations with an open social media profile that connects them to a military person may be vulnerable to a targeted attack from a military adversary. Phase 3 explored the adoption of security behaviours from Key Relations and identified that most participants do make any social media profiles private. However, the small percentage that either identified they only did this sometimes or not at all do present a potential risk to military cyber resilience if they share information about their military person.

Findings across the Phases of the research highlighted the main risk of Key Relations sharing information online is sharing operational information. This includes information about deployment location, movement dates and timings. However also includes specifics about who is deploying such as number of personnel and their personal information. Phase 2 discussed how this sharing of information by Key Relations may occur incidentally as a result of other influences such as social norms. Spottswood and Hancock (2017) explain how when users are deciding the



detail of information that should disclose on social media they follow behavioural norms that are set by others, in order to appear likeable to these other users. In the context of Military Key Relations, if these individuals see others on their social network posting location information, they may do this also in order to gain approval from others. This could be heightened even further for a Military Key Relation where military experiences are new, and they see other Key Relations behaving in this way. Additionally findings from Phase 2 explained influences such as lack of understanding about application permissions and pride of their military person results in oversharing of information online. Sharing operational information of any level of detail can present a vulnerability due to the risk of a potential threat actor aggregating information shared by multiple Key Relations and then acting on this information.

There is the potential that age may influence the extent a Key Relations' online behaviour may present a risk to military cyber resilience. Phases 1 and 2 found a clear pattern of younger generations using a wider range of communication platforms, specifically newer social media applications, such as Snapchat and BeReal, as well as Twitter and Instagram. This is consistent with findings for the general UK population, where younger individuals are more likely to use newer applications such as TikTok (Ofcom, 2022). The broad range of applications used by younger people may make them more vulnerable to an attack because there are more platform settings to consider and configure securely. Comparatively, Key Relations from older generations who are reluctant to keep up with the evolution of technology may use platforms due to necessity of keeping in contact with their military person and may be less confident in applying security behaviours (Morrison et al. 2021). Considering age differences and the potential differences in approaching online behaviours and consequently online security is important for guiding future cybersecurity initiatives, to ensure materials are relevant for the audience.

### 7.2.3. Current approaches to Cybersecurity training, education and awareness for Military Key Relations.

Cybersecurity training, awareness and education initiatives are suggested by some researchers a key part of building a cybersecurity culture (Uchendu et al. 2021). Outside of the context of Military Key Relations, cybersecurity training, education and awareness occurs in a variety of formats, such as presentations, gamified training, and simulated exercises, each with their strengths and challenges (Chowdury & Gkioulos, 2021). Chapter 2 discussed some of these challenges, including how cybersecurity awareness campaigns can be disengaging and inappropriate for the audience (Bada et al. 2018) and due to a lack of consideration of cultural factors (Aldawood & Skinner, 2019). Also identified in Chapter 2 is the lack of literature on existing cybersecurity training, education and awareness campaigns for Military Key Relations. This thesis addressed that gap, with Phase 2 findings identifying that this may be due to there being very little provided to Military Key Relations about their online behaviour, with existing approaches focusing on engaging those who live on military patches and relying on military personnel to convey information to their Key Relations. This was reiterated in the findings from Phase 3 where only a handful of Key Relations reported being invited to cybersecurity training from a military organisation or receiving cyber education and awareness materials. Some participants in Phase 3 also reported they have discussions with their military person about what they are happy for the Key Relation to post online about their job.

Relying on military personnel to communicate security requirements for online behaviours to their Key Relations has its limitations. Personnel whose job role does not involve any information security element will not have expertise in this area to provide an in-depth

explanation of the importance and the reasoning behind why their Key Relations should apply cyber secure behaviours. As Ramachandran et al. (2012) highlighted those who don't believe cybersecurity is relevant to them as they are not cyber experts, may not consider themselves as having a responsibility for cybersecurity. This may present one explanation as to why Military Key Relations reported being more confident in their knowledge of cyber risks and security behaviours than they are confident in their understanding of these elements of cybersecurity. Personnel without expertise in information security may simply be aware of the secure behaviours required to comply with a cybersecurity policy, but do not possess the understanding for why these behaviours are important. Therefore, it would not be possible for them to communicate something they are unaware of themselves. Additionally, Phase 2 highlighted that discussions in this area does not come naturally for all personnel and their Key Relations. There is the potential that relationships between military personnel and their Key Relations which are already strained may not be relationships that encourages open and honest dialogue. Even for those relationships that do have this open and honest communication, there is the potential that Key Relations may take offence to personnel relaying this information, as they may perceive it as personnel disliking their Key Relations sharing how proud they are of them in their job role. There are multiple reasons that personnel may not explain the underlying reasons for why Key Relations should engage in secure online behaviours. Notwithstanding the reasoning, there was a range of confidence scores provided by participants in Phase 3 when asked about their confidence in knowledge and understanding of cyber risk and security risk behaviours. Furthermore, scores about the level of risk associated with online behaviours demonstrates uncertainty and a lack of understanding towards cyber risk behaviours and how to behave securely online. This demonstrates a requirement for a more targeted approach to engaging with Military Key Relations about cybersecurity.

#### 7.2.4. Accountability and Responsibility for Military Key Relations' online behaviours

Findings from across the Phases indicate that a shared responsibility for Military Key Relations' online behaviour when considering the influence on military cyber resilience, may be the best approach. The responsibility should be shared between the organisation, the personnel and the Key Relations. Uchendu et al. (2021) define responsibility as an employee's commitment to performing security related tasks. When considering the role of the military personnel in shared responsibility, this definition is appropriate as it highlights that an employee has an obligation to ensure they are contributing positively to the cybersecurity of an organisation. For military personnel however, this can only be done if they are provided with the tools by their employer. Responses from the interviews in Phase 2 highlighted how a large percentage of serving military personnel do not work in roles that would provide them with the expertise to understand the online threat landscape for military organisations, or how to implement measures to mitigate against these threats. Therefore, it is the responsibility of the organisation to foster a culture where cybersecurity is valued by all employees, and that this is reinforced within their personal life, with their Key Relations.

Nel and Drevin (2019) explain that responsibility is determined by ensuring individuals are aware of their role within security. This definition might be more appropriate for Military Key Relations as it does not focus on stakeholders for security being employees at an organisation. Whilst the findings from Phase 3 suggested that not all participants may not be aware of the full extent their behaviour influences military organisations' cyber resilience, they would be willing

to spend the time learning. Phase 3 found that a large percentage of Key Relations would attend an annual initiative organised by the Ministry of Defence to provide military friends and relatives with an overview of how they contribute to military cyber resilience, and how they should behave online to be cybersecure. This demonstrates that Key Relations are happy to be actively involved in the sharing of the responsibility for their online behaviours if they are provided with the opportunity to do so. To ensure engagement with any future cybersecurity initiatives, military organisations should consider the challenges of potential barriers for Key Relations attending or engaging with materials, discussed in the following section, [Recommendations for future Cybersecurity initiatives with Military Key Relations.](#)

Fostering a Cybersecurity Culture that values knowledge sharing and learning from mistakes rather than punishment is important for creating an organisation with a positive Cybersecurity Culture (Dekker, 2018). Findings from Phase 2 also highlighted that this value on learning from mistakes over punishment is a key aspect when considering who is accountable for Key Relations' online behaviours. This is consistent with Dekker (2018) who highlighted that an organisation without blame is not one without accountability. Multiple participants in Phase 2 highlighted they would not consider their Key Relations accountable for a misstep in online behaviour that results in sensitive military information being shared, as they may not have the knowledge provided to them to know what is acceptable to share. Getting Key Relations involved in the military community by engaging with cybersecurity campaigns would be useful in providing Key Relations with the information they require to make safer decisions online. However, Phase 3 highlighted that Key Relations would be reluctant to engage in cybersecurity initiatives if there are disciplinary measures for themselves or their military due to poor engagement with materials, or if they make a mistake in their online behaviour. One of the recommendations that came out of the Phase 2 interviews was to create a two-way method of communication between Key Relations and military organisations so that Key Relations can be provided with guidance when unsure how to behave online, and for them to have a direct contact to report any potential threats or insecure behaviours. This also provides the potential to reward Key Relations who engage and comply with military cybersecurity requirements and establish cybersecurity champions within the Military Key Relations community. A cybersecurity champion is one that embodies values of a secure organisation and adopts security behaviours from cybersecurity policy and encourages others to also adopt these secure behaviours (Uchendu et al. 2021). Alshaikh (2020) suggests that creating a network of cybersecurity champions is important in developing a positive Cybersecurity Culture in an organisation.

### 7.3. Evaluation of the Research

As discussed in the Literature review in Chapter 2, simply knowing the culture and experiences of military personnel is insufficient to claim cultural competency (Redmond et al. 2015). This research sought and applied the experiences and opinions of Dstl Military Advisors, who are serving personnel from each of the Front-Line Commands in the UK Armed Forces. Whilst both my grandfathers have previously served in the UK military, making my grandmothers and both parents Key Relations of military personnel, neither of them is currently serving, nor were they active serving personnel during my lifetime. Therefore, this does not provide me with extensive first-hand insight into the experiences of military culture for personnel, or Military Key Relations. Being an independent researcher with limited first-hand knowledge into the experience of Military culture, was beneficial as I entered into the research with no pre-conceived notion of the findings except from what was outlined in the literature. This is particularly

important when considering how this might influence participant responses in the semi-structured interviews. Whilst there was the potential to draw on family experiences when interpreting participants opinions during the analysis of the interviews, having an additional researcher analyse the data, and discuss the final themes reduced the possibility my own experiences influenced the findings. It also means that there was no power dynamic interplay due to military rank, or fear of repercussions due to revealing a risk behaviour that might result in a disciplinary measure in a different circumstance. Whilst benefits exist to being an independent researcher, future work on this topic may benefit from further exploration of the influence of culture with a researcher who does have first-hand experience of serving in the military or being a military key relation.

One benefit of future research being conducted by a researcher with first-hand military experience is access to participants. One of the main challenges across Phases 1 and 3 of the research project was the sample size for both of these surveys. Within this research, Dstl Military Advisors and Technical Partners facilitated communication to invite individuals to participate in the research. Whilst this was beneficial in accessing the target population, I had limited control over assessing the engagement with research adverts and links, aside from the data provided by the survey platform, Qualtrics. Due to the nature of the research being exploratory the small sample sizes have been sufficient to provide the insight required to address the objectives. Additionally, Phase 1 was also supported by the findings from Phase 2. Phase 2 not only included a range of participants in the participant sample, but also consisted of qualitative findings in the form of semi-structured interviews, providing a more in-depth understanding of the perspectives of military personnel, as well as SMEs. However, the findings from Phase 3 are presented with the acknowledgement that it would be beneficial to have a wider range of Military Key Relations in the participant group, to explore different perspectives. As highlighted, this PhD thesis forms part of a wider programme of work at Dstl, where the next study is likely to be taken forward to conduct qualitative focus groups with Military Key Relations to provide additional insight into the findings from Phase 3. Challenges with recruitment during this research do provide the opportunity to highlight lessons learned when trying to access military personnel and their Key Relations. Lessons learned and potential mitigations are included in table 7.2 below.

**Table 7.2:**

*A summary of lessons learnt from challenges with recruiting participants in Phases 1 & 3 and success in recruiting participants in Phase 2, along with recommended solutions for application of these lessons in future research.*

<b>Lessons learned</b>	<b>Possible application of solutions</b>
Ensure adequate time within projects for ethical approval when working with the (extended) military community	<ul style="list-style-type: none"> <li>• Sample size justifications and calculations clearly highlighted in any ethics protocols.</li> <li>• Minimum participants required to provide sufficient insight should be outlined, as well as the ideal number of participants.</li> </ul>
Ensure adequate time to conduct multiple iterations of inviting individuals to participate in the research	<ul style="list-style-type: none"> <li>• Clear deadlines should be outlined for when study adverts/invites are re-circulated due to insufficient survey tractions.</li> <li>• If using gatekeepers, or those in similar roles such as Military Advisors, ensure it is clear ahead of time when they might be out of office for a number of weeks. This is particularly important in a military environment when points</li> </ul>

	of contact may not have access to their emails for weeks at a time.
Make use of pre-established connections where possible	<ul style="list-style-type: none"> <li>• Survey traction increased in Phase 3 when a member of the Key Relations community shared the study advert in a community centre for military Key Relations.</li> <li>• In future research this may look like using methods such as newsletters and flyers in more community centres/military patches to engage with a pre-established community.</li> <li>• Making use of snowball sampling is also important in this area, to build trust and rapport.</li> </ul>

This thesis recruited participants who are associated with the UK Military. This included individuals currently serving in the British Armed Forces, SMEs working in defence within the UK, and Key Relations whose military person is currently serving in the British Armed Forces. As identified throughout the thesis, when considering culture, there is the potential that dimensions of national culture may influence Information Security Culture within an organisation. As a Western culture, the UK has an individualistic culture, which has been suggested to affect compliance with security requirements if they involved restraining individual behaviour (Zhang et al. 2018). Therefore, recommendations for addressing online risk behaviours within this thesis may only be relevant for Key Relations of military personnel serving in a military of a Western country. The findings may not be generalisable to other countries, such as non-Western countries, or those with a collectivist culture.

## 7.4. Impact of the Research

### 7.4.1. Recommendations for Stakeholders

The following section outlines some key recommendations that can be taken from the research findings that are relevant to each stakeholder group.

#### *Recommendations for Dstl*

1. Apply the definition of Key Relations in future research when considering military friends and relatives.
2. Build on relationships briefly outlined in this research but not currently included in the definition of Key Relations to determine whether any other Key Relations should be included, such as in-laws and previous partners who share children.
3. Create and distribute outputs that provide an overview of how Key Relations can influence cyber resilience in military organisations and how this might be reduced through the use of training, education & awareness.
  - a. This will also require identification of relevant partners who can make use of the research.
4. More research is required to explore the opinions of Key Relations themselves when considering cybersecurity training, education & awareness. This should focus on methods of dissemination, and how to reduce potential barriers to engagement.

### *Recommendations for the FLCs*

1. This research can be used a justification to allocate resources for cybersecurity training, education & awareness in military Key Relations, due to the identification that potential risk behaviours could negatively impact military cyber resilience.
2. Apply the definition of Key Relations to guide who to approach in the future when wanting to engage with military personnel's friends and relatives. This can be in the context of cybersecurity, or other spaces, such as healthcare engagement.
  - a. Considering resource limitations, this may require prioritising certain Key Relations such as Long-term partners, Short-term partners, children for a quick-win, and setting a plan for engaging other Key Relations in the near future.
  - b. Using the approach above may require additional consideration whether personnel's Key Relations are friends, as well as family members.
3. Conduct a risk assessment to determine what the severity of impact on assets for your unit would be if Key Relations shared information about these assets online.
4. Create guidance that identifies what Key Relations can and cannot share online about their military person and their unit.
  - a. Consider situations where this might change, for example, deployment.

### *Recommendations for policy creators*

1. Refer to the definition of Key Relations to identify specific friends and relatives that should be included/receive future guidance.
2. Findings can be used to create guidance on how military Key Relations should behave online to ensure Cyber resilient military organisations.

## **7.4.2. Recommendations for future Cybersecurity initiatives with Military Key Relations**

This research project created a precise and broad definition of Military Key Relations, including a variety of types of family and friends. This means that future cybersecurity initiatives will have a clear direction of who to invite to participate in and engage with these materials. Identifying which Key Relations military organisations should engage with is important for increasing participation in future cybersecurity initiatives. Future initiatives should also consider the content and form of training, education and awareness to increase participation levels. Phase 2 interviews with representatives of military personnel and subject matter experts identified some participants' perceive existing cybersecurity training and education materials provided by military organisations as repetitive and irrelevant to the individuals it is delivering the information to. This is consistent with Bada et al. (2018) who highlight that often cybersecurity awareness campaigns are distributed without evaluating how appropriate and representative of the threat landscape these campaigns are. It appears this may happen for some cybersecurity materials within military organisations with the threat landscape not being sufficiently up to date

or encompassing of the range of threats. When considering the content of future cybersecurity materials for initiatives to engage Military Key Relations, materials should be engaging and appropriate for the audience, and adequately represent the potential threats and how to effectively mitigate against them. This can help ensure Military Key Relations actively repeatedly engage with cybersecurity initiatives rather than create disinterest due to the materials being too narrow and repetitive.

As discussed in the previous section, creating a Cybersecurity Culture within military organisations that encourages accountability over punishment or disciplinary measures is key for ensuring that there is no barrier of fear preventing Key Relations from engaging with future cybersecurity initiatives. Additionally, the approach taken in any future initiatives should consider the importance of secure language rather than fearful language, in a non-patronising manner. Future cybersecurity initiatives provided by Military organisations to engage Key Relations should also consider other barriers identified within this research project. Lester et al. (2012) highlighted that healthcare interventions with military families are often left incomplete due to relocation. This is consistent with findings from Phase 3 where Key Relations frequently mentioned location being a potential reason they would not engage with future cybersecurity campaigns. Furthermore, participants stated that due to being relocated as part of their military person's job, away from their families that finding childcare to attend an event is much more difficult. Childcare was one of the most frequently mentioned barriers by Key Relations and so future cybersecurity initiatives should provide solutions to ensure those who are interested in engaging with the materials, are able to, and so that individuals such as parents of young children are not left out by design. Suggestions from the Phase 3 discussion included running events that provide childcare, or to provide training, or education and awareness materials in an online format. Providing participants with this information online may be more beneficial as it means that Key Relations are able to engage with the information in their own time and refer back to it as and when required. This recommendation was also highlighted by participants in Phase 2. However, there are also benefits with in-person sessions, with research into engagement with cybersecurity initiatives within older adults suggesting that an in-person peer led event encouraged inclusion of individuals who would ordinarily be unable to seek cybersecurity information (Nicholson et al. 2021).

### 7.4.3. Application of Findings Outside of Military Key Relations

Whilst this research aimed to focus on exploring how online behaviours of Military Key Relations contribute to military cyber resilience, it has applications for other populations, both internal and external to the military. In the process of exploring the behaviours of Key Relations, the findings also provide insight into the online behaviours of Military Personnel. Most of these findings will be fed directly into Dstl with the recommendation the findings should be considered when creating future cybersecurity initiatives. However, the key takeaways suggest that whilst personnel may have the awareness and understanding of what information they need to protect when online, and how this should be done, other factors may ultimately influence the success of the most secure online behaviour being performed. Additionally, the findings from Phase 2 and Phase 3 indicate that Military Key Relations who openly discuss cybersecurity requirements for military information with their Military Personnel have greater awareness about what they can and cannot post, and how military information should be shared if the Key Relations wish to share it. Therefore, a takeaway from this research for military personnel's cybersecurity training is that knowledge sharing with their Key Relations about keeping military information, such as operational details, safe and how to do that, should be encouraged.

Additionally, Phase 2 interviews highlighted how the military workforce is progressing by reducing the number of full-time serving personnel. Instead, it is adopting a military whole-force approach that incorporates more reservists and defence contractors. The results from this project may not be so applicable to reservists and defence contractors themselves, as Phase 2 interviews highlighted how these individuals are still required to complete cybersecurity training modules provided by military organisations. However, it may apply to the Key Relations of these individuals, who are a step removed from the military community meaning that they may not find it as easy to access support services provided by the military. However, these Key Relations may still have access to sensitive military information from projects or operations a reservist or contractor is part of. Therefore, it would require additional knowledge on what information cannot be shared, and how to behave online in a way that keeps military information safe and positively contributes to military cyber resilience.

This research project's findings can also be extrapolated for different organisations in industries that work with sensitive information. This could include other government organisations, including politicians, financial and banking organisations, organisations in the legal sector and healthcare providers. For example, in 2020 a trainee solicitor shared emails with a friend, as they shared a common enjoyment of discussing the law. However, these conversations resulted in the trainee solicitor disclosing privileged client information with this friend, including personal identity and medical information (McKinney, 2020). Whilst there was no additional consequence involving a threat actor of information shared in this case, this example demonstrates the potential role of Key Relations in influencing organisational cyber resilience in alternative industries to the military. Whilst these industries deal with particularly sensitive information that could be extremely detrimental should a cyber-attack occur, any organisation that handles personal information and is subject to GDPR and DPA laws should consider how their employee's interactions with their friends and relatives may present a risk where this information could be vulnerable to being exploited by a threat actor.

## 7.5. Directions for Future Research

As mentioned in the previous section, 7.4. Impact of the research, discussions with military personnel and subject matter experts in defence highlighted the development of a military whole force that encompasses reservists and external contractors. This has implications for the role of culture, as reservists can experience dissonance between military and civilian culture due to the different values (Howard, 2006). This thesis only recruited active serving personnel, and their Key Relations. Throughout the research process, I received offers for assistance with recruitment from multiple individuals connected with the reservist community. Due to the research outline, and ethics protocols focussing only on serving personnel, the decision was made that making an amendment to this would widen the scope of the research too much for an exploratory project. However, the interest in the research from the reservist community indicates that further research with reservists and their Key Relations would be beneficial in providing a deeper insight in this area. This is an important step when considering the aim of creating a cyber resilient organisation that addresses any potential areas of cyber vulnerability.

This research project explored online risk behaviours of Military Key Relations mainly through investigating direct communication between Key Relations and Military personnel, with a small number of questions focusing on indirect or broadcast communication behaviours. However, moving forward, research in this area should continue exploring any other potential



online risk behaviours that Military Key Relations engage in that could influence military organisational cyber resilience. Exploring a wider spectrum of online information sharing behaviour, in more depth, would be beneficial. For example, indirect or broadcast messaging behaviours on social media. This could include behaviours such as posting on newsfeeds on Facebook, Instagram, X, and other social media platforms, or posting stories on these platforms and others. Some of these behaviours arose in Phase 2 of the research, and Phase 3 briefly asked about these types of behaviours when asking participants how they alter their online behaviour when considering their military person. These behaviours included considering the operational information that is shared about their military person in Facebook posts when discussing them leaving or returning from deployment and ensuring any pictures do not contain military information. Zero Military Key Relations identified that they use BeReal to communicate with their military person, with no real risk to military cyber resilience being identified in the findings from this research project. BeReal's main feature provides users with a notification once a day where users are encouraged to share a front and back camera picture of their immediate surroundings (BeReal, 2024). In this thesis, direct communication was explored when discussing platform usage, and so participants may not have highlighted they use BeReal in the findings as the nature of BeReal encourages feed posts through this notification, rather than direct communication between users. Military Key Relations' behaviour on BeReal may present a risk to military cyber resilience when considering behaviours that do not involve direct communication, for example if sensitive military information is inadvertently shared in the background of a picture in a post. Future research should explore these behaviours in more depth to understand the extent Military Key Relations engage in these behaviours and how they could present a risk to cyber resilience. Additionally, future work looking at online behaviours when creating or engaging with content on online forums and online blogs.

It is also important to note that this research provides an insight into the risk behaviours and recommendations for addressing these behaviours considering the current trends in online communication and online behaviours. However, it is important that research is constantly measuring these behavioural trends and updating the approach to address these trends so that this does not create a vulnerability in organisational cyber resilience.

## 7.6. Conclusion

The existing approach to involving military friends and relatives in Cybersecurity is under researched with no clear direction for who to include when considering the influence on military cyber resilience. This thesis provided a clear definition of military friends and relatives that should be included in the definition of Military Key Relations. This was identified through three Phases of research exploring perspectives from a variety of stakeholders, including military personnel, subject matter experts and Military Key Relations. This definition is broader than definitions previously identified in the literature, which either focussed primarily on next of kin relationships, did not consider the role of friends as Key Relations, or lacked specificity and clarity.

The thesis identified how Key Relations information sharing behaviours online can present a risk of being exploited by a military adversary, and the potentially fatal consequences of this vulnerability. Whilst the current approach to cybersecurity training, education and awareness for Military Key Relations is limited, the thesis included recommendations for how to address this going forward by engaging with Key Relations to ensure more effective cybersecurity resilience of military organisations. The findings from this thesis highlighted how the

responsibility for encouraging a culture where cybersecurity is valued within Military Key Relations should be shared between military organisations, personnel and Key Relations. Whilst the objectives of this research were addressed in this thesis, further research would benefit in exploring the understanding of the perspectives of Military Key Relations in more detail. This thesis forms part of a programme of work in this area, within Dstl, and the findings from this thesis guide directions for future work outside of the PhD project.

The thesis explored the role of Military Key Relations in contributing to military cyber resilience by understanding who Key Relations are, their potential online risk behaviours and methods of reducing the effect of these behaviours by identifying accountability and responsibility. This thesis identified the value of military organisations engaging with the extended military community about cybersecurity to ensure organisational cyber resilience.

## References

- Abbas Naqvi, M. H., Jiang, Y., Miao, M., & Hasnain Naqvi, M. (2020). The effect of social influence, trust, and entertainment value on social media use: Evidence from Pakistan. *Cogent Business & Management*, 7(1). <https://doi.org/10.1080/23311975.2020.1723825>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. [https://doi.org/https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/https://doi.org/10.1016/0749-5978(91)90020-T)
- Ajzen, I., Joyce, N., Sheikh, S., & Gilbert Cote, N. (2011). Knowledge and the Prediction of Behavior: The Role of Information Accuracy in the Theory of Planned Behavior. *Basic and Applied Social Psychology*, 33, 101-117. <https://doi.org/10.1080/01973533.2011.568834>
- Alarcon, G. M., & Lee, M. A. (2022). The Relationship of Insufficient Effort Responding and Response Styles: An Online Experiment. *Frontiers in Psychology*, 12(2021). <https://doi.org/10.3389/fpsyg.2021.784375>
- Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, 11(3). <https://doi.org/10.3390/fi11030073>
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567-575. <https://doi.org/https://doi.org/10.1016/j.chb.2015.03.054>
- Alnifie, K. M., & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. *Journal of Information Security*, 14(2), 93-110. <https://doi.org/10.4236/jis.2023.142007>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98. <https://doi.org/https://doi.org/10.1016/j.cose.2020.102003>
- Alshaikh, M., Naseer, H., Ahmad, A., & Sean, B. M. (2019). Toward sustainable behaviour change: An approach for cyber security education training and awareness. *European Conference on Information Systems: Information Systems for a Sharing Society, ECIS 2019*,
- Alvinus, A., & Homberg, A. (2019). Silence-breaking butterfly effect: Resistance towards the military within #MeToo. *Gender, work and organization*, 26(9), 1255-1270. <https://doi.org/10.1111/gwao.12349>
- Ambore, S., Doğan, H. E., & Apeh, E. (2021, July). Development of Usable Security Heuristics for Fintech. In *34th British HCI Conference* (pp. 121-132). BCS Learning & Development.
- American Psychological Association. (2024). *Resilience*. <https://www.apa.org/topics/resilience>
- Anwar, M., He, W., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.

<https://doi.org/https://doi.org/10.1016/j.chb.2016.12.040>

- Auxier, B., & Anderson, M. (2021). *Social Media Use in 2021*. Pew Research Center.
- Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50, 171-181. <https://doi.org/10.1016/j.ijinfomgt.2019.05.014>.
- Bada, M., Sasse, A., & Nurse, J. R. C. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society,
- Bada, M., Von Solms, B., & Agrafiotis, I. (2018). *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study* International Conference on CyberTechnologies and Cyber-Systems,
- Baek, T. H., & Yoon, S. (2022). Pride and gratitude: Egoistic versus altruistic appeals in social media advertising. *Journal of Business Research*, 142, 499-511. <https://doi.org/https://doi.org/10.1016/j.jbusres.2021.12.066>.
- Bailey, T. S. (2019). *The Relationship Between Military Deployment and Spouses' Anxiety, Depression, and Stress* [Walden University].
- Bak, J. Y., Kim, S., & Oh, A. (2012). Self-Disclosure and Relationship Strength in Twitter Conversations. 50th Annual Meeting of the Association for Computational Linguistics, Jeju, Republic of Korea.
- Bambauer, D. E. (2013). Privacy Versus Security. *The Journal of Law and Criminology*, 103(3), 667-684.
- Barreto, A. B., & Costa, P. C. G. (2019). Cyber-ARGUS - A mission assurance framework. *Journal of Network and Computer Applications*, 133, 86-108. <https://doi.org/https://doi.org/10.1016/j.jnca.2019.02.001>
- Barsade, S. G., & O'Neill, O. A. (2014). What's love got to do with it? A longitudinal study of the culture of companionate love and employee and client outcomes in a long-term care setting. *Administrative Science Quarterly*, 59(4), 551-598.
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058. <https://doi.org/https://doi.org/10.1016/j.tele.2017.04.013>
- Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, 54(7), 887-901. <https://doi.org/https://doi.org/10.1016/j.im.2017.01.003>
- Benson, V., & McAlaney, J. (2019). *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press.
- BeReal. (2024). *Time to BeReal*. <https://help.bereal.com/hc/en-us/articles/7350386715165--Time-to-BeReal>.

- Berner, J., Rennemark, M., Jogreus, C., & Berglund, J. (2012). Distribution of personality, individual characteristics and internet usage in Swedish older adults. *Aging & Mental Health*, 16(1), 119-126. <https://doi.org/10.1080/13607863.2011.602958>
- Bhushan, B., Sahoo, G., & Rai, A. K. (2017, 15-16 Sept. 2017). Man-in-the-middle attack in wireless and computer networking — A review. 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall),
- Bittner, L. (2014). *How is Social Media Used by Military Families to Communicate During Deployment?* [St Catherine University]. [https://sophia.stkate.edu/msw\\_papers/289](https://sophia.stkate.edu/msw_papers/289)
- Bodeau, D., & Graubart, R. (2016). Cyber resilience metrics: Key observations. *The MITRE Corporation*.
- Bonanno, G. A. (2008). Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events? *Psychological Trauma: Theory, Research, Practice, and Policy*, 1, 101-113. <https://doi.org/https://doi.org/10.1037/1942-9681.S.1.101>
- Born, J., & Frank, C. (2023). Direct and indirect barriers to hypothetical access to care among Canadian forces health services personnel. *Research in Health Services & Regions*, 2(1), 11.
- Brammer, S. E., Punyanunt-Carter, N., M., & Duffee, R. S. (2022). Oversharing on social networking sites: A contemporary communication phenomenon. *Computers in Human Behavior Reports*, 8, 1-4. <https://doi.org/https://doi.org/10.1016/j.chbr.2022.100236>
- Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. SAGE.
- Buijs, V. L., Jeronimus, B. F., Lodder, G. M. A., Riediger, M., Luong, G., & Wrzus, C. (2023). Interdependencies between family and friends in daily life: Personality differences and associations with affective well-being across the lifespan. *European Journal of Personality*, 37(2), 154-170. <https://doi.org/10.1177/08902070211072745>
- Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, 15(1), 48-64. <https://doi.org/10.1057/cpcs.2012.13>
- Cabinet Office. (2021). *The National Resilience Strategy: A Call for Evidence*. <https://www.gov.uk/government/calls-for-evidence/national-resilience-strategy-call-for-evidence>
- Cabinet Office. (2023). *Government Security Classifications Policy*. <https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html#definitions-for-official-secret-and-top-secret>
- Calisi, R. M., & Science, a. W. G. o. M. i. (2018). How to tackle the childcare-conference conundrum. *Proceedings of the national academy of sciences*, 115(12). <https://doi.org/10.1073/pnas.1803153115>

- Cascavilla, G., Conti, M., Schwartz, D. G., & Yahav, I. (2015). Revealing Censored Information Through Comments and Commenters in Online Social Networks. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*,
- Castro, C. (2022). *Instagram's 'precise location' tracking is nothing new, here's how to turn it off*. techradar.pro. Retrieved 9th January from <https://www.techradar.com/how-to/instagrams-precise-location-tracking-is-nothing-new-heres-how-to-turn-it-off>
- Cattell, R. B. (1956). Second-order personality factors in the questionnaire realm. *Journal of Consulting Psychology, 20*(6), 411-418.  
<https://doi.org/https://doi.org/10.1037/h0047239>
- Chase, M., Deshpande, A., Ghosh, E., & Malvai, H. (2019). SEEMless: Secure End-to-End Encrypted Messaging with less Trust. *2019 ACM SIGSAC conference on computer and communications security*,
- Chassidim, H., Perentis, C., Toch, E., & Lepri, B. (2020). Between privacy and security: the factors that drive intentions to use cyber-security applications. *Behaviours & Information Technology, 40*(16), 1769-1783.  
<https://doi.org/10.1080/0144929X.2020.1781259>
- Chatman, J. A., & O'Reilly, C. A. (2016). Paradigm lost: Reinvigorating the study of organizational culture. *Research in Organizational Behavior, 36*, 199-224.  
<https://doi.org/https://doi.org/10.1016/j.riob.2016.11.004>.
- Chavez, C. (2008). Conceptualizing from the inside: Advantages, complications, and demands on insider positionality. *The qualitative report, 13*(3), 474-494.
- Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity, 8*(1).
- Chen, C. C., Dawn Medlin, B., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), 360-376.
- Chowdury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review, 40*.  
<https://doi.org/10.1016/j.cosrev.2021.100361>.
- Church, K., & de Oliveira, R. (2013). What's up with WhatsApp?: comparing mobile instant messaging behaviors with traditional SMS. 15th international conference on Human-computer interaction with mobile devices and services, Munich, Germany.
- Clark, D. (2023). *Number of personnel in the armed forces of the UK 2023, by age*. Statista.  
<https://www.statista.com/statistics/580534/number-of-personnel-in-uk-armed-forces-by-age/>
- Clements-Nolle, K., Lensch, T., Yang, Y., Martin, H., Peek, J., & Yang, W. (2021). Attempted Suicide Among Adolescents in Military Families: The Mediating Role of Adverse Childhood Experiences. *Journal of Interpersonal Violence, 36*, 11743-11754.  
<https://doi.org/https://doi.org/10.1177/0886260519900976>

- Clever, M., & Segal, D. R. (2013). The Demographics of Military Children and Families. *The Future of Children*, 23(2), 13-39.
- Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management*, 36(4), 306-322.
- Coolican, H. (2018). *Research Methods and Statistics in Psychology* (7 ed.). Taylor & Francis Group.
- Cooper, J. (2006). The digital divide: The special case of gender. *Journal of computer assisted learning*, 22(5), 320-334.
- Crane, M. F., Forbes, D., Lewis, V., O'Donnell, M., & Dell, L. (2022). The interplay between social interaction quality and wellbeing in military personnel during their initial two-years of service. *Military Psychology*, 34(5), 503-515.  
<https://doi.org/10.1080/08995605.2021.2015937>
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (Third edition ed.). SAGE.
- Cullen, R. (2001). Addressing the digital divide. *Online information review*, 25(5), 311-320.
- da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, 101713. <https://doi.org/10.1016/j.cose.2020.101713>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.  
<https://doi.org/10.1016/j.cose.2009.09.002>
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196-206.
- Davis, K. (2012). Friendship 2.0: Adolescent's experiences of belonging and self-disclosure online. *Journal of Adolescence*, 35(6), 1527-1536.  
<https://doi.org/10.1016/j.adolescence.2012.02.013>.
- Davis, R. T. (2011). *US Arms and the Media in the 20th Century*. DIANE Publishing.
- Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A reverse digital divide: comparing information security behaviors of generation Y and generation Z adults. *International journal of cybersecurity intelligence & cybercrime*, 3(1), 42-55.
- Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). *In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception IEEE European symposium on security and privacy (EuroS&P)*, Stockholm, Sweden.
- Defense Science Board. (2013). Resilient military systems and the advanced cyber threat. *Defense Science Board*.

- Dekker, S. (2018). *Just culture: restoring trust and accountability in your organization*. Crc Press.
- Deters, F. G., & Mehl, M. R. (2013). Does Posting Facebook Status Updates Increase or Decrease Loneliness? An Online Social Networking Experiment. *Social Psychological and Personality Science*, 4(5), 579-586.  
<https://doi.org/https://doi.org/10.1177/1948550612469233>
- Devotta, K., Woodhall-Melnik, J., Pedersen, C., Wendaferew, A., Dowbor, T.P., Guilcher, S.J., Hamilton-Wright, S., Ferentzy, P., Hwang, S.W., & Matheson, F.I. (2016). Enriching qualitative research by engaging peer interviewers: a case study. *Qualitative research*, 16(6), pp.661-680.
- Dhillon, G. (1997). The context of information system security. *Managing Information System Security*, 8-28.
- Dincelli, E., Goel, S., & Warkentin, M. (2017). *Understanding Nuances of Privacy and Security in the Context of Information Systems* Twenty-third Americas Conference on Information Systems, Boston.
- Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information and Computer Security*.  
<https://doi.org/https://doi.org/10.1108/ICS-07-2023-0116>
- Drummet, A. R., Coleman, M., & Cable, S. (2004). Military Families Under Stress: Implications for Family Life Education. *Family Relations: Interdisciplinary Journal of Applied Family Science*, 52(3), 279-287. <https://doi.org/10.1111/j.1741-3729.2003.00279.x>
- Dunbar, T. (2010). *How Many Friends Does One Person Need?: Dunbar's Number and other evolutionary quirks*. Faber and Faber.
- Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, 132.  
<https://doi.org/https://doi.org/10.1016/j.cose.2023.103372>
- Dupuis, M., & Crossler, R. (2019). The compromise of one's personal information: Trait affect as an antecedent in explaining the behavior of individuals. *Proceedings of the 52<sup>nd</sup> Hawaii International Conference on System Sciences*.
- Edgar, T. W., & Manz, D. O. (2017). *Research Methods for Cyber Security*. Syngress.
- Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of business*, 38(2), 61-73.
- Elo, S., & Kyngas, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107-115. <https://doi.org/10.1111/j.1365-2648.2007.04569.x>
- Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 15.
- Fennelly, L. J., & Perry, M. A. (2020). Chapter 35 - Building a Sustainable Culture of Security. In



- S. J. Davies & L. J. Fennelly (Eds.), *The Professional Protection Officer (Second Edition)* (pp. 397-401). Butterworth-Heinemann. <https://doi.org/https://doi.org/10.1016/B978-0-12-817748-8.00035-3>
- Fitzsimons, M. V., & A., Krause-Parello, C. A. (2009). Military Children: When Parents Are Deployed Overseas. *The Journal of School Nursing*, 25(1), 40-47. <https://doi.org/10.1177/1059840508326733>
- ForcesNet. (2024, March 4). *Alleged German air force leaking claiming UK personnel on the ground in Ukraine 'worrying'*. [Alleged German air force leak claiming UK personnel on the ground in Ukraine 'worrying'](https://www.forces.net/news/ukraine/german-air-force-leak-claiming-uk-personnel) (forces.net)
- Friedland, G., & Sommer, R. (2010). Cybercasing the Joint: On the Privacy Implications of Geo-Tagging. 5th USENIX conference on Hot topics in Security.
- Garside, D., Ponnusamy, A., Chan, S., & Picking, R. (2012). Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems: Research Issues and Future Solutions. *Future Internet*, 4(1), 253-264. <https://doi.org/10.3390/fi4010253>
- Genter, S., Trejo García, Y., & Nichols, E. (2022). Drag-and-Drop Versus Numeric Entry Options: A Comparison of Survey Ranking Questions in Qualtrics. *Journal of User Experience*, 17(3), 117-130.
- Get Safe Online. (2024). *About Get Safe Online*. <https://www.getsafeonline.org/about-us/>
- Gill, L. (2021). *Organisational Resilience to Cyber-Attacks*. Defence Science and Technology Laboratory UK.
- Gore, J. S., Cross, S. E., & Morris, M. L. (2006). Lets be friends: Relational self-construal and the development of intimacy. *Personal Relationships*, 13, 83-102. <https://doi.org/https://doi.org/10.1111/j.1475-6811.2006.00106.x>
- Greene, K., Derlega, V. J., & Mathews, A. (2006). Self-Disclosure in Personal Relationships. In A. L. Vangelisti & D. Perlman (Eds.), *The Cambridge Handbook of Personal Relationships*. Cambridge University Press. <https://doi.org/https://doi.org/10.1017/CBO9780511606632.023>
- Gribble, R., Mahar, A. L., Keeling, M., Sullivan, K., McKeown, S., Burchill, S., . . . Castro, C. A. (2020). Are we family? A scoping review of how military families are define in mental health and substance use research. *Journal of Military, Veteran and Family Health*, 6(2), 85-119. <https://doi.org/10.3138/jmvfh-2019-0054>
- Gundu, T. (2019). *Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaine ICCWS 2019 14th International Conference on Cyber Warfare and Security*, Stellenbosch University, South Africa.
- Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.
- Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, 133, 111-123.

- Hamzah, Z. A. Z., Kamarudin, K., Hajimaming, P. T., & Yakoob, N. A. (2020). Digital Technology and the Impact on Communication Language and Mastery of Generation X and Y for Correspondence Language. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(9).
- Harrell, M. C. (2001). Army officers' spouses: Have the white gloves been mothballed? *Armed Forces and Society*, 28(1), 55-75.
- Haslam, D. M., Tee, A., & Baker, S. (2017). The Use of Social Media as a Mechanism of Social Support in Parents. *Journal of Child and Family Studies*, 26, 2026-2037.  
<https://doi.org/https://doi.org/10.1007/s10826-017-0716-6>
- Haynes, D. (2020, October 28). *Coronavirus: Submarine commander loses job after BBQ party during lockdown*. Sky News. <https://news.sky.com/story/coronavirus-submarine-commander-loses-job-after-bbq-party-during-lockdown-11980236>
- Hertzog, M. A. (2008). Considerations in determining sample size for pilot studies. *Research in nursing & health*, 31(2), 180-191.
- Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.
- Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1). <https://doi.org/https://doi.org/10.9707/2307-0919.1014>
- Hogan, P. F., & Seifert, R. (2010). Marriage and the Military: Evidence That Those Who Serve Marry Earlier and Divorce Earlier. *Armed Forces & Society*, 36(3), 420-438.  
<https://doi.org/10.1177/0095327X09351228>
- Hollnagel, E., (2010). Epilogue: RAG – The Resilience Analysis Grid. As cited in Pariès, J., Hollnagel, E., & Wreathall, J. (2010). *Resilience engineering in practice : A guidebook*. Taylor & Francis Group.
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates.
- Houston, J. B., Pfefferbaum, B., Sherman, M. D., Melson, A. G., Jeon-Slaughter, H., Brand, M. W., & Jarman, Y. (2009). Children of deployed National Guard troops: Perceptions of parental deployment to Operation Iraqi Freedom. *Psychiatric Annals*, 39(8).
- House of Commons. (2013). *Defence and Cyber-Security: Defence Committee*.  
<https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10604.htm>
- Howard, J. L. (2006). The Role of Culture in Shaping Perceptions of Discrimination among Active Duty and Reserve Forces in the US Military. *Employee Responsibilities and Rights Journal*, 18, 171-187. <https://doi.org/https://doi.org/10.1007/s10672-006-9015-x>
- Howitt, D. (2019). *Introduction to qualitative research methods in psychology*. Pearson UK.
- Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why Employees (Still)

Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*, 22(1). <https://doi.org/10.2196/16775>

- Johanson, G. A., & Brooks, G. P. (2010). Initial Scale Development: Sample Size for Pilot Studies. *Educational and Psychological Measurement*, 70(3), 394-400. <https://doi.org/10.1177/0013164409355692>
- Kaiser, N., Henry, K., & Eyjólfssdóttir, H. (2022). Eye contact in video communication: experiences of co-creating relationships. *Frontiers in Psychology*, 13. <https://doi.org/https://doi.org/10.3389/fpsyg.2022.852692>
- Keeling, M., Wessely, S., Dandeker, C., Jones, N., & Fear, N. T. (2015). Relationship Difficulties Among U.K. Military Personnel: Impact of Sociodemographic, Military, and Deployment-Related Factors. *Marriage & Family Review*, 51(3). <https://doi.org/10.1080/01494929.2015.1031425>
- Kirke, C. (2012). Insider anthropology: Theoretical and empirical issues for the researcher. In H. Carreiras & C. Castro (Eds.), *Qualitative Methods in Military Studies* (pp. 17-30). Routledge.
- Kirlappos, I., Parkin, S., & Sasse, M. A. Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security. Workshop on Usable Security, San Diego, California.
- Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber Risk, Market Failures, and Financial Stability (IMF Working Paper No. 185)* (Vol. 2017). International Monetary Fund. <https://doi.org/https://doi.org/10.5089/9781484313787.001>
- Kronsell, A. (2012). *Gender, sex and the postnational defense: Militarism and peacekeeping*. Oxford University Press.
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Kruger, L. J., Rodgers, R. F., Long, S. J., & Lowy, A. S. (2019). Individual interviews or focus groups? Interview format and women's self-disclosure. *International Journal of Social Research Methodology*, 22(3), 245-255. <https://doi.org/10.1080/13645579.2018.1518857>
- Ladwig, R. C. (2023). Managerial influences on the inclusion of transgender and gender-diverse employees: A critical multi-method study. *Australian Journal of Management*, 48(4), 693-710. <https://doi.org/10.1177/03128962231179371>
- Laffaye, C., Cavella, S., Drescher, K., & Rosen, C. (2008). Relationships among PTSD symptoms, social support, and support source in veterans with chronic PTSD. *Journal of Traumatic Stress: Official Publication of The International Society for Traumatic Stress Studies*, 21(4), 394-401.
- Laser, J. A., & Stephens, P. M. (2011). Working with military families through deployment and beyond. *Clinical Social Work Journal*, 39(1), 28-38.

- Lawson, S. T., Yeo, S. K., Haoran, Y., & Greene, E. (2016). *The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate* 8th International Conference on Cyber Conflict (CyCon),
- Leenen, L., & van Vuuren, J. J. (2019). *Framework for the Cultivation of a Military Cyber Security Culture* International Conference on Cyber Warfare and Security.
- Lester, P., Saltzman, W. R., Woodward, K., Glover, D., Leskin, G. A., Bursch, B., ... & Beardslee, W. (2012). Evaluation of a family-centered prevention intervention for military children and families facing wartime deployments. *American Journal of Public Health, 102*, 48-54.
- Liebermann, O., & Britzky, H. (2024, March 5). *Air Force employee accused of sharing classified information on foreign dating website*. CNN.  
<https://edition.cnn.com/2024/03/04/politics/air-force-employee-classified-information-dating-site/index.html>
- Mack, A., & Rock, I. (1998). Inattentional Blindness: Perception without Attention. In R. D. Wright (Ed.), *Visual Attention*. Oxford University Press.
- Malmio, I. (2022). Ritual of (un)changing masculinity: cohesion or diversity? A study of the fraternization traditions of Swedish cadets' at the Military Academy. *International Journal for Masculinity Studies, 17*(3), 181-195.  
<https://doi.org/10.1080/18902138.2022.2033543>
- Mancini, J. A., Walker O'Neal, C., Martin, J. A., & Bowen, G. L. (2018). Community Social Organization and Military Families: Theoretical Perspectives on Transitions, Contexts, and Resilience. *Journal of Family Theory & Review, 10*(3), 550-565.  
[https://doi.org/ https://doi.org/10.1111/jftr.12271](https://doi.org/10.1111/jftr.12271)
- Marotta, A., & Pearlson, K. (2019). *A Culture of Cybersecurity at Banca Popolare di Sondrio* Twenty-fifth Americas Conference on Information Systems, Cancun.
- Martins, A., & Eloff, J. (2002, July). Assessing Information Security Culture. In *ISSA* (pp. 1-14).
- Matassi, M., Boczkowski, P. L., & Mitchelstein, E. (2019). Domesticating WhatsApp: Family, friends, work, and study in everyday communication. *New Media & Society, 21*(10), 2183-2200. [https://doi.org/https://doi.org/10.1177/1461444819841890](https://doi.org/10.1177/1461444819841890)
- Mayring, P. (2014). Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173>
- McCabe, C. T., Watrous, J. R., & Galarneau, M. R. (2020). Trauma exposure, mental health, and quality of life among injured service members: Moderating effects of perceived support from friends and family. *Military Psychology, 32*(2), 164-175.  
<https://doi.org/10.1080/08995605.2019.1691406>
- McCants, N. (2022). *The Resource Allocation Process and the Effects on Cybersecurity Culture* (Doctoral dissertation, Capella University).

- McKinney, C. (2020, January 7). *Ban for former DWF trainee solicitor who emailed client information to a mate*. Legal Cheek. <https://www.legalcheek.com/2020/01/ban-for-former-dwf-trainee-solicitor-who-emailed-client-information-to-a-mate/>
- Meadows, S. O., Tanielian, T., Karney, B., Schell, T., Griffin, B. A., Jaycox, L. H., . . . Vaughan, C. A. (2017). The Deployment Life Study: Longitudinal analysis of military families across the deployment cycle. *Rand health quarterly*, 6(2).
- Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6(42). <https://doi.org/https://doi.org/10.1186/1748-5908-6-42>
- Miller, L. L., & Aharoni, E. (2015). *Understanding Low Survey Response Rates Among Young U.S. Military Personnel*. RAND Corporation.
- Ministry of Defence. (2013). *UK Armed Forces Annual Personnel Report*. <https://assets.publishing.service.gov.uk/media/5a7c9821ed915d12ab4bbd43/uk-af-personnel-report-1-april-2013-revised.pdf>
- Ministry of Defence. (2022). *UK Armed Forces Families Strategy 2022-32*. [https://assets.publishing.service.gov.uk/media/61e80893e90e07037ac9e10b/UK\\_Armed\\_Forces\\_Families\\_Strategy\\_2022\\_to\\_2032.pdf](https://assets.publishing.service.gov.uk/media/61e80893e90e07037ac9e10b/UK_Armed_Forces_Families_Strategy_2022_to_2032.pdf)
- Minkov, M., Bond, M. H., Dutt, P., Schachner, M., Morales, O., Sanchez, C., . . . Mudd, B. (2018). A Reconsideration of Hofstede's Fifth Dimension: New Flexibility Versus Monumentalism Data From 54 Countries. *Cross-Cultural Research* 52(3), 309-333. <https://doi.org/10.1177/1069397117727488>
- Minkov, M., Dutt, P., Schachner, M., Morales, O., Sanchez, C., Jandosova, J., . . . Mudd, B. (2017). A revision of Hofstede's individualism-collectivism dimension: A new national index from a 56-country study. *Cross Cultural & Strategic Management*, 24(3), 386-404. <https://doi.org/https://doi.org/10.1108/CCSM-11-2016-0197>
- Minkov, M., & Kaasa, A. (2020). A test of Hofstede's model of culture following his own approach. *Cross Cultural & Strategic Management*, 28(2), 383-406. <https://doi.org/https://doi.org/10.1108/CCSM-05-2020-0120>
- Montanez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.01755>
- Morrison, B., Coventry, L., & Briggs, P. (2021). How do Older Adults feel about engaging with Cyber-Security? *Human Behaviour & Emerging Technology*, 3, 1033-1049. <https://doi.org/10.1002/hbe2.291>
- National Cyber Security Centre. (2020). Using passwords to protect your devices and data. <https://www.ncsc.gov.uk/files/Using-passwords-protect-devices-data-infographic.pdf>
- Nathe, J. M., Oskoui, T. T., & Weiss, E. M. (2023). Parental Views of Facilitators and Barriers to Research Participation: Systematic Review. *Pediatrics*, 151(1). <https://doi.org/10.1542/peds.2022-058067>

- NHS England. (2024). *Armed Forces family life*.  
<https://www.england.nhs.uk/commissioning/armed-forces/armed-forces-family-life/>
- Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and Computer Security*, 27(2), 164-164.
- Neubaum, G., Metzger, M., Kramer, N., & Kyewski, E. (2023). How Subjective Norms Relate to Personal Privacy Regulation in Social Media: A Cross-National Approach. *Social Media + Society*, 9(3). <https://doi.org/10.1177/20563051231182365>
- Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). *Training and Embedding Cybersecurity Guardians in Older Communities* Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan.  
<https://doi.org/10.1145/3411764.3445078>
- Niehaves, B., & Plattfaut, R. (2014). Internet adoption by the elderly: employing IS technology acceptance theories for understanding the age-related digital divide. *European Journal of Information Systems*, 23(6), 708-726. <https://doi.org/10.1057/ejis.2013.19>
- Nikken, P. (2019). Parents' instrumental use of media in childrearing: Relationships with confidence in parenting, and health and conduct problems in children. *Journal of Child and Family Studies*, 28(2), 531-546.
- Ofcom. (2022). *Adults' Media Use and Attitudes report*.  
[https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0020/234362/adults-media-use-and-attitudes-report-2022.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0020/234362/adults-media-use-and-attitudes-report-2022.pdf)
- Office for National Statistics. (2019). *Milestones: journeying through adulthood*.  
<https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/milestonesjourneyingthroughadulthood/2019-12-17>
- Office for National Statistics. (2024). *National life tables – life expectancy in the UK: 2020 to 2022*.  
<https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/lifeexpectancies/bulletins/nationallifetablesunitedkingdom/2020to2022>
- O'Neal, C. W., Peterson, C., & Mancini, J. A. (2022). Military Adolescent's experiences of change and discontinuity: Associations with psychosocial factors and school success. *Family Relations*, 1-20.
- O'Neal, C. W., & Mancini, J. A. (2021). Military families' stressful reintegration, family climate, and their adolescents' psychosocial health. *Journal of Marriage and Family*, 83(2), 375-393.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66(May 2017), 40-51.  
<https://doi.org/https://doi.org/10.1016/j.cose.2017.01.004>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire

- (HAIS-Q). *Computers & security*, 42, 165-176.  
<https://doi.org/https://doi.org/10.1016/j.cose.2013.12.003>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611.  
<https://doi.org/https://doi.org/10.1016/j.cose.2011.12.010>
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cyber security: an integrated methodological approach. *Cognition, Technology & Work*, 24, 371-390.  
<https://doi.org/https://doi.org/10.1007/s10111-021-00683-y>
- Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2012). Variations in Information Security Cultures across Professions: A Qualitative Study. *Communications of the Association for Information Systems*, 33(11), 163-204. <https://doi.org/10.17705/1CAIS.03311>
- Rea, A., Marshall, K., & Farrell, D. (2022). Capability of web-based survey software: An empirical review. *American Journal of Business*, 37(1), 1-13.
- Rea, J., Behnke, A., Huff, N., & Allen, K. (2015). The Role of Online Communication in the Lives of Military Spouses. *Contemporary Family Therapy*, 37, 329-339.  
<https://doi.org/https://doi.org/10.1007/s10591-015-9346-6>
- Redmond, S. A., Wilcox, S. L., Campbell, S., Kim, A., Finney, K., Barr, K., & Hassan, A. M. (2015). A brief introduction to the military workplace culture. *Military Culture*, 9-20.  
<https://doi.org/10.3233/WOR-141987>
- Renaud, K., & Dupuis, M. (2020). *Cyber security fear appeals: unexpectedly complicated*. Proceedings of the New Security Paradigms Workshop, San Carlos, Costa Rica.  
<https://doi.org/10.1145/3368860.3368864>
- Rhee, H., Ryu, Y., & Kim, C. (2005). *I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security*. International Conference on Information Systems, Las Vegas, NV, USA.
- Ribeiro, S., Renshaw, K. D., & Allen, E. S. (2023). Military-related relocation stress and psychological distress in military partners. *Journal of Family Psychology*, 37(1), 45.
- Richardson, G. E. (2002). The metatheory of resilience and resiliency. *Journal of Clinical Psychology*, 58(3), 307-321. <https://doi.org/https://doi.org/10.1037/1942-9681.S.1.101>
- Romero, D. H., Riggs, S. A., & Ruggero, C. (2015). Coping, Family Social Support, and Psychological Symptoms Among Student Veterans. *Journal of Counseling Psychology*, 62(2), 242-252.
- Royal Air Force Families Federation (2020, June 10). *Get Safe Online: You, the internet and your wellbeing*. <https://www.raf-ff.org.uk/the-internet-and-your-wellbeing/>
- Royal Navy. (2024). *Families/Deployment: Keeping in Touch*.  
<https://www.royalnavy.mod.uk/families-and-veterans/families/keeping-in-touch#familygrams>

- Rözer, J., Mollenhorst, G., & Poortman, A. R. (2016). Family and friends: Which types of personal relationships go together in a network?. *Social Indicators Research*, 127, 809-826.
- Rubin, O. (2015). Contact between parents and adult children: The role of time constraints, commuting and automobility. *Journal of Transport Geography*, 49, 76-84.  
<https://doi.org/https://doi.org/10.1016/j.jtrangeo.2015.10.013>
- Rubinstein, I. (2012). Regulating Privacy by Design. *Berkeley Technology Law Journal*, 26, 1409.
- Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57, 442-451.  
<https://doi.org/https://doi.org/10.1016/j.chb.2015.12.037>
- Sandhu, R. S. (1992). Lattice-based enforcement of chinese walls. *Computers & Security*, 11(8), 753-763.
- Sciara, S., Contu, F., Bianchini, M., Chiocchi, M., & Sonnewald, G. G. (2021). Going public on social media: The effects of thousands of Instagram followers on users with a high need for social approval. *Current Psychology*, 1-15.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-131. <https://doi.org/https://doi.org/10.1023/A:1011902718709>
- Sepúlveda Estay, D. A., Rishikesh, S., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97.  
<https://doi.org/https://doi.org/10.1016/j.cose.2020.101996>.
- Sewart, M. R. (2022). *Understanding the experiences of military families* [Northumbria University].
- Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media*, 9(4), 475-480.  
<https://doi.org/http://dx.doi.org/10.1037/ppm0000247>
- Skinner, E. A. (1996). A Guide to Constructs of Control. *Journal of Personality and Social Psychology*, 71(3), 549-570.
- Skomorovsky, A. (2014). Deployment Stress and Well-being Among Military Spouses: The Role of Social Support. *Military Psychology*, 26(1), 44-54.  
<https://doi.org/http://dx.doi.org/10.1037/mil0000029>
- Smaliukiene, R., Labutis, G., & Juozapavicius, A. (2020). Pro-Environmental Energy Behavior in the Military: Assessing Behavior Change Factors at a Selected Military Unit. *Energies*, 13(219). <https://doi.org/10.3390/en13010219>
- Smith, D. (2015). Dual-military families: Confronting a stubborn military institution. In R. Moelker, M. Andres, G. Bowen, & P. Manigart (Eds.), *Military Families and War in the 21st Century* (pp. 57-72). Routledge.



- Soeters, J. L. (1997). Value Orientations in Military Academies: A Thirteen Country Study. *Armed Forces & Society*, 24(1), 7-32.
- Soeters, J. L., Winslow, D. J., & Weibull, A. (2007). Military Culture. In G. Caforio (Ed.), *Handbook of the Sociology of the Military*. Springer. [https://doi.org/https://doi.org/10.1007/0-387-34576-0\\_14](https://doi.org/https://doi.org/10.1007/0-387-34576-0_14)
- Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information & Computer Security*, 26(5), 533-550.
- Sommestad, T., & Hallberg, J. (2013). A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance. *Security and Privacy Protection in Information Processing Systems*, Berlin, Heidelberg.
- Spottswood, E. L., & Hancock, J. T. (2017). Should I Share That? Prompting Social Norms That Influence Privacy Behaviors on a Social Networking Site. *Journal of Computer-Mediated Communication*, 22(2), 55-70. <https://doi.org/10.1111/jcc4.12182>
- Sprecher, S., & Hendrick, S. S. (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social and Clinical Psychology*, 23(6), 857-877. <https://doi.org/DOI:10.1521/jscp.23.6.857.54803>
- SSAFA. (2024). *We are SSAFA*. <https://www.ssafa.org.uk/about-us>
- Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the Association for Computing Machinery*, 54(3), 70-75. <https://doi.org/10.1145/1897852.1897872>
- Strasser-Burke, N., & Symonds, J. (2020). Who Do You Want to Be Like? Factors Influencing Early Adolescents' Selection of Accessible and Inaccessible Role Models. *The Journal of Early Adolescence*, 40(7), 914-935. <https://doi.org/10.1177/0272431619880619>
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information systems research*, 1(3), 255-276.
- Stutzman, F., & Hartzog, W. (2012). Obscurity by Design: An Approach to Building Privacy into Social Media. ACM 2012 conference on Computer Supported Cooperative Work, Seattle, Washington, USA.
- Taipale, S., & Farinosi, M. (2018). The big meaning of small messages: The use of WhatsApp in intergenerational family communication. Human Aspects of IT for the Aged Population. Acceptance, Communication and Participation: 4th International Conference, Las Vegas, NV.
- Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, 17, 179-186. <https://doi.org/https://doi.org/10.1007/s10799-015-0252-2>
- Tellis, G. J., Prabhu, J. C., & Chandy, R. K. (2009). Radical innovation across nations: The preeminence of corporate culture. *Journal of marketing*, 73(1), 3-23.

- The British Army. (2024). *Hive Information Centres*. <https://www.army.mod.uk/people/health-wellbeing-welfare-support/hive/>
- The Culture Factor Group. (2024). *Country Comparison Tool*. <https://www.hofstede-insights.com/country-comparison-tool>
- The National. (2021, November 30). *Leaked video shows moment British F-25 jet crashes into Mediterranean Sea during take-off*. <https://www.thenationalnews.com/world/2021/11/30/leaked-video-shows-moment-british-f-35-jet-crashes-into-mediterranean-sea-during-take-off/>
- The National Academies of Science, Engineering & Medicine. (2019). *Strengthening the military family readiness system for a changing American society* (S. Menestrel & K. W. Kizer, Eds. Vol. 3). National Academies Press.
- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109. <https://doi.org/https://doi.org/10.1016/j.cose.2021.102387>
- Valkenburg, P. M., & Jochen, P. (2009). Social Consequences of the Internet for Adolescents: A Decade of Research. *Current Directions in Psychological Science*, 18(1), 1-5. <https://doi.org/https://doi.org/10.1111/j.1467-8721.2009.01595.x>
- Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts. *MIS quarterly*, 39(2), 345-366.
- Van Den Berg, P. T., & Wilderom, C. P. M. (2004). Defining, Measuring, and Comparing Organisational Cultures. *Applied Psychology*, 53(4), 570-582. <https://doi.org/10.1111/j.1464-0597.2004.00189>
- Vijayakumar, N., & Pfeifer, J. H. (2020). Self-disclosure during adolescence: exploring the means, targets, and types of personal exchanges. *Current Opinion in Psychology*, 31, 135-140. <https://doi.org/https://doi.org/10.1016/j.copsyc.2019.08.005>.
- Vuga, J., & Juvan, J. (2013). Work-family conflict between two greedy institutions - the family and the military. *Current Sociology*, 61(7), 1058-1077. <https://doi.org/https://doi.org/10.1177/0011392113498881>
- Vuga, J., & Juvan, J. (2013). Work-family conflict between two greedy institutions – the family and the military. *Current Sociology*, 61(7), 1058-1077. <https://doi.org/10.1177/0011392113498881>
- Wadsworth, S. M., Whiteman, S., Lester, P., Stander, V., & Christ, S. (2022). Parental Deployment and Military Children: A Century of Research. In J. E. Glick, V. King, & S. M. McHale (Eds.), *Parent-Child Separation: Causes, Consequences, and Pathways to Resilience* (Vol. 1, pp. 161-188). Springer.
- Wagner, N., Sahhin, C. S., Winterrose, M., Riordan, J., Hanson, D., Peña, J., & Streilein, W. W. (2016). Quantifying the mission impact of network-level cyber defensive mitigations. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 14(3). <https://doi.org/https://doi.org/10.1177/1548512916662924>

- Walker, R. A., Colclough, M., Limbert, C., & Smith, P. M. (2022). Perceived barriers to, and benefits of physical activity among British military veterans that are wounded, injured, and/or sick: a behaviour change wheel perspective. *Disability and rehabilitation*, 44(6), 900-908.
- Wallston, K. A., Wallston, B. S., Smith, S., & Dobbins, C. J. (1987). Perceived control and health. *Current Psychology*, 6, 5-25.
- Wang, Y.-C., Burke, M., & Kraut, R. (2016). Modeling Self-Disclosure in Social Networking Sites. 19th ACM conference on computer-supported cooperative work & social computing, San Francisco, CA.
- Ward, J., Dogan, H., Apeh, E., Mylonas, A., & Katos, V. (2017). Using human factor approaches to an organisation's Bring Your Own Device scheme. *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017*, Vancouver, Canada.
- Wankhede, C. (2024, January 2022). *Is WhatsApp safe to use? How does it ends-to-end encryption work?* Android Authority. <https://www.androidauthority.com/whatsapp-encryption-safe-3087607/>
- Weinstein, N. D. (1980). Unrealistic Optimism About Future Life Events. *Journal of Personality and Social Psychology*, 39(5), 806-820.
- WhatsApp. (2024). *StayConnected*. <https://www.whatsapp.com/stayconnected>
- Wilcox, K., Kramer, T., & Sen, S. (2011). Indulgence or Self-Control: A Dual Process Model of the Effect of Incidental Pride on Indulgent Choice. *Journal of Consumer Research*, 38(1), 151-163. <https://doi.org/10.1086/657606>
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88. <https://doi.org/https://doi.org/10.1016/j.cose.2019.101640>
- Williams, P. A. (2009). What does security culture look like for small organizations?. In *Proceedings of the 7th Australian Information Security Management Conference*.
- Wirth, A. (2017). The economics of cybersecurity. *Biomedical instrumentation & technology*, 51(s6), 52-59.
- Woodall, K. A., Esquivel, A. P., Powell, T. M., Riviere, L. A., Amoroso, P. J., & Stander, V. A. (2022). Influence of family factors on service members' decision to leave the military. *Family Relations*, 72(3), 1138-1157. <https://doi.org/10.1111/fare.12757>
- Wrzus, C., Hänel, M., Wagner, J., & Neyer, F. J. (2013). Social Network Changes and Life Events Across the Life Span: A Meta-Analysis. *Psychological Bulletin*, 139(1), 53-80. <https://doi.org/10.1037/a0028601>
- Wu, J., Zhou, J., Ma, J., Mei, S., & Ren, J. (2011). *An active data leakage prevention model for insider threat* 2011 2nd International Symposium on Intelligence Information Processing

and Trusted Computing,

- Yahav, I., Schwartz, D. G., & Silverman, G. (2014). Detecting unintentional information leakage in social media news comments. 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014),
- Zanchetta, C., Schiff, H., Novo, C., Cruz, S., & Vaz de Carvalho, C. (2022). Generational Inclusion: Getting Older Adults Ready to Own Safe Online Identities. *Education Sciences*, 12. <https://doi.org/https://doi.org/10.3390/educsci12100715>
- Zhang, X., & Yang, H. (2018). Impact of Cross-Culture on Behavioural Information Security. *Journal of Integrated Design and Process Science*, 22(2), 63-80. <https://doi.org/10.3233/JID180003>
- Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, 86, 914-925. <https://doi.org/https://doi.org/10.1016/j.future.2016.10.007>
- Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187. <https://doi.org/https://doi.org/10.1016/j.ijhcs.2019.05.005>
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62. <https://doi.org/10.1080/08874417.2020.1712269>

# Appendix A: Phase 1 Online Survey Questions

## Information sheet

### ***Exploring the role of Key Relations in cyber resilience within the Armed Forces***

Please take a look over the following information about the study before consenting to taking part.

---

**Study title:** Exploring the role of key friends and relations in cyber resilience within the Armed Forces (MODREC Application No: 2138/MODREC/ 22)

**Invitation to take part:** You are being invited to take part in this research as you have been identified as being helpful in providing insight on how those in close relationships with military employees can influence cyber resilience of military organisations.

Before you decide, it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information.

We would like you to take 24 hours 'thinking time' after reading this Participant Information Sheet and Consent Form to consider whether or not you wish to take part in the study.

#### **What is the purpose of this research?**

This study is the first phase of a research study which is collecting data on how those in close relationships with military employees can influence cyber resilience within military organisations. Cyber resilience is the ability to predict, withstand and recover from cyber-attacks.

#### **Who is doing the research?**

The research is being conducted by researchers at Bournemouth University and The Defence Science and Technology Laboratory (Dstl).

#### **What will I be asked to do?**

The first stage of this study will involve completing an online survey which will take about 10 minutes to complete. Questions asked within this questionnaire will consist of asking your age, gender and job role and who you consider to be a close relationship, as well as how frequently you contact friends and relatives.

#### **What are the direct benefits or possible disadvantages of taking part?**

There are no direct benefits to participants for taking part.

There are no disadvantages to taking part. There is the potential that the topics that arise in the survey may be triggering or sensitive to certain situations for some individuals, please do not answer any questions you do not feel comfortable answering please exit the survey if you do not wish to continue at any point.

Questions within the survey may give you the option to provide free-text responses, mostly with regards to disclosing those you have relationships with and what you communicate with them about. Due to the survey collecting information which potentially permits some identification (age, gender, job role and rank), please consider your responses when reporting sensitive relationships and non-compliant behaviours.

**Do I have to take part?**

No, participation is entirely voluntary. There are also no disadvantages if you choose to not participate in the research.

**Can I withdraw from the research and what will happen if I withdraw?**

You can withdraw at any point before or during the survey. Once you have clicked 'submit' on this questionnaire you are consenting to your responses being used within the research and you can no longer withdraw as it will not be possible to identify your responses. You will be reminded of this at the end of the survey. Your participation in or withdrawal from this survey will not affect yours, or anyone else's career.

**Will I receive any expenses or payments?**

You can claim experimental test allowance (ETA), currently at £3.06, per test. As the survey is considered two tests, £6.12, will be offered. The process for applying for this ETA will be detailed at the end of the survey.

**Who do I contact if I have any questions?**

*Name:* Francesca Kooner-Evans

*Tel No:* [REDACTED]

*E-mail:* fcoonerevans@bournemouth.ac.uk

**Who do I contact if I have a complaint?**

*Name:* Julie Turner-Cobb

*Tel No:* 01202 962039

*E-mail:* jturnercobb@bournemouth.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 online data will be stored in electronic format in password protected files, which only the named researchers will have access to. The data will be stored for 5 years in accordance with the ethical guidelines provided by the British Psychological Society. Data is processed in line with the Data Protection Act 2018 and uses the legal basis for processing your personal data of "consent" and a 'task in the public interest' and is for research purposes under GDPR and DPA 2018.

**Who has reviewed the study?** This study has been reviewed and given favourable opinion by the Ministry of Defence Research Ethics Committee (MODREC).

**Further Information and Contact Details**

Name : Francesca Kooner-Evans

Address: Poole House P335, Talbot Campus, Bournemouth University, Fern Barrow, Poole, BH12 5BB Tel No: [REDACTED]  
E-mail: fcoonerevans@bournemouth.ac.uk

Compliance with the Declaration of Helsinki This study will be conducted in accordance with the principles defined in the Declaration of Helsinki as adopted at the 64th WMA General Assembly at Fortaleza, Brazil in October 2013.

---

### Consent

The nature aims and risks of the research have been explained to me. I have read and understood the Participant Information Sheet provided in this survey and understand what is expected of me. All my questions have been answered fully to my satisfaction.

Yes

---

I understand that if I decide at any time during the research that I no longer wish to participate in this project, I can notify the researchers involved and be withdrawn from it immediately without having to give a reason. I also understand that I may be withdrawn from the study at any time by the research team. In neither case will this be held against me in subsequent dealings with the Ministry of Defence

Yes

---

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as confidential and handled in accordance with the provisions of the Data Protection Act 2018

Yes

---

This consent is specific to the particular study described in the Participant Information Sheet and shall not be taken to imply my consent to participate in any subsequent study or deviation from that detailed here

Yes

---

I understand that in the event of my sustaining injury, illness or death as a direct result of participating as a volunteer in this research, I or my dependants may enter a claim with the Ministry of Defence for compensation under the provisions of the no-fault compensation scheme, details of which are attached

Yes

---

I have had the opportunity to take 24 hours after reading the Participant Information Sheet and this Consent Form to consider whether or not I wish to take part in the study

Yes

---

I agree to participate in this study

Yes

---

If you do not consent to any of the above please exit the study by closing the browser

---

### Demographics

Q1) What is your age? (If you would prefer not to say, please put "prefer not to say")

\_\_\_\_\_

---

Q2) What gender do you identify as?

Male

Female

Non-binary

Prefer not to say

Gender identity not listed here (please specify)

\_\_\_\_\_

---

Q3) What is your job role?

\_\_\_\_\_



Q4) What is your job rank?

- OF-S (Officer Cadet)
  - OF-D (Mid / 2LT / Plt Off)
  - OF-1 (SLt /Lt /Fg Off)
  - OF-2 (Lt / Capt / Flt Lt)
  - OF-3 (Lt Cdr / Maj / Sqn Ldr)
  - OF-4 (Cdr / Lt Col / Wg Cdr)
  - OF-5 (Capt / Col / Gp Capt)
  - OF-6 (Cdre / Brig / Air Cdre)
  - OF-7 (RAdm / Maj Gen / AVM)
  - OF-8 (VAdm / Lt Gen / Air Mshl)
  - OF-9 (Adm / Gen / Air Chf Mshl)
  - OF-10 (AotF / FM / MRAF)
- 

Q5) What branch of the military do you serve?

- Army
  - Royal Navy
  - Royal Air Force
  - Civilian
- 

### Definitions

Throughout the survey the phrase "Social Media" will be used. Please consider this definition of social media when answering the questions which include social media.

Social media is websites and applications (apps) that enable users to create and share content or to participate in social networking. Examples include Facebook, Instagram and Tiktok, amongst others.

---

## Spouse

Q6) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

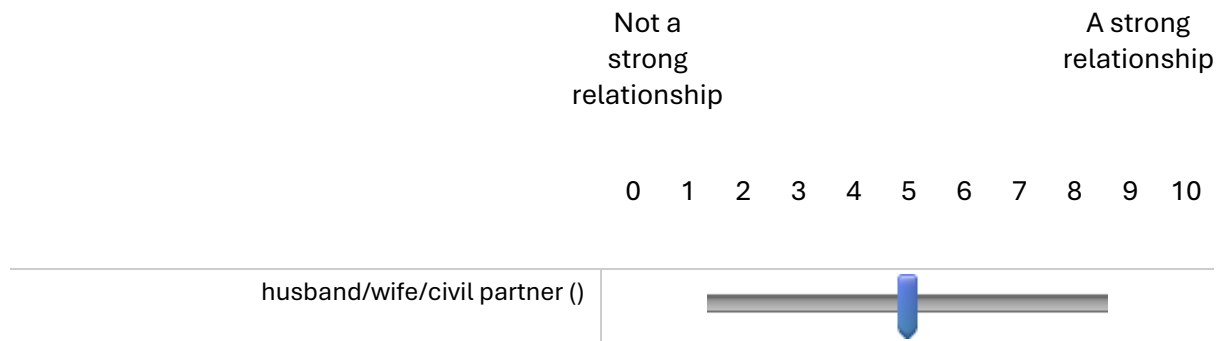
Assuming you have a husband/wife/civil partner, would you contact them?

Yes

No

*Display This Question: If Q6= Yes*

Q7) With these people that you communicate with (husband/wife/civil partner) how strong would you say this relationship is?



*Display This Question: If Q6= Yes*

Q8) Imagine you are on deployment, how often would you contact your husband/wife/civil partner?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Husband/wife/civil partner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q6= Yes

Q9) If you were communicating with your husband/wife/civil partner, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q6= Yes

Q10) Please select all the topics you might discuss when communicating with your husband/wife/civil partner

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Other family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

### Cohabiting Partner

Q11) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

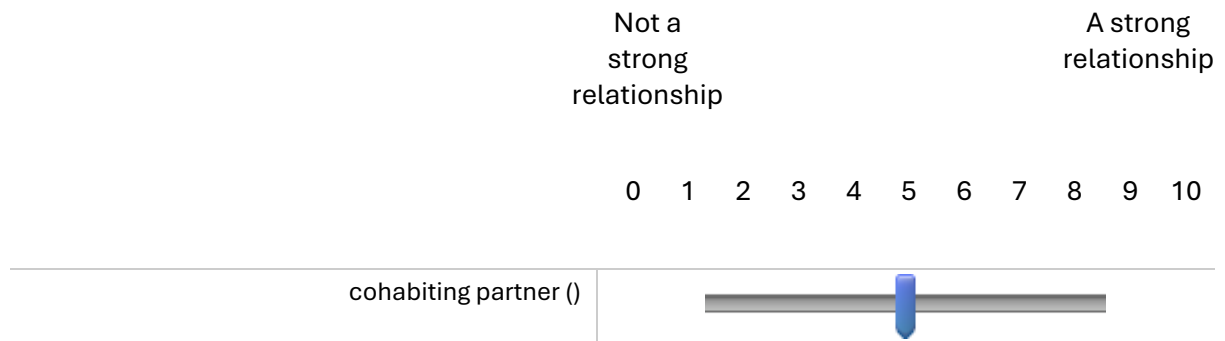
Assuming you have a cohabiting partner, would you contact them?

Yes

No

*Display This Question: If Q11= Yes*

Q12) With these people that you communicate with (cohabiting partner) how strong would you say this relationship is?



*Display This Question: If Q11= Yes*

Q13) Imagine you are on deployment, how often would you contact your cohabiting partner?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
cohabiting partner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q11= Yes

Q14) If you were communicating with your cohabiting partner, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q11= Yes

Q15) Please select all the topics you might discuss when communicating with your cohabiting partner

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Other family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

### Short term partner

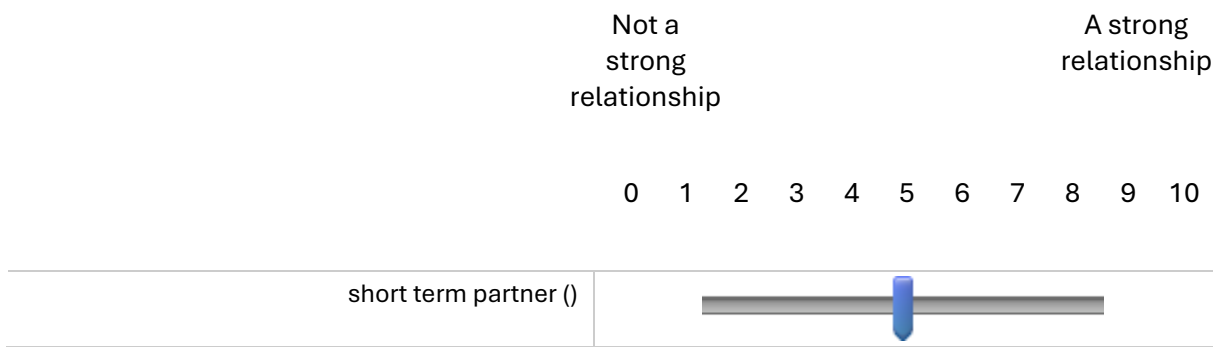
Q16) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

Assuming you have a short term partner (less than one year) would you contact them?

- Yes
- No

*Display This Question: If Q16= Yes*

Q17) With these people that you communicate with (short term partner) how strong would you say this relationship is?



*Display This Question: If Q16= Yes*

Q18) Imagine you are on deployment, how often would you contact your short term partner?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
short term partner	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q16= Yes

Q19) If you were communicating with your short term partner, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (Please state)
- 

Display This Question: If Q16= Yes

Q20) Please select all the topics you might discuss when communicating with your short term partner

- Your day to day work schedule e.g. How work was today (1)
  - Advice about personal problems (2)
  - Advice about work problems (3)
  - Their day to day activities e.g. what they did today (5)
  - Other family members (6)
  - Information about friends (8)
  - Information about colleagues (9)
  - Other (please specify) (10) \_\_\_\_\_
-

## Child

Q21) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

Assuming you have a son/daughter, would you contact them?

Yes

No

---

*Display This Question: If Q21 = Yes*

Q22) Imagine you are on deployment, how often would you contact your son/daughter?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Son/daughter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

---

*Display This Question: If Q21 = Yes*

Q23) If you were communicating with your son/daughter, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ Other (please state)
-



Display This Question: If Q21 = Yes

Q24) With these people that you communicate with (son/daughter) how strong would you say this relationship is?



Display This Question: If Q21 = Yes

Q25) Please select all the topics you might discuss when communicating with your child

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

#### Parent/Guardian


Q26) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

Assuming you have a parent/guardian, would you contact them?

- Yes
- No

Display This Question: If Q26 = Yes

Q27) With these people that you communicate with (parent/guardian) how strong would you say this relationship is?

	Not a strong relationship	A strong relationship								
	0	10								
Parent/guardian ()										

Display This Question: If Q26 = Yes

Q28) Imagine you are on deployment, how often would you contact your parent/guardian?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Parent/guardian	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q26 = Yes

Q29) If you were communicating with your parent/guardian, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ Whatsapp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ Other (please state)

Display This Question: If Q26 = Yes

Q30) Please select all the topics you might discuss when communicating with your parent/guardian

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

---

### Grandparent

Q31) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media, for messaging and video calls.

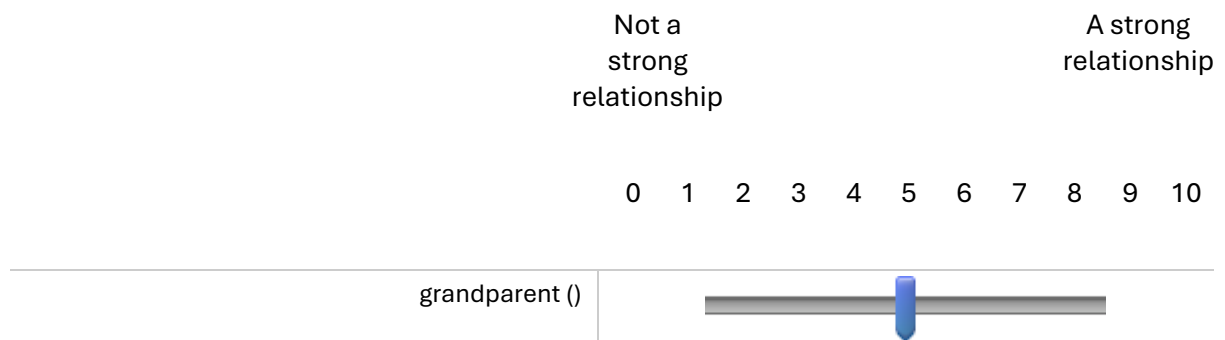
Assuming you have a grandparent, would you contact them?

- Yes
- No

---

Display This Question: If Q31 = Yes

Q32) With these people that you communicate with (grandparent) how strong would you say this relationship is?



Display This Question: If Q31 = Yes

Q33) Imagine you are on deployment, how often would you contact your grandparent?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
grandparent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q31 = Yes

Q34) If you were communicating with your grandparent, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ WhatsApp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ Other (please state)

Display This Question: If Q31 = Yes

Q35) Please select all the topics you might discuss when communicating with your grandparent

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

### Aunt/Uncle

Q36) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

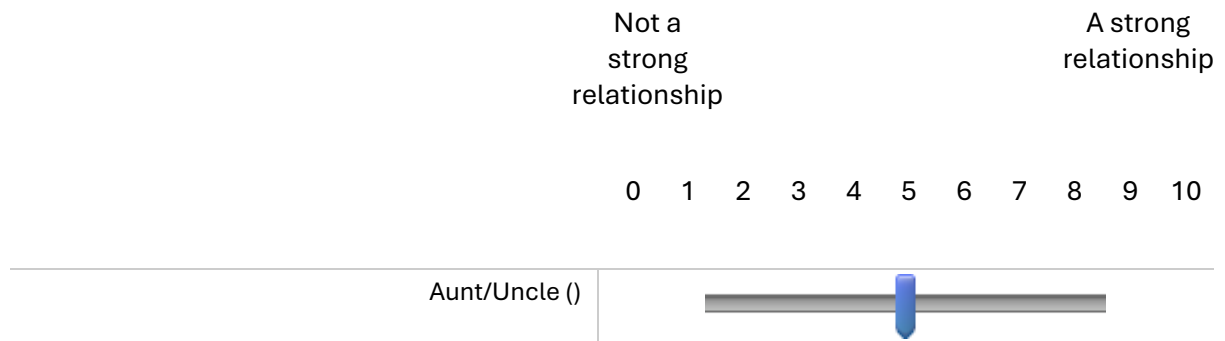
Assuming you have an aunt/uncle, would you contact them?

Yes

No

*Display This Question: If Q36 = Yes*

Q37) With these people that you communicate with (aunt/uncle) how strong would you say this relationship is?



*Display This Question: If Q36 = Yes*

Q38) Imagine you are on deployment, how often would you contact your aunt/uncle?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Aunt/uncle (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q36 = Yes

Q39) If you were communicating with your aunt/uncle, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q36 = Yes

Q40) Please select all the topics you might discuss when communicating with your aunt/uncle

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Other family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

### Cousin

Q41) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

Assuming you have a cousin, would you contact them?

Yes

No

*Display This Question: If Q41 = Yes*

Q42) Imagine you are on deployment, how often would you contact your cousin?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Cousin (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

*Display This Question: If Q41 = Yes*

Q43) With these people that you communicate with (cousin) how strong would you say this relationship is?

	Not a strong relationship	A strong relationship
	0	10
Cousin ()		

Display This Question: If Q41 = Yes

Q44) If you were communicating with your cousin, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q41 = Yes

Q45) Please select all the topics you might discuss when communicating with your cousin

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Other family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-



**Other individual 1**

Q46) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls.

Is there anyone else you would contact that has not already been mentioned?

(As mentioned in the information sheet - due to the survey collecting information which potentially permits some identification, please consider your responses when reporting sensitive relationships and non-compliant behaviours and only respond in a way with which you are comfortable).

Yes (please specify) \_\_\_\_\_

No

*Display This Question: If Q46 = Yes*

Q47) Please specify who this individual is

\_\_\_\_\_

*Display This Question: If Q46 = Yes*

Q48) With these people that you communicate with (other individual) how strong would you say this relationship is?

Not a strong relationship A strong relationship

0 1 2 3 4 5 6 7 8 9 10



Display This Question: If Q46 = Yes

Q49) Imagine you are on deployment, how often would you contact this other individual?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Other individual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q46 = Yes

Q50) If you were communicating with your this individual, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ Whatsapp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ Other (please state)

Display This Question: If Q46 = Yes

Q51) Please select all the topics you might discuss when communicating with this other individual

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

---

**Other individual 2**

Q52) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media, for messaging and video calls.

Is there anyone else you would contact that has not already been mentioned?

(As mentioned in the information sheet - due to the survey collecting information which potentially permits some identification, please consider your responses when reporting sensitive relationships and non-compliant behaviours and only respond in a way with which you are comfortable).

- Yes (please specify) \_\_\_\_\_
- No

---

Display This Question: If Q52 = Yes

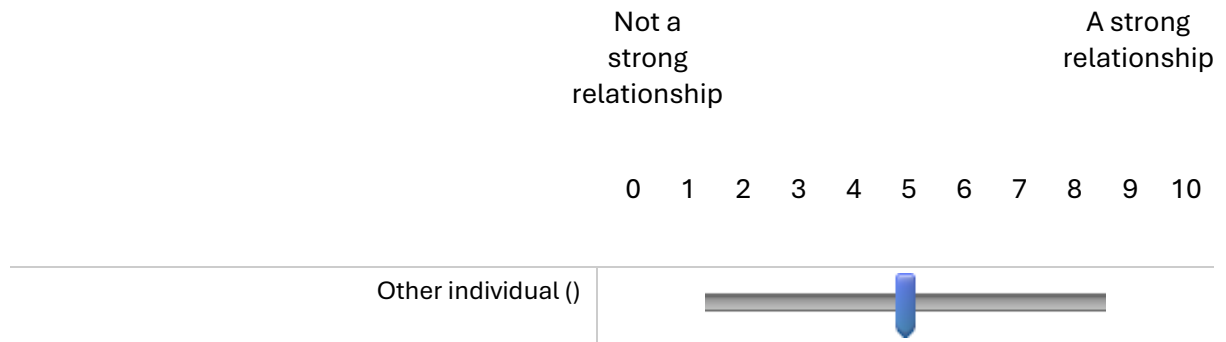
Q53) Please specify who this individual is

\_\_\_\_\_

---

Display This Question: If Q52 = Yes

Q54) With these people that you communicate with (other individual) how strong would you say this relationship is?



Display This Question: If Q52 = Yes

Q55) Imagine you are on deployment, how often would you contact this other individual via social media?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Other individual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q52 = Yes

Q56) If you were communicating with your this individual, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ Whatsapp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ Other (please state)

Display This Question: If Q52 = Yes

Q57) Please select all the topics you might discuss when communicating with this other individual

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Other family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

## Friends

Q58) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls

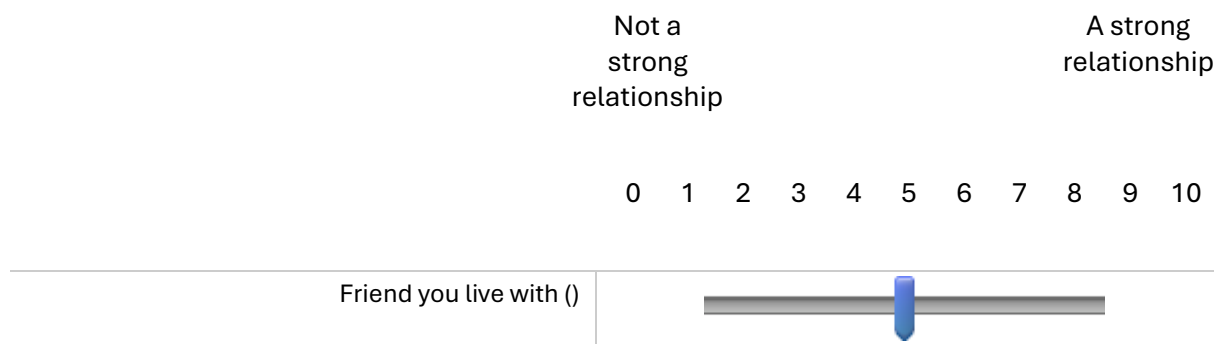
Assuming you have a friend you live with, would you contact them?

Yes

No

*Display This Question: If Q58 = Yes*

Q59) How strong would you say this relationship is with your friend you live with?



*Display This Question: If Q58 = Yes*

Q60) Imagine you are on deployment, how often would you contact your friend you live with?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Friend you live with	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

*Display This Question: If Q58 = Yes*

Q61) If you were communicating with your friend you live with, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ Whatsapp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
- \_\_\_\_\_ Other (please state)

*Display This Question: If Q58 = Yes*

Q62) Please select all the topics you might discuss when communicating with your friend you live with

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Information about family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

School friend

Q63) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls

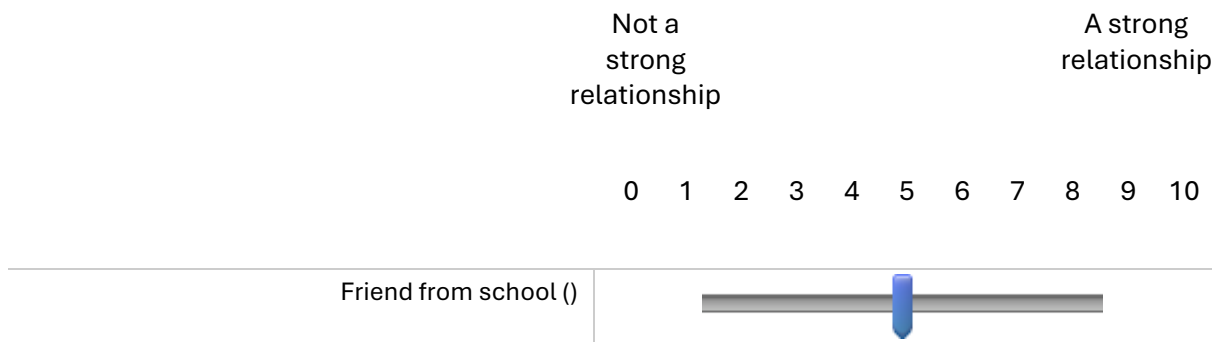
Assuming you have a friend from school, would you contact them?

Yes

No

Display This Question: If Q63 = Yes

Q64) How strong would you say this relationship is with your friend from school ?



Display This Question: If Q63 = Yes

Q65) Imagine you are on deployment, how often would you contact your friend from school?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
friend from school (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



*Display This Question: If Q63 = Yes*

Q66) If you were communicating with your friend from school, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (please state)
- 

*Display This Question: If Q63 = Yes*

Q67) Please select all the topics you might discuss when communicating with your friend from school

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Information about family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

### Family - Friend

Q68) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls

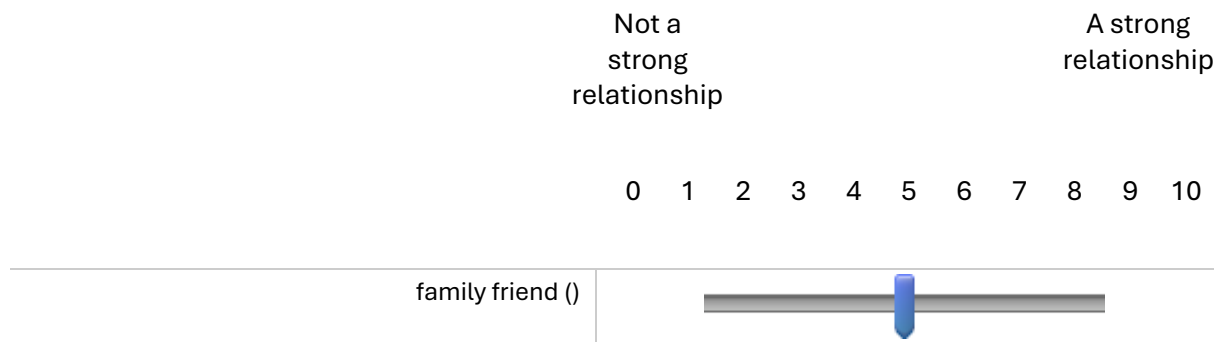
Assuming you have a family friend, would you contact them?

Yes

No

*Display This Question: If Q68 = Yes*

Q69) How strong would you say this relationship is with your family friend?



*Display This Question: If Q68 = Yes*

Q70) Imagine you are on deployment, how often would you contact your family friend?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
family friend (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q68 = Yes

Q71) If you were communicating with your family friend, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q68 = Yes

Q72) Please select all the topics you might discuss when communicating with your family friend

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Information about family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

**Online friend - met**

Q73) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls

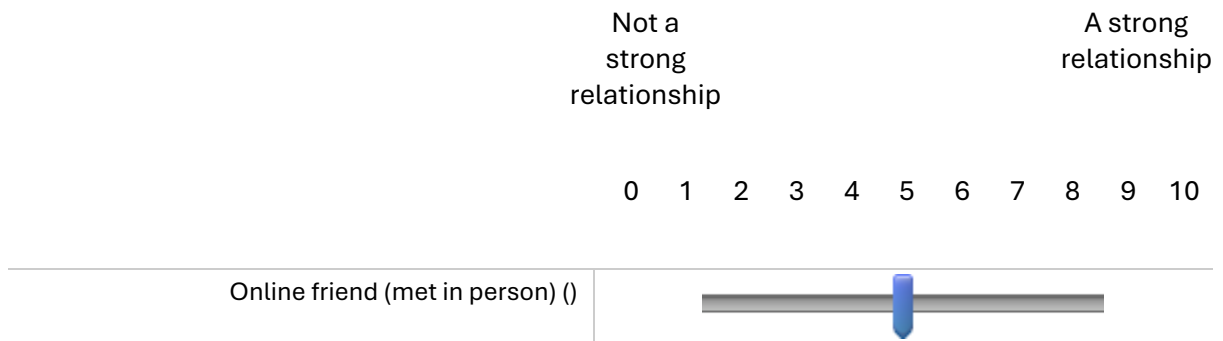
Assuming you have a friend you met online (but have since met in person), would you contact them?

Yes

No

*Display This Question: If Q73 = Yes*

Q74) How strong would you say this relationship is with your online friend (met in person)?



*Display This Question: If Q73 = Yes*

Q75) Imagine you are on deployment, how often would you contact your online friend (met in person)?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
online friend (met in person)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Display This Question: If Q73 = Yes

Q76) If you were communicating with your online friend (met in person), what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (please state)
- 

Display This Question: If Q73 = Yes

Q77) Please list any other methods of communication you would use to communicate with your online friend (met in person) with which were not included in the last question

---

Display This Question: If Q73 = Yes

Q78) Please select all the topics you might discuss when communicating with your online friend (met in person)

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Information about family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

Online friend - never met

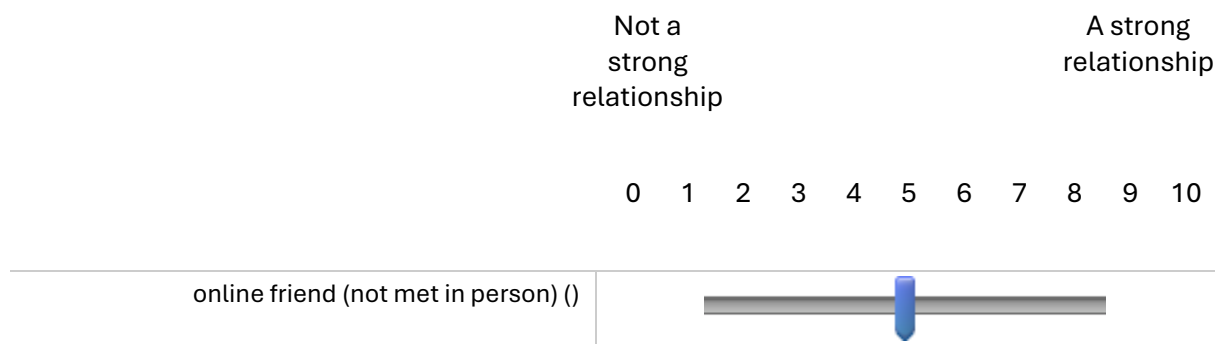
Q79) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media for messaging and video calls

Assuming you have a friend you have only ever spoken to online, would you contact them?

- Yes
- No

Display This Question: If Q79 = Yes

Q80) How strong would you say this relationship is with your online friend (not met in person)?



Display This Question: If Q79 = Yes

Q81) Imagine you are on deployment, how often would you contact your online friend (not met in person)?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
online friend (not met in person)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

*Display This Question: If Q79 = Yes*

Q82) If you were communicating with your online friend (not met in person), what is your preferred method of communication? Please rank from most preferred to least preferred.  
Note: You will have the option in the next question to list any others not included

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ A dating app e.g. bumble/tinder/hinge
  - \_\_\_\_\_ Other (please state)
- 

*Display This Question: If Q79 = Yes*

Q83) Please select all the topics you might discuss when communicating with your online friend (not met in person)

- Your day to day work schedule e.g. How work was today
  - Advice about personal problems
  - Advice about work problems
  - Their day to day activities e.g. what they did today
  - Information about family members
  - Information about friends
  - Information about colleagues
  - Other (please specify) \_\_\_\_\_
-

**Other individual 3**

Q84) Imagine you are on deployment and could not speak to those you are close to face-to-face and had to use social media, for messaging and video calls.

Is there anyone else you would contact that has not already been mentioned?

(As mentioned in the information sheet - due to the survey collecting information which potentially permits some identification, please consider your responses when reporting sensitive relationships and non-compliant behaviours and only respond in a way with which you are comfortable).

- Yes (please specify) \_\_\_\_\_
- No

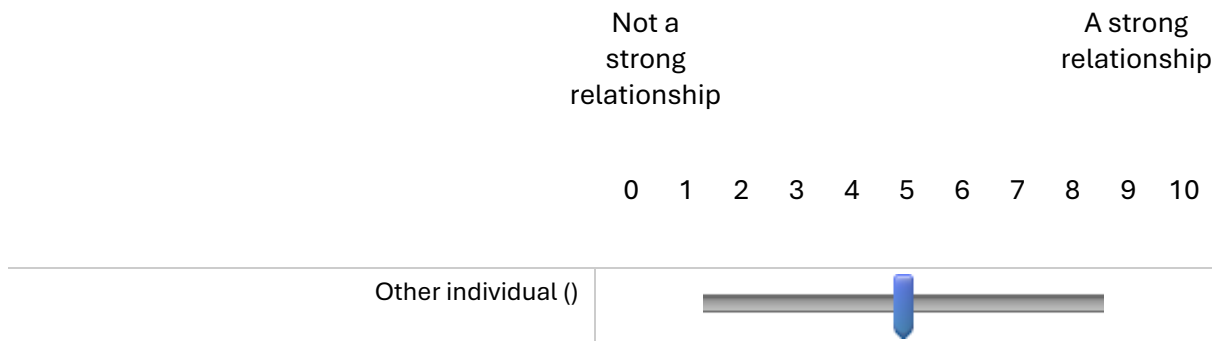
*Display This Question: If Q84 = Yes*

Q85) Please specify who this individual is

\_\_\_\_\_

*Display This Question: If Q84 = Yes*

Q86) With these people that you communicate with (other individual) how strong would you say this relationship is?



*Display This Question: If Q84 = Yes*

Q87) Imagine you are on deployment, how often would you contact this other individual via social media?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Other individual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



---

*Display This Question: If Q84 = Yes*

Q88) If you were communicating with your this individual, what is your preferred method of communication? Please rank from most preferred to least preferred.

- \_\_\_\_\_ Facebook
- \_\_\_\_\_ Text message/SMS
- \_\_\_\_\_ Email
- \_\_\_\_\_ Phone call
- \_\_\_\_\_ Instagram
- \_\_\_\_\_ Snapchat
- \_\_\_\_\_ Twitter
- \_\_\_\_\_ Whatsapp
- \_\_\_\_\_ Facetime
- \_\_\_\_\_ Skype
- \_\_\_\_\_ Other (please state)

---

*Display This Question: If Q84 = Yes*

Q89) Please select all the topics you might discuss when communicating with this other individual

- Your day to day work schedule e.g. How work was today
- Advice about personal problems
- Advice about work problems
- Their day to day activities e.g. what they did today
- Other family members
- Information about friends
- Information about colleagues
- Other (please specify) \_\_\_\_\_

### Consideration for platform

Q90) What is the most important consideration for platforms which influences how you choose to communicate with your relations?

---

Q91) What is the most important consideration for platforms which influences how you choose to communicate with your friends?

---

---

### Debrief

Thank you for participating in this study, your participation is greatly appreciated! If you have any questions or concerns regarding this study, please feel to contact the researcher, Francesca Kooner-Evans ([fkoonerevans@bournemouth.ac.uk](mailto:fkoonerevans@bournemouth.ac.uk)).

If you have any other concerns about this study or would like to speak with someone not directly involved in the research study, you may contact the Deputy Head of Department (Research) in Psychology at Bournemouth University, Julie Turner-Cobb ([jturnercobb@bournemouth.ac.uk](mailto:jturnercobb@bournemouth.ac.uk)).

**If you feel upset after having completed the study or find that some questions or aspects of the study triggered distress and feel you would like assistance, please contact:**

- TogetherAll - a smartphone app free for all serving personnel, veterans and families providing safe, anonymous support with trained counsellors.
- Samaritans – Available 24 hours a day on 116 123 to talk through concerns, worries and troubles.
- Combat Stress/rethink – Available 24 hours a day on 0800 138 1619 to provide emotional support, a listening ear and signposting service.

#### **How can I receive expenses or payment?**

You can claim experimental test allowance (ETA), currently at £3.06, per test. For completing this survey, you are able to claim for two tests (£6.12).

To ensure your responses in this survey remain anonymous, you will not be required to fill in any personal details. To claim ETA please email the chief investigator, Frankie Kooner-Evans at [fkoonerevans@bournemouth.ac.uk](mailto:fkoonerevans@bournemouth.ac.uk), with the subject line "**Cyber Resilience Research - ETA**"

The investigator will pass your request on to the Military Advisors for this study, in order for the ETA to be claimed.

Clicking the button below submits your responses to the survey. Please ensure that if you wish to complete the survey you click this button.

## Appendix B: Phase 2 Semi-Structured Interview Questions

*Before all interviews take place, the researcher will explain a little bit about themselves and the research, a script is included:*

Thank you for taking the time to talk to me today, before we start the interview, I am going to provide some information about myself and the research you have been asked to participate in. I am a student at Bournemouth University currently working towards a PhD with my research focussing on cyber resilience within military organisations – specifically in relation to friends and relatives of military personnel.

You have been asked to participate in this part of the research to provide an understanding about the online security behaviours of friends and relatives, from the perspective of an expert in the area. Please only provide as much information to any of the questions as you feel comfortable – and just to remind you that all identifiable information will be redacted following the interview. Where possible, please self-redact and anonymise descriptions of yourself and others during the discussion.

If you wish to stop the interview at any time just let me know and you do not need to provide a reason, there will be no detriment to you choosing to continue to participate or if you decide you do not want to participate.

Do you have any questions you wish to ask me about the interview?

Based on this, are you still happy to proceed with the interview?

### **Representatives of the military group**

#### **Opening Questions:**

Q) Please explain a little bit about your role, including how long you've been in this role - provide as much or little detail as you feel comfortable with

Q) Who would you describe as your close relations, in terms of whether that consists of family and/or friends? Provide as much or little detail as you feel comfortable with

#### **Friends and relatives specific**

Q) What online behaviours do you think your friends and relations exhibit that could present a cybersecurity risk to a military organisation?

- Prompt: Are there any risk behaviours that your friends and relations might exhibit on social media?
  - Further prompt: risk behaviours examples might include sharing locations online, speaking to people they do not know offline etc.
- Prompt: Can you think of any behaviours which could present a risk by you and your friends and relations communicating on a shared internet network, or by using the same devices such as a laptop or tablet?

- Further prompt: risk behaviours for sharing devices and networks might include access to sensitive information, sharing sensitive information due to poor password management etc.
- Follow up: why do you think these are risks?

Q) Please briefly explain what cybersecurity training and awareness you receive as part of your role?

- Prompt: If you haven't received any training yet in this role, can you briefly explain the cybersecurity training and awareness you received in a previous role?
- Follow up: What do you think is good about this training?
- Follow up: Is there anything that you think could be improved?

Q) What existing cybersecurity training and awareness programmes for friends and relations are you aware of?

- Follow up: What do you think would be good to include that isn't already?
- Follow up: Is there anything that you receive as part of your cybersecurity training that you think it would be good for friends and relations to receive also?

Q) Even though friends and relations of military employees can be a potential target for military adversaries, do you think the responsibility for their online behaviour should fall solely to them or others as well?

- Follow up: Why do you think the responsibility should fall to those individuals?
- Follow up: Can you provide any potential barriers of friends and relations being responsible for their own online behaviour?
  - Prompt: Do you think friends and relations would fully engage with a cybersecurity and awareness programme that they had to complete in their own time?

***Future research:***

Following this phase there will be 2 more Phases with the friends and relations themselves, to gain their perspectives of their own vulnerability. Phase 3 will be an online survey and phase 4 will be focus groups.

Q) What are the main things you think would be helpful to ask these individuals to which will help guide the formation of education and awareness programmes in the future?

**Subject matter experts (SMEs) with experience in delivering cybersecurity education and awareness**

***Opening Questions:***

Q) Please explain a little bit about your role, including how long you've been in this role - provide as much or little detail as you feel comfortable with

Q) Who would you describe as your close relations, in terms of whether that consists of family and/or friends? Provide as much or little detail as you feel comfortable with

### ***Friends and relatives specific***

Q) What online behaviours do you think friends and relations exhibit that could present a cybersecurity risk to a military organisation?

- Prompt: Are there any risk behaviours that your friends and relations might exhibit on social media?
  - o Further prompt: risk behaviours examples might include sharing locations online, speaking to people they do not know offline etc.
- Prompt: Can you think of any behaviours which could present a risk by you and your friends and relations communicating on a shared internet network, or by using the same devices such as a laptop or tablet?
  - o Further prompt: risk behaviours for sharing devices and networks might include access to sensitive information, sharing sensitive information due to poor password management etc.
- Follow up: why do you think these are risks?

Q) Please briefly explain what cybersecurity training and awareness you receive as part of your role?

- o Prompt: If you haven't received any training yet in this role, can you briefly explain the cybersecurity training and awareness you received in a previous role?
- Follow up: What do you think is good about this training?
- Follow up: Is there anything that you think could be improved?

Q) What existing cybersecurity training and awareness programmes for friends and relations are you aware of?

- Follow up: What do you think would be good to include that isn't already?
- Follow up: Is there anything that you receive as part of your cybersecurity training that you think it would be good for friends and relations to receive also?

Q) Even though friends and relations of military employees can be a potential target for military adversaries, do you think the responsibility for their online behaviour should fall solely to them or others as well?

- Follow up: Why do you think the responsibility should fall to those individuals?

### ***Future research:***

Following this phase there will be 2 more Phases with the friends and relations themselves, to gain their perspectives of their own vulnerability. Phase 3 will be an online survey and phase 4 will be focus groups.

Q) What are the main things you think would be helpful to ask these individuals to which will help guide the formation of education and awareness programmes in the future?

### **Subject matter experts (SMEs) with experience in cyber incident reporting and monitoring**

#### ***Opening Questions:***

Q) Please explain a little bit about your role, including how long you've been in this role - provide as much or little detail as you feel comfortable with

Q) Who would you describe as your close relations, in terms of whether that consists of family and/or friends? Provide as much or little detail as you feel comfortable with

Q) Please briefly explain what cybersecurity training and awareness you receive as part of your role?

- Follow up: What do you think is good about this training?
- Follow up: Is there anything that you think could be improved?

### ***Friends and relatives specific***

Q) What online behaviours do you think friends and relations exhibit that could present a cybersecurity risk to a military organisation?

- Prompt: Are there any risk behaviours that your friends and relations might exhibit on social media?
  - o Further prompt: risk behaviours examples might include sharing locations online, speaking to people they do not know offline etc.
- Prompt: Can you think of any behaviours which could present a risk by you and your friends and relations communicating on a shared internet network, or by using the same devices such as a laptop or tablet?
  - o Further prompt: risk behaviours for sharing devices and networks might include access to sensitive information, sharing sensitive information due to poor password management etc.
- Follow up: why do you think these are risks?

Q) What recommendations would you suggest, to mitigate against potential risks that friends and relations present to military organisations, when they're online?

Q) What do you think would be good to include in training and awareness programmes for friends and relations to address these behaviours?

- Is there anything that you receive as part of your cybersecurity training that you think it would be good for friends and relations to receive also?

Q) Even though friends and relations of military employees can be a potential target for military adversaries, do you think the responsibility for their online behaviour should fall solely to them or others as well?

- Why do you think the responsibility should fall to those individuals?

### ***Future research:***

Following this phase there will be 2 more Phases with the friends and relations themselves, to gain their perspectives of their own vulnerability. Phase 3 will be an online survey and phase 4 will be focus groups.

Q) What are the main things you think would be helpful to ask these individuals to which will help guide the formation of education and awareness programmes in the future?

## Appendix C: Phase 3 Online Survey Questions

### ***Exploring the role of Key Relations in cyber resilience within the Armed Forces***

Please read over the following information about the study before consenting to taking part.

---

#### **Participant Information Sheet**

**Study title:** Exploring the role of key friends and relations in cyber resilience within the Armed Forces (MODREC Application No: 2138/MODREC/ 22)

**Invitation to take part:** You are being invited to take part in this research as you identify as a friend or relative to a military service person, and this research seeks to explore the perspective of Key Relations of military personnel in how they influence cyber resilience of military organisations.

You will also be 16 years or older. If you are under 16 years of age, please do not complete this survey. If you are 16 or 17 years old, you should seek additional consent from a parent or legal guardian before completing this survey.

Before you decide, it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask the researchers if there is anything that is not clear or if you would like more information. We would like you to take 24 hours 'thinking time' after reading this Participant Information Sheet and Consent Form to consider whether or not you wish to take part in the study.

#### **What is the purpose of this research?**

This research project consists of four separate Phases of data collection, with the current study being the third phase. The aim of the research project is to explore how friends and relatives of military personnel can influence cyber resilience within organisations. Cyber resilience is the ability to predict, withstand and recover from cyber-attacks. This phase builds on Phases 1 & 2 which explored the perspective of military personnel and subject matter experts. The current phase aims to understand the perspective of friends and relatives themselves in relation to cyber resilience.

#### **Who is doing the research?**

The research is being conducted and match-funded by researchers at Bournemouth University and The Defence Science and Technology Laboratory (Dstl), which is part of the Ministry of Defence.

#### **Why have I been invited to take part?**

This phase of the research aims to recruit approximately 380 participants. You have been invited to take part because you are 16 years or older and identify as one of the following friends or relations:

- Wife/Husband/Civil Partner
- Short term partner (less than 1 year)
- Unmarried Partner
- Parent/Guardian

- Grandparent
- 'Extended family' e.g. Cousin/Aunt/Uncle/Niece/Nephew
- Co-habiting friend/roommate
- Friend from school
- Child
- 'Close' or 'Best' friend

**Do I have to take part?**

No, participation is entirely voluntary. There are no disadvantages if you choose not to participate in the research.

**What will I be asked to do?**

This phase will involve completing an online survey which will take about 20 minutes to complete.

The survey will begin by asking your age, gender and what friend/relation you identify as to your military person. Questions will then ask about your online communication behaviour with this individual. To finish, you will be asked about your understanding of your online risk, particularly with how you consider your military person and their information when behaving online.

**What are the direct benefits or possible disadvantages of taking part?**

There are no direct benefits to participants for taking part.

There are no disadvantages to taking part. There is the potential that the questions in the survey may be triggering or sensitive to situations for some individuals. Please do not answer any questions you do not feel comfortable answering. Please exit the survey if you do not wish to continue at any point.

Questions in the survey may give you the option to provide free-text responses. Due to the survey collecting information which potentially permits some identification (age, gender, military person's service branch), please consider your responses when discussing sensitive information.

**Can I withdraw from the research and what will happen if I withdraw?**

You can withdraw at any point before or during the survey. Once you have clicked 'submit' on this questionnaire you are consenting to your responses being used within the research. After you have clicked 'submit' we are not able to identify your responses, and so you will not be able to withdraw. You will be reminded of this at the end of the survey.

Your participation in or withdrawal from this survey will not affect your service person's career.

**Will I receive any expenses or payments?**

After completing the survey you can choose to enter into a prize draw for a £25 Amazon Voucher. There are 4 x £25 vouchers available. The process for entering the prize draw will be explained at the end of the survey.

**Who do I contact if I have any questions?**

Name: Francesca Kooner-Evans

Tel No: [REDACTED]



*E-mail:* fcoonerevans@bournemouth.ac.uk

**Who do I contact if I have a complaint?**

*Name:* Julie Turner-Cobb

*Tel No:* 01202 962039

*E-mail:* jturnercobb@bournemouth.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 online data will be stored in electronic format in password protected files, which only the named researchers will have access to. The data will be stored for 5 years in accordance with the ethical guidelines provided by the British Psychological Society. Data is processed in line with the Data Protection Act 2018 and uses the legal basis for processing your personal data "where we have your informed consent" and is for research purposes under GDPR and DPA 2018. Please see the MOD privacy notice for more details.

**Who has reviewed the study?** This study has been reviewed and given favourable opinion by the Ministry of Defence Research Ethics Committee (MODREC).

**Further Information and Contact Details**

*Name :* Francesca Kooner-Evans

*Address:* [REDACTED]  
[REDACTED]

*E-mail:* fcoonerevans@bournemouth.ac.uk

Compliance with the Declaration of Helsinki This study will be conducted in accordance with the principles defined in the Declaration of Helsinki as adopted at the 64th WMA General Assembly at Fortaleza, Brazil in October 2013.

---

**Start of Block: Consent**

We would now like you to read through the Consent Form questions below. Once you have read through, please take 24 hour 'thinking time' to consider whether or not you wish to take part in the study.

I have had the opportunity to take 24 hours after reading the Participant Information Sheet and this Consent Form to consider whether or not I wish to take part in the study.

Yes

---

The nature, aims and risks of the research have been explained to me. I have read and understood the Participant Information Sheet (version 1) and understand what is expected of me. All my questions have been answered fully to my satisfaction.

Yes

---

I understand that if I decide at any time during the research that I do not want to participate in this project, I can withdraw from the study by exiting the browser, and without giving a reason.

I also understand that I may be withdrawn from the study at any time by the research team. Neither of these things will be held against me in future contact with the Ministry of Defence

Yes

---

I consent to the processing of my personal information for the purposes of this research study. I understand that information will be treated as confidential and handled in accordance with the provisions of the Data Protection Act 2018

Yes

---

This consent is specific to the study described in the Participant Information Sheet and shall not be taken to imply my consent to participate in any future study or deviation from details outlined to me.

Yes

---

I understand that in the event of my sustaining injury, illness or death as a direct result of participating as a volunteer in this research, I or my dependents may enter a claim with the Ministry of Defence for compensation under the provisions of the no-fault compensation scheme, details of which can be found in the following document: [Arrangements for the payment of no fault compensation to participants in modrec approved studies](#)

Yes

---

I can confirm I am 16 years old or above

Yes

---

I agree to participate in this study

Yes

---

If you do not consent to any of the above please exit the study by closing the browser.

---

### Start of Block: Demographics

Q1) What is your age? (If you would prefer not to say, please put "prefer not to say")

---

---

Q2) What gender do you identify as?

- Male
  - Female
  - Non-binary
  - Prefer not to say
  - Gender identity not listed here (please specify)
- 
- 

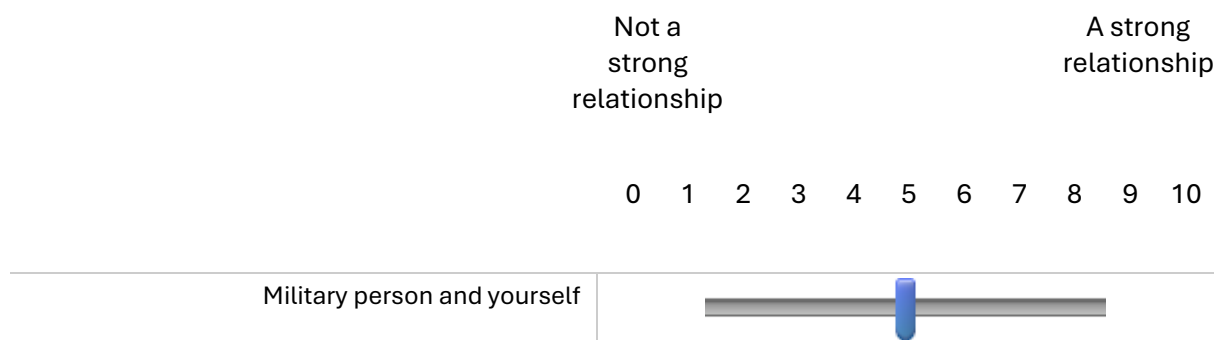
Q3) What branch of the military does your military person serve?

- Army
  - Royal Navy
  - Royal Air Force
  - Civilian
- 
-

Q4) What relation is your military person to you?

- Husband/Wife/Civil Partner
- Unmarried partner
- Short term partner (less than 1 year)
- Child
- Parent/Guardian
- Brother/Sister
- Grandchild
- Aunt/Uncle
- Niece/Nephew
- Cousin
- School friend
- Best/Close friend
- Online friend
- Family friend
- Other (please specify) \_\_\_\_\_

Q5) With this individual - how strong would you say this relationship is?



---

Start of Block: Communication frequency & platform considerations

Q6) Imagine your military person is on deployment, how often would you contact them?

	Once a year	Twice a year	Once a month	2 to 3 times a month	Once a week	Everyday (when possible)
Military Person	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

---

Q7) When communicating with this individual, what is your preferred method of communication? Please rank from most preferred **(1)** to least preferred **(10)**.

For platforms which you do not use, please enter 0 next to them.

- \_\_\_\_\_ Facebook
  - \_\_\_\_\_ Text message/SMS
  - \_\_\_\_\_ Email
  - \_\_\_\_\_ Phone call
  - \_\_\_\_\_ Instagram
  - \_\_\_\_\_ Snapchat
  - \_\_\_\_\_ Twitter
  - \_\_\_\_\_ Telegram
  - \_\_\_\_\_ Whatsapp
  - \_\_\_\_\_ Facetime
  - \_\_\_\_\_ Skype
  - \_\_\_\_\_ BeReal
  - \_\_\_\_\_ Discord
  - \_\_\_\_\_ LinkedIn
  - \_\_\_\_\_ Dating App (e.g. Tinder/Bumble/Hinge)
  - \_\_\_\_\_ Other (please state)
- 

Q8) What is the most important consideration for platforms which influences how you choose to communicate with this military person?

\_\_\_\_\_

---

Q9) Based on your opinion and knowledge of online safety, are there any platforms you think to be more secure than others? Please state these platforms here

\_\_\_\_\_

Q10) Please provide a brief justification for why you think the platform(s) you identified in the previous question are more secure.

---

**Start of Block: Risk Behaviour Questions**

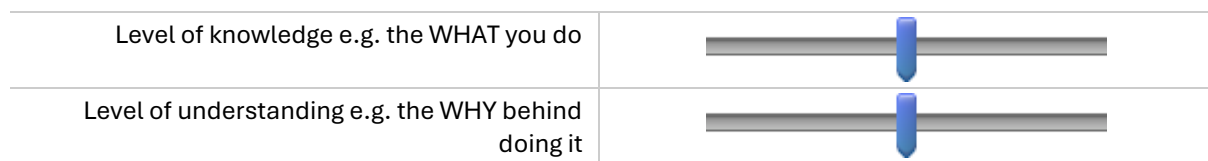
Q11) Please indicate your confidence in your **knowledge** and **understanding** of cybersecurity risk and behaviours you can engage in to protect yourself and others online.

An example of **knowledge** of a behaviour to reduce an online risk would be ensuring all social media networks profiles (e.g. Facebook) are set to private.

An example of **understanding** would be knowing that engaging in this safety behaviour reduces the amount of personal information that is available to be used by a malicious individual.

I have limited confidence in my knowledge/understanding    I am fairly confident but my level of knowledge/understanding could be improved    I feel very confident in my knowledge/understanding

0   1   2   3   4   5   6   7   8   9   10



Page Break

---

The following questions focus on your online behaviour and the choices that you make in relation to keeping **yourself** and **your own** information safe online.

Q12) Please indicate the level of cyber risk you think is demonstrated by engaging in these online behaviours

	No risk	Some risk	Unsure	A little risk	Extensive risk	Not applicable because I don't use this platform
Sharing your location in a post e.g. on instagram/facebook/twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sharing your location in a story e.g. Snapchat/whatsapp/facebook/instagram	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Being tagged in a picture by your colleagues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Being tagged in a picture by your family	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Being tagged in a picture by your friends	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Turning your geolocation settings on in your social networking apps e.g. Facebook/Instagram/Twitter/BeReal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Making your profile private (not public) e.g. on instagram/twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

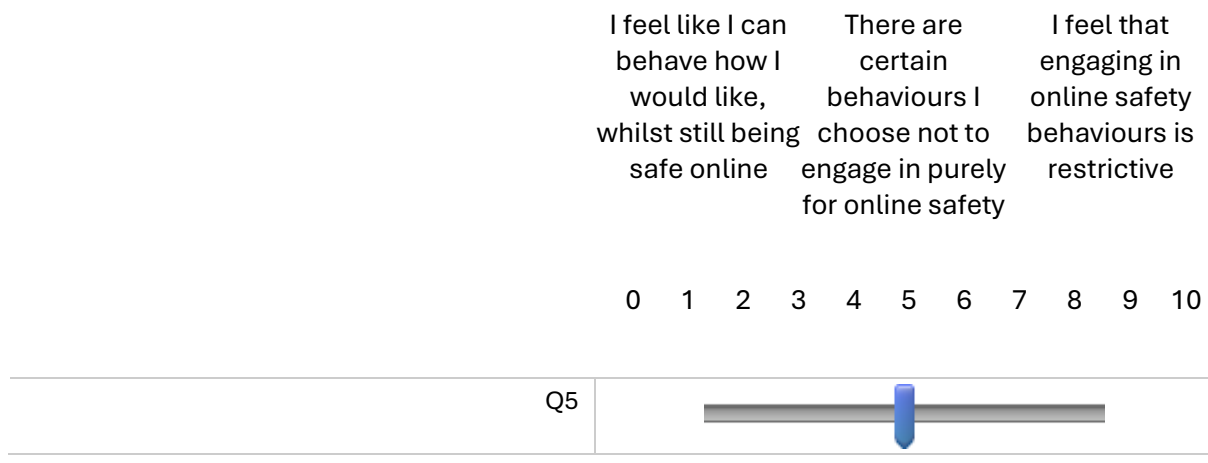
Q13) Please indicate what behaviours you engage in to keep yourself and your information safe online

	Yes	No	Uncertain	N/A because I don't have this device or platform
Anti-virus installed on your phone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-virus installed on your laptop	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-virus installed on a tablet (e.g. Ipad/Microsoft Surface/Samsung Tab...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use different passwords for different accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable auto-updates on devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable auto-updates on communication platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable two factor-authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Connect to public wi-fi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q14) To what extent do you think that engaging in online safety behaviours is restrictive on your online behaviours?



For example, not posting your location when on holiday.



The following questions focus on your online behaviour and the choices that you make in relation to keeping **your military person's** information safe online.

This includes information about the individual e.g. their role and rank, but also their unit e.g. location.

Q15) Please indicate the level of cyber risk you think is demonstrated by engaging in these online behaviours.

	No risk	Some risk	Unsure	A little risk	Extensive risk
Sharing location of your military counterpart in a post e.g., on Instagram/Facebook/Twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sharing location of your military counterpart in a story on Snapchat/WhatsApp/Facebook/Instagram	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagging your military counterpart in pictures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Geo-location settings switched on	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Making your profile private (not public) e.g., on Instagram/twitter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q16) Please indicate what behaviours you engage in to keep your military person's information safe online.

	Yes	No	Uncertain	N/A because I don't have this device or platform
Anti-virus installed on your phone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-virus installed on your laptop	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-virus installed on a tablet (e.g. Ipad/Microsoft Surface/Samsung Tab...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use different passwords for different accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable auto-updates on devices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable auto-updates on communication platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enable two factor-authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Connect to public wi-fi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q17) To what extent do you think that engaging in online safety behaviours is restrictive on your online behaviours?

For example, not sharing where your military person is deployed before they return home

I feel like I can behave how I would like, whilst still being safe online  
 There are certain behaviours I choose not to engage in purely for online safety  
 I feel that engaging in online safety behaviours is restrictive

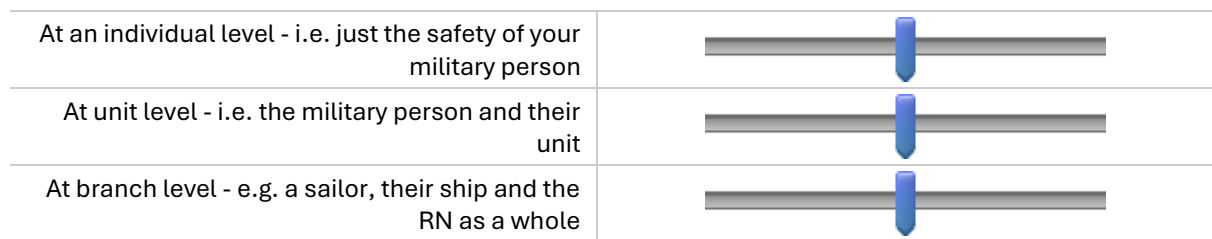
0 1 2 3 4 5 6 7 8 9 10



Q18) To what extent do you think your online behaviour influences the safety of your military person from a military adversary?

No influence at all  
 Some influence but not a lot  
 My behaviour has a direct influence

0 1 2 3 4 5 6 7 8 9 10



Start of Block: Training, awareness & education

Q19) Have you ever been invited to or attended any cybersecurity training from a military organisation?

Yes

No

---

\* Display if Q19 = Yes

Q20) If yes to the previous question, please describe the nature of this training including what it consisted of and who provided it.

---

---

Q21) Have you ever received any education and awareness materials e.g., leaflet, emails or been forwarded a link on cybersecurity from a military organisation?

Yes

No

---

\* Display if Q21 = Yes

Q22) If yes to the previous question, please describe the nature of these materials including an overview of the content and who provided it.

---

---

Q23) If you were given the opportunity to attend an annual brief providing you with an overview of the online threats you should be aware of and how to behave in a way that protects your military service person, would this be something you would attend?

	Yes	No	Perhaps, depending on other factors
Would you attend a cybersecurity briefing for friends and relatives of military persons?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q24) Please state any barriers that would prevent you from engaging with any cybersecurity initiatives, such as the one mentioned above.

---

---

### Start of Block: Future Phases Google Form

Thank you for completing all the survey questions! The final phase of this research will focus on building on these responses in online focus groups. Particularly focusing on the needs and wants of friends and relatives for Cybersecurity training, education and awareness.

If this sounds like something you would be interested in hearing more about, please follow this link to a google form to enter a contact email address: <https://forms.gle/zfYg6uGEyzXtXLd18>

This process ensures the response to your survey remains anonymous, as there is no way of connecting your email to the survey response. The information from this email will be stored separately to any study data and it will be used purely for prize draw purposes, before being destroyed.

If not, please head to the next section which explains the £25 Amazon voucher prize draw and directions to support services.

---

### Start of Block: Debrief

Thank you for participating in this study, your participation is greatly appreciated! Please read the following information and ensure **you click the submit button** at the bottom of the page once completed.

If you have any questions or concerns regarding this study, please feel to contact the researcher, Francesca Kooner-Evans ([fkoonerevans@bournemouth.ac.uk](mailto:fkoonerevans@bournemouth.ac.uk)).

If you have any other concerns about this study or would like to speak with someone not directly involved in the research study, you may contact the Deputy Head of Department (Research) in Psychology at Bournemouth University, Julie Turner-Cobb ([jturnercobb@bournemouth.ac.uk](mailto:jturnercobb@bournemouth.ac.uk)).

**If you feel upset after having completed the study or find that some questions or aspects of the study triggered distress and feel you would like assistance, please contact:**

- TogetherAll - a smartphone app free for all serving personnel, veterans and families providing safe, anonymous support with trained counsellors.
- Samaritans – Available 24 hours a day on 116 123 to talk through concerns, worries and troubles.
- Combat Stress/rethink – Available 24 hours a day on 0800 138 1619 to provide emotional support, a listening ear and signposting service.

- The Ripple Pond - Available on 0333 900 1028 and via email at [help@theripplepond.org](mailto:help@theripplepond.org) to support adult family members of physically or psychologically injured British Forces personnel and veterans.
- 

### **How can I enter the Amazon voucher prize draw?**

There are 4 x £25 Amazon vouchers to win in a prize draw for participants of this survey.

To be entered please follow the link and enter your name and email here: <https://forms.gle/9kBfiye5rhiaNa1k8>

This process ensures the response to your survey remains anonymous, as there is no way of connecting your email to the survey response. The information from this email will be stored separate to any study data and it will be used purely for prize draw purposes, before being destroyed.

---

Clicking the button below submits your responses to the survey. Please ensure that if you wish to complete the survey you click this button.

**End of Survey**

## **Study Title: Exploring the role of key friends and relations in cyber resilience within the Armed Forces**

### **RECRUITMENT FOR AN ONLINE SURVEY**

We're looking for participants over the age of 18 who are serving military members.

Dstl, in partnership with Bournemouth Uni, are co-funding some PhD research exploring how friends and relatives can influence organisational cyber resilience within a military context.

We're asking participants to complete an online survey which will explore the online behaviours of friends and relations, to help develop and direct future cyber security education and awareness materials.



If this is something you are interested in, please following the link to the research survey here:

[https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV\\_ereZQGt4j94g5My](https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV_ereZQGt4j94g5My)

The survey will close on **March 31st** and no further responses will be collected.

## Appendix E: Phase 3 Advert



RECRUITMENT FOR A 20-MINUTE ONLINE SURVEY:



### How to engage with the extended military community to keep themselves and their military person safe online

We're looking for individuals who are:

- A relative or friend of serving military members
- 16 years or older

Gathering opinions from friends and relatives on your experiences of online risk and online behaviours

For a chance of winning 1 of 4 x £25 Amazon vouchers by participating.

Copy the link below, scan the QR code below, or email the researcher.

The survey will close on January 31<sup>st</sup> 2024.

[https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV\\_ebxDaShEnJdZ2lw](https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV_ebxDaShEnJdZ2lw)



Link to survey



Please take a copy of the researchers email or the survey website

koonerevans@  
bournemouth.ac.uk

koonerevans@  
bournemouth.ac.uk

koonerevans@  
bournemouth.ac.uk

koonerevans@  
bournemouth.ac.uk

koonerevans@  
bournemouth.ac.uk

koonerevans@  
bournemouth.ac.uk

[https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV\\_ebxDaShEnJdZ2lw](https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV_ebxDaShEnJdZ2lw)

[https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV\\_ebxDaShEnJdZ2lw](https://bournemouthpsych.eu.qualtrics.com/jfe/form/SV_ebxDaShEnJdZ2lw)



## Appendix F: MODREC Letter of Favourable Opinion for Phases 1 & 2



**MODREC Secretariat**  
**Defence Science and Technology**

Dstl Portsdown West, Fareham, PO17 6AD  
Telephone: 0300 153 5372  
E-mail: [DST-MODRECTeam@mod.gov.uk](mailto:DST-MODRECTeam@mod.gov.uk)



Our Reference: 2138/MODREC/22

Date: 15 Jun 2022

Dear Francesca,

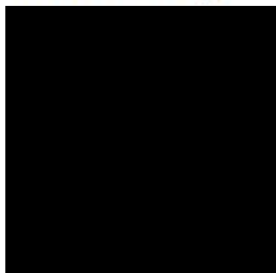
***Exploring the role of key friends and relations in cyber resilience within the Armed Forces – V4.1***

Thank you for submitting your revised application (2138/MODREC/22) with tracked changes and the covering letter with detailed responses to the MODREC letter. I can confirm that the revised protocol has been given favourable opinion ex-Committee.

This favourable opinion is valid for the duration of the research and is conditional upon adherence to the protocol – please inform the Secretariat if any amendment becomes necessary.

Please note that under the terms of JSP 536 you are required to notify the Secretariat of the commencement date of the research, and submit annual and final/termination reports to the Secretariat on completion of the research.

Yours sincerely,



## Appendix G: Bournemouth University letter of Ethical Approval for Phases 1 & 2



Dear Francesca Kooner-Evans,

Your checklist (Exploring the role of key friends and relations in cyber resilience within the Armed Forces) has now been reviewed and **APPROVED** in line with **BU's Research Ethics Code of Practice**.

The reviewer provided the following comments:

No additional comments provided

You can now save and/or print off a hard copy of the checklist at <https://ethics.bournemouth.ac.uk>.

This approval relates to the ethical context of the work. Specific aspects of the implementation of the research project remain your professional responsibility.

It is your responsibility to ensure that where the scope of the research project changes, such changes are evaluated to ensure that the ethical approval you have been granted remains appropriate.

Should you need to make any modifications to your project e.g. request an extension, increase the number participants (recruitment), submit an Amendment Request via the online ethics checklist. Requests will be considered by the original Approver. Changes cannot be implemented until relevant approvals are in place. See 'Amendments' for further guidance.

*Students – if the scope of your research changes, please discuss with your Tutors/Supervisors before submitting a new checklist or an Amendment Request.*

Many thanks

For UG/PGT enquiries – please contact your Supervisor in the first instance

## Appendix H: Theme table for themes from Thematic Analysis of the Phase 2 pilot study

Themes	Subthemes	Codes
Defining close relations	Defining close relations as dependents	<ul style="list-style-type: none"> <li>• Consider partner and parents close relations [PS1]</li> <li>• Close knit family consists of wife and children [PS2]</li> <li>• Parents and siblings also considered close relations [PS2]</li> </ul>
	Different approaches to relationships	<ul style="list-style-type: none"> <li>• More functional relationship with parents than partner [PS1]</li> <li>• Would be more ruthless with own parents compared with in-laws when discussing online behaviour [PS1]</li> <li>• Different approach for information security when considering family, friends and unknown civilians [PS2]</li> </ul>
	Maintenance of non-Key Relationships	<ul style="list-style-type: none"> <li>• Other relationships not considered close relations are maintained but not a priority [PS1]</li> <li>• Monthly or fortnightly contact with other relationships due to other priorities, such as a family [PS1]</li> </ul>
The role of individual differences in friends and relatives online behaviour	Generational differences influence behaviour	<ul style="list-style-type: none"> <li>• Humans choose to hide behind age as an excuse [PS1]</li> <li>• With aging they've chosen not to learn, rather than losing the ability to [PS1]</li> <li>• Decision to focus on learning what is required rather than wanting to learn everything possible [PS1]</li> <li>• Facebook considered old by children [PS2]</li> <li>• Youngest children don't have Facebook account [PS2]</li> </ul>
	Adopting military culture	<ul style="list-style-type: none"> <li>• Family experience of relocating for military job [PS2]</li> <li>• Wife wouldn't post anything due to being in military when younger and being military spouse for a long time [PS2]</li> <li>• Strong family background of security due to military experience means children have online awareness [PS2]</li> </ul>

		<ul style="list-style-type: none"> <li>• Family approach to security is second nature due to experience of military life [PS2]</li> <li>• Example of child creating a video involving themselves and other military families that was vetted to ensure no information shared that could be compromising [PS2]</li> <li>• No requirement to keep information secure by someone not regulated by military rules [PS2]</li> </ul>
	Difference in threat acceptance	<ul style="list-style-type: none"> <li>• Reducing online presence is a priority for military personnel not civilians [PS1]</li> <li>• For F&amp;Rs posting online is a nice memory, compared to military person it's sensitive information [PS1]</li> <li>• Difference in threat acceptance between military person and F&amp;Rs [PS1]</li> <li>• Individual expectations from security behaviours [PS1]</li> <li>• Potential conflict for F&amp;Rs following rules but needing an online profile for businesses [PS1]</li> <li>• Military career makes information security second nature to personnel [PS2]</li> </ul>
	Different knowledge levels for the importance of online safety	<ul style="list-style-type: none"> <li>• Lack of understanding from F&amp;Rs about the individual's reduced online presence [PS1]</li> <li>• Some threats aren't realistic or recognisable to F&amp;Rs [PS1]</li> <li>• F&amp;Rs can understand what they want of themselves but only in their own risk appetite, not considering how the forces might be different [PS1]</li> <li>• Not being in military environment can results in a lack of awareness of cyber threat to military personnel [PS2]</li> </ul>
	Desiring acceptance of others online	<ul style="list-style-type: none"> <li>• Information sharing occurs when F&amp;Rs want to share good news [PS2]</li> <li>• F&amp;Rs want endorphin rush of receiving messages from others about military person coming home [PS2]</li> <li>• Individuals with access to sensitive information might have the mindset to show off what they know [PS2]</li> <li>• Military person might choose to share classified information to increase how other people perceive them [PS2]</li> <li>• F&amp;Rs who are admirers of senior military personnel can share information to promote themselves [PS2]</li> </ul>

Risk behaviours of friends and relatives	Expectation of access to personnel information	<ul style="list-style-type: none"> <li>• Use of technical devices is not unexpected in current society [PS1]</li> <li>• F&amp;Rs want to know where service person is geographically [PS2]</li> <li>• Movement programme requires most scrutiny as is detailed but F&amp;Rs want to know where service person is [PS2]</li> </ul>
	Risk of sharing operational information	<ul style="list-style-type: none"> <li>• Sharing operational timings and dates presents risk if posted online [PS1]</li> <li>• Biggest cyber risk from F&amp;Rs is lack of awareness of sensitivities of ship movement [PS2]</li> <li>• Ship movement programme between 72 hour and 4 weeks provides most risk due to it being specific [PS2]</li> <li>• Discussions about long-term ship programmes discussed more openly because there are no specific dates [PS2]</li> <li>• 48 hour ship programme sharing less risk as people outside of the military bubble can access information [PS2]</li> <li>• Information sharing in itself may not present risk but could advertise relationship that could be exploited to access military person [PS2]</li> <li>• Main cyber concerns are the personnel, social and political aspects of sharing information in the public domain [PS2]</li> </ul>
	Reduced understanding results in accidental compromise	<ul style="list-style-type: none"> <li>• Risk of F&amp;Rs not understanding what they post online [PS1]</li> <li>• Risk of F&amp;Rs not understanding how online risk works [PS1]</li> <li>• Limited understanding from friends and relatives about what they're posting online or how information can be combined [PS1]</li> <li>• Defines F&amp;Rs risk into 3 main behaviours: usage, lack of understanding how it works and lack of understanding of the overall picture [PS1]</li> <li>• Extended family are less technically savvy so will choose to share with Facebook just in case [PS1]</li> <li>• Risk of inadvertent cyber mistakes or accidental compromise due to not understanding implications of actions [PS2]</li> <li>• Accidental compromise of information in background of BeReal picture that person doesn't see but someone else might notice [PS2]</li> </ul>

		<ul style="list-style-type: none"> <li>• Cyber risk and concern for younger personnel with newer spouses who have less exposure to military culture but still high access to information [PS2]</li> </ul>
	Word of mouth	<ul style="list-style-type: none"> <li>• Information sharing works in stages, shared first with partner, then partner shares with their parents [PS1]</li> <li>• Word of mouth is a concern on military patches and social media [PS2]</li> </ul>
	Generational differences in behaviour influence risk	<ul style="list-style-type: none"> <li>• Dad refuses to embrace technology, and being in minority is a social problem but not security issue as family assist him online when required [PS2]</li> <li>• Older generation could present risk because they are provided with technology they don't understand [PS2]</li> <li>• Younger generation understand how to use social media but maybe not implications of behaviours [PS2]</li> <li>• Concerns about what children engage with and post on social media but not with themselves or their role, as that they would before posting about them or role [PS2]</li> </ul>
Impact of friends and relatives cyber risk	Information can be targeted by an adversary	<ul style="list-style-type: none"> <li>• Risk of adversaries accumulating information that is posted online [PS1]</li> <li>• If F&amp;R shares information about a ships movement ahead of time it is sufficient for an adversary to react [PS2]</li> </ul>
	Information sharing can have political and social ramifications	<ul style="list-style-type: none"> <li>• Political ramifications can be an impact of information sharing [PS2]</li> <li>• F&amp;Rs can share opinion from service person onwards [PS2]</li> <li>• Political consequences occur when individual opinion is seen as representative of military opinion [PS2]</li> <li>• Defamatory comments about a colleague/superior can be shared onwards by F&amp;Rs [PS2]</li> <li>• Political ramifications of comments about defence spending [PS2]</li> </ul>
		<ul style="list-style-type: none"> <li>• Receive a large amount of general training [PS1]</li> <li>• Regular briefings are unit dependent [PS1]</li> </ul>

Existing cyber training and awareness approach	Military culture does not encourage cyber mindset	<ul style="list-style-type: none"> <li>• Role specific training for risk management [PS1]</li> <li>• Online training is more standardised [PS1]</li> <li>• Cyber knowledge for sailors is based on mindset of not being technical rather than naivety or lack of training [PS2]</li> <li>• Mindset to turn to a more technical person for a response in cyber [PS2]</li> <li>• Cyber training is available if sought out but a cyber understanding is not encouraged [PS2]</li> <li>• Cyber focused job role means cyber understanding more significant than average service person [PS2]</li> </ul>
	Fear of embarrassment or not knowing	<ul style="list-style-type: none"> <li>• Sailors in command fear appearing foolish or showing a lack of understanding to subordinates [PS2]</li> <li>• Mindset of sailors not wanting to lose face and be embarrassed by saying they don't know something [PS2]</li> </ul>
	Limitations of cyber training and awareness for employees	<ul style="list-style-type: none"> <li>• Targeting training is challenging due to diverse employment group [PS1]</li> <li>• Provided with locally produced pamphlets at various quality [PS1]</li> <li>• When online learning is every 3 years content is missing [PS1]</li> <li>• Cybersecurity messaging can be inconsistent and unclear [PS1]</li> <li>• Some key elements of cyber awareness can get lost in the noise [PS1]</li> <li>• Locally produced materials often produced by best available individual rather than a cyber specialist [PS1]</li> <li>• Local materials are adhoc and can range from a list of rules to more detailed explanations about safe online behaviour [PS1]</li> <li>• No information in annual security brief for military personnel about how cyber habits of F&amp;Rs can affect the service [PS2]</li> <li>• General cyber defence training is minimal [PS2]</li> </ul>
	Existing approach for F&Rs	<ul style="list-style-type: none"> <li>• Training F&amp;Rs get in their own jobs isn't as high a level, more basic [PS1]</li> <li>• F&amp;Rs rely on their own individual understanding to make a decision [PS1]</li> </ul>

Improving training and awareness for F&Rs	Accessible materials for everyone	<ul style="list-style-type: none"> <li>• Everyone needs to know cyber basics [PS1]</li> <li>• Education that everyone may not have the same understanding about online safety [PS1]</li> <li>• Cyber is a complicated field and people like it to be explained simply [PS1]</li> <li>• Sharing the why with F&amp;Rs is important, the how is the challenge [PS2]</li> </ul>
	Importance of the why, as well as the what	<ul style="list-style-type: none"> <li>• F&amp;Rs need to know what information not to share [PS2]</li> <li>• Concern over F&amp;Rs not understanding why information compromise is so important [PS2]</li> <li>• Letter to spouse, children and parents of serving personnel to highlight the specific reasons why information needs to be retained [PS2]</li> <li>• Understanding of information compromise is obvious to service person but not F&amp;Rs [PS2]</li> <li>• Hard hitting point that service person could die due to accidental information sharing by F&amp;R online [PS2]</li> </ul>
	Pride encourages engagement with materials	<ul style="list-style-type: none"> <li>• Pride would encourage parents to engage with cyber training and education materials if they were provided [PS1]</li> <li>• Those with relatives who are not British nationals would try really hard to engage with British military rules if provided with them [PS1]</li> </ul>
	Keeping up with threat landscape	<ul style="list-style-type: none"> <li>• Challenging to identify most recent and therefore most relevant training [PS1]</li> <li>• Challenge as cyber is a constantly evolving field [PS1]</li> <li>• Facebook privacy rules: Change frequently but not drastically enough to be updated about rules [PS1]</li> </ul>
	Overcoming fear and information overload	<ul style="list-style-type: none"> <li>• Majority of people experience information overload when constantly presented with new materials about the same threats [PS1]</li> <li>• Individuals need to know how to take responsibility for behaviour without being scared to do anything online [PS1]</li> </ul>



Responsibility for friends and relatives' online behaviour	Military personnel to keep their information secure	<ul style="list-style-type: none"> <li>• Educating the military person to be responsible for their information is more valuable than educating F&amp;Rs [PS1]</li> <li>• F&amp;Rs don't post a lot about military person online without discussion being had [PS1]</li> <li>• Controls information spread by contacting certain individuals less frequently [PS1]</li> <li>• Responsibility for physical cyber risks from F&amp;Rs sharing devices or networks falls to service person [PS2]</li> <li>• Existing examples of physical cybersecurity breaches related to service person rather than F&amp;Rs [PS2]</li> <li>• Responsibility of service person to know rules to avoid opportunity for compromise through physical cyber risk [PS2]</li> </ul>
	Military personnel to communicate requirements to friends and relatives	<ul style="list-style-type: none"> <li>• Comfortable to politely discuss in-laws' online behaviour [PS1]</li> <li>• Military personnel should have a healthy discussion with F&amp;Rs about what they find acceptable to be posted online [PS1]</li> <li>• Close relations would expect them to discuss cyber risk [PS1]</li> <li>• Responsibility of service member to inform F&amp;Rs when questions about role are too detailed to respond [PS2]</li> <li>• Sailors taught from onset of career to inform family members that ship programming is sensitive [PS2]</li> <li>• Onus of military person to translate information about cyber awareness to F&amp;Rs [PS2]</li> </ul>
	Barriers to communication between F&Rs and military personnel	<ul style="list-style-type: none"> <li>• Wouldn't want to upset in-laws by asking them to remove something online [PS1]</li> <li>• Challenge of language barrier between family members [PS1]</li> <li>• Potential that setting boundaries for online behaviour might cause tension in fragile relationships [PS1]</li> <li>• Differences in expectations of behaviour can cause tension [PS1]</li> <li>• Potential lack of awareness of what children had posted on social media so if content presents cyber risk [PS2]</li> </ul>

## Appendix I: Theme table for themes from Thematic Analysis of the Phase 2 main study

<b>Theme</b>	<b>Sub-Theme</b>	<b>Codes</b>
Definition of Key Relations is diverse	Key Relations are immediate family	<ul style="list-style-type: none"> <li>• Wife, young son and parents are considered close relations [P1]</li> <li>• Considers immediate family as Key Relations [P3]</li> <li>• Key Relations as wife, kids, parents [P3]</li> <li>• Mum, dad and brother considered close relations [P6]</li> <li>• Close relations are just family not any friends [P6]</li> <li>• Close relations are wife and parents [P7]</li> <li>• Wife and children considered close relations [P8]</li> <li>• Dad lives overseas but has regular contact [P8]</li> <li>• Speaks to siblings, parents and spouse frequently [P9]</li> <li>• Wife is closest relation [P11]</li> <li>• Considers mum and brother as close family relations [P11]</li> <li>• Immediate close relations are wife and children [P12]</li> <li>• Considers close relations as immediate family [P13]</li> <li>• Immediate family including mum, dad and brother are close relations [P14]</li> <li>• Girlfriend is a close relation [P14]</li> <li>• Immediate family, friends and work colleagues are close relations [P15]</li> <li>• Key Relations are close family and friends [P17]</li> <li>• Unavoidable sharing information about role with spouse [P17]</li> <li>• Close relations are immediate family and not as extensive as cousins [P17]</li> </ul>
	Extended family are Key Relations	<ul style="list-style-type: none"> <li>• Wife's parents and siblings considered Key Relations [P3]</li> <li>• Cyber risk can come from extended family as well as direct family [P6]</li> <li>• Grandparents and Auntie considered close relations [P6]</li> <li>• Close relations are just family not any friends [P6]</li> <li>• Some of wife's family considered close relations [P8]</li> <li>• Brother's family and wife's family are all considered close relations [P11]</li> <li>• Immediate close relations are in-laws who they see regularly [P12]</li> <li>• Close family relations are parents, siblings, kids, nephews &amp; nieces, and grandparents [P13]</li> <li>• Close relations are mix of family and friends [P14]</li> <li>• Close aunt and uncle considered close relations [P14]</li> </ul>

	Friends are Key Relations	<ul style="list-style-type: none"> <li>• A couple of friends considered Key Relations [P3]</li> <li>• Mix of long term and newer friends, but all local [P3]</li> <li>• Acquaintances through hobbies and sports [P3]</li> <li>• Close relations are closer friends outside the army [P7]</li> <li>• Neighbours are close friends and considered close relations [P8]</li> <li>• Key Relations are a mix between friends and family [P9]</li> <li>• Speaks to friends and work colleagues frequently [P9]</li> <li>• Limited integration of non-work friends with work life due to distance [P9]</li> <li>• Close friends consist of colleagues, friends from prior to joining military and their partners [P11]</li> <li>• A network of friends that ripples out in terms of closeness [P12]</li> <li>• Considers close relations as immediate friend circle [P13]</li> <li>• Military personnel has two parts of their life with a friendship group for each [P13]</li> <li>• Close circle of friends are from school [P13]</li> <li>• Close relations are mix of family and friends [P14]</li> <li>• Best friend is a close relation [P14]</li> <li>• Immediate family, friends and work colleagues are close relations [P15]</li> <li>• Key Relations are close family and friends [P17]</li> </ul>
	Key Relations are situation dependent	<ul style="list-style-type: none"> <li>• Close relations are F&amp;Rs they routinely speak to [P7]</li> <li>• Friends inside the army considered colleagues first as clearances makes conversations easier [P7]</li> <li>• Close relations can be dependent on environment and situation [P8]</li> <li>• Children live with their mum so ex-spouse considered within Key Relations [P8]</li> <li>• Relies on colleagues at work and considered close relations but not at home [P8]</li> <li>• Definition of loved ones/dependents is open for interpretation [P13]</li> <li>• Anyone with access to social media page could be considered as close [P13]</li> <li>• Defining close relations is challenging due to globalisations of contacts [P15]</li> <li>• Individual perceptions of relationships influences terminology [P15]</li> </ul>
	Term dependents is out-dated	<ul style="list-style-type: none"> <li>• Complaints about dependent terminology not reflecting individuals' lives outside of being a military relative [P15]</li> <li>• Term dependent is derogatory as F&amp;Rs don't depend on military personnel [P15]</li> <li>• Societal movement towards dual-working families and the perception of women's roles in the workplace influences terminology [P15]</li> <li>• Military currently mainly views dependents included on JPA as of interest for them [P16]</li> </ul>

<p>Friends and relatives' online behaviours present risk to military cyber resilience</p>	<p><i>Oversharing of military information online</i></p>	<ul style="list-style-type: none"> <li>• Wife sharing relocation information narrows down where military person is based [P1]</li> <li>• Triangulation of online friends/connections all from same location [P1]</li> <li>• Information shared by close relations might be up to OS from context but no higher [P1]</li> <li>• Easy to work out if son moves school every couple of year then he's probably military [P1]</li> <li>• Pattern of life is a target for an adversary [P3]</li> <li>• Triangulation of operational movement shared by parents and other F&amp;Rs [P5]</li> <li>• Adversaries might need final puzzle piece accessed through F&amp;Rs [P5]</li> <li>• F&amp;Rs sharing location and ship information on social media presents security risk [P6]</li> <li>• Upon joining military parents and brother posted about it online [P6]</li> <li>• F&amp;Rs posting about passing out provides overview of new military intakes [P6]</li> <li>• Information shared online can be triangulated to present higher risk [P7]</li> <li>• Experience of mum sharing information onwards about location and timings of exercise [P7]</li> <li>• Parents sharing a tagged picture or post of personnel can present risk from adversary [P9]</li> <li>• Has friends whose parents post online about where their child is about to deploy [P12]</li> <li>• Children oversharing online makes them more vulnerable than necessary [P12]</li> <li>• Sharing flight times with F&amp;Rs to make plans can become risky if they overshare [P13]</li> <li>• F&amp;Rs posting military person's movements and base location is detrimental [P14]</li> <li>• Risk of geo-location tags pinned to a photo [P14]</li> <li>• Information about military F&amp;Rs can be found on donation pages [P14]</li> <li>• Information sharing is a risk regardless of the vector being a serving person or F&amp;R [P15]</li> <li>• Risk of people sharing too much information unnecessarily [P15]</li> <li>• Large cyber risk of aggregation of online information [P15]</li> <li>• Risk vectors for military organisations are data aggregation and individual targeting and blackmail [P15]</li> <li>• Different individuals commenting minute information can be harvested by adversaries [P15]</li> <li>• Sharing security classifications increases likelihood of individual targeting [P15]</li> <li>• Threat actors relying on opportunity that information is posted by F&amp;Rs [P17]</li> <li>• Open-source examples of individuals sharing military information in online forums to win arguments [P17]</li> <li>• Piece together military person returning home if a spouse has multiple beauty appointments [P17]</li> <li>• Huge amount of information can be aggregated about operations from F&amp;Rs social media posts [P17]</li> <li>• Risk of amalgamation of different information that multiple people posted innocently [P17]</li> </ul>
---	--	--

	<i>Increased risk of public social media profiles</i>	<ul style="list-style-type: none"> <li>• Risk of F&amp;Rs sharing classified information on an open or public social media account [P5]</li> <li>• Son experienced trolling due to not monitoring security settings and having an open profile [P8]</li> <li>• Showing off life on open social media profile can be detrimental to own and family's safety [P14]</li> <li>• Fitness tracking apps with open profiles can indicate perimeter of military bases to anyone [P14]</li> <li>• Risk of open Facebook groups for military spouses and partners [P14]</li> <li>• Open social media profiles vital role in risk of F&amp;Rs to military organisations [P14]</li> <li>• Risk of being able to connect military person and their F&amp;Rs in the online domain [P15]</li> <li>• Example of John Sawers previous MI6 chief wife's open Facebook profile and sharing details of life [P16]</li> <li>• Open social media platforms present risk [P16]</li> </ul>
	<i>Risks specific to social media platforms</i>	<ul style="list-style-type: none"> <li>• Facebook is a cyber risk [P1]</li> <li>• Parents on school WhatsApp group spread information quickly [P1]</li> <li>• Videos shared on WhatsApp are lost and can quickly go off ship [P5]</li> <li>• Friends parents tag them in Instagram and Facebook posts about deployment [P6]</li> <li>• Risk of friends sharing information on Reddit forum or Instagram comment on post [P7]</li> <li>• Afghanistan example where threat actors would use social media to pinpoint soldiers and target F&amp;Rs to reach serving personnel [P8]</li> <li>• Adversary could find service person through friend list on parents social media profile [P9]</li> <li>• Facebook, Instagram, and Twitter are similar so similar risk [P13]</li> <li>• Frequency oversharing on LinkedIn due to advertising to future employers [P13]</li> <li>• Balance of oversharing on LinkedIn whilst selling themselves to employers [P13]</li> <li>• Current role and security clearance shouldn't be on LinkedIn [P13]</li> <li>• BeReal and Snapchat 2 of the most risky social media platforms [P14]</li> <li>• F&amp;Rs posting snapchats of military person returning home with bag and uniform in background [P14]</li> <li>• Military personnel may lock down social media profiles but risk of being tagged by wider online network [P14]</li> <li>• Heavy Strava use as a western app indicates military activity in non-western countries [P16]</li> <li>• Online risk to military is from behaviour on social media rather than direct cyber-attack [P17]</li> </ul>
	Behaviours considered less risky online	<ul style="list-style-type: none"> <li>• Wife's Facebook page is bland so not considered security threat [P1]</li> <li>• Parents aren't on Facebook [P1]</li> <li>• Not worried about parents' risk due to lack of online presence [P1]</li> <li>• Physical risk at home less risky unless extreme nefarious activity occurring [P3]</li> <li>• Network security perceived higher as house is physically isolated with little passing traffic [P9]</li> <li>• Work conversations spoken about less over open networks as socialising rather than working [P9]</li> <li>• Father-in-law not getting involved with new tech reduces threat avenue of new technology [P9]</li> </ul>

		<ul style="list-style-type: none"> <li>• People tend to understand that twitter is a public forum so less information shared [P17]</li> </ul>
	<i>Non-military related cyber risk behaviours</i>	<ul style="list-style-type: none"> <li>• Worried about parents being victim of a scam and losing their money [P1]</li> <li>• Concern over parent falling victim to phishing emails and scams if they're not savvy [P3]</li> <li>• In-laws are susceptible to scams on social media due to naïveté of believing advert deals [P8]</li> <li>• Reminding in-laws that if something is too good to believe online then it probably is a scam [P8]</li> <li>• Parents in law don't understand online banking is very secure and would rather bank in person [P8]</li> <li>• Risk of shared devices with financial information already set up [P13]</li> </ul>
Suggested reasons individuals engage in insecure online behaviours	<i>Expectation of social media</i>	<ul style="list-style-type: none"> <li>• Has Facebook and LinkedIn accounts as a placeholder [P1]</li> <li>• LinkedIn account required if leaving role in military [P1]</li> <li>• Challenging to tell deployed personal not to take their personal devices as access is expected [P3]</li> <li>• Pervasiveness of technology makes it difficult to control where and how devices are used [P3]</li> <li>• Challenges of not being on social media can occur for non-work reasons such as information about children's activities [P3]</li> <li>• Online risk becomes bigger with each generation that becomes more involved with technology [P6]</li> <li>• Existing account on most social media platforms but not used [P8]</li> <li>• TikTok used when bored to look at funny videos [P8]</li> <li>• LinkedIn account for potential transition into civilian role [P8]</li> <li>• People can become addicted to social media with large screen times [P8]</li> <li>• Evolutions of the pervasiveness of technology since joining the Army [P8]</li> <li>• Signal, WhatsApp, and messenger used within military [P8]</li> <li>• Expectation to share information on social media otherwise it's not real [P13]</li> <li>• Natural part of current society to share everything online [P13]</li> <li>• Risk of shared devices increases as society becomes more dependent on technology [P14]</li> <li>• Society is becoming increasingly dependent on social media [P14]</li> <li>• Everyone being aware of online risks is important when living in a digital age [P16]</li> <li>• Requirement of mobile phones for most operations [P17]</li> </ul>
	<i>Desire for acceptance from others</i>	<ul style="list-style-type: none"> <li>• Desire for societal acceptance is a risk to cyber resilience [P8]</li> <li>• People post online to gain acceptance from others and make gains in life [P8]</li> <li>• Sharing of information online to climb social hierarchy [P9]</li> <li>• Idea of seeking self-gratification from social media [P14]</li> <li>• Society standard of popularity contest of likes, views and followers online [P14]</li> <li>• Information sharing and obsession over like/follower/view counts increasing with increase of careers in social media [P14]</li> </ul>

	<p><i>Lack of understanding about technology and risk</i></p>	<ul style="list-style-type: none"> <li>• Parents incorrectly name WhatsApp [P1]</li> <li>• Parents make lots of mistakes when using technology [P1]</li> <li>• Parents don't know what Instagram or TikTok are [P1]</li> <li>• Misconception end-to-end encryption makes WhatsApp more secure [P1]</li> <li>• Family lacks understanding of what they can post about military person on social media [P6]</li> <li>• Own family lacks understanding that information shared online is open to everyone [P7]</li> <li>• Lack of understanding that internet is amazing tool but also very dangerous [P14]</li> <li>• F&amp;Rs not being aware of risk of accepting friend requests from unknown people [P17]</li> </ul>
	<p><i>Lack of consideration of app permissions</i></p>	<ul style="list-style-type: none"> <li>• When an app asks for location permissions people automatically select allow [P6]</li> <li>• Experience of colleague not realising location settings on BeReal were automatically posting ship deployment locations in posts [P6]</li> <li>• Automatic locations on social media posts can provide information about base and personnel locations [P6]</li> <li>• Lack of awareness about location permissions is a big gap in security [P6]</li> <li>• Risk of automatically posting a photo online without switching off geo-tag [P6]</li> <li>• Easy to not realise risk of social media settings until a common societal discussion point [P8]</li> <li>• Perception the media hypes up security settings [P8]</li> <li>• Those with a connection to the military should be ruthless about security settings on a new app [P8]</li> <li>• Risk of geo-location tags pinned to a photo [P14]</li> <li>• Risk of sharing information on Facebook within trusted network with incorrect privacy settings [P17]</li> </ul>
	<p><i>Accidental compromise</i></p>	<ul style="list-style-type: none"> <li>• Wife knowing work pattern increases chance of incidentally sharing classified information [P1]</li> <li>• F&amp;Rs can inadvertently share information they can't take back [P6]</li> <li>• Gaps in vulnerabilities as people don't realise what they're posting presents risk [P6]</li> <li>• Friends share information onwards to win argument or interest without understanding impact [P7]</li> <li>• Potential that a friend might post something sensitive inadvertently [P12]</li> <li>• F&amp;Rs are influential audience that if missed can inadvertently leak important information [P12]</li> <li>• F&amp;Rs oversharing information is not malicious or purposeful [P13]</li> <li>• Incidental background information shared on BeReal due to intended purpose of app [P14]</li> <li>• F&amp;Rs living on base film tiktok trends without realising background environment [P14]</li> <li>• Posting pictures of military children at events may include information about other military personnel and their children [P14]</li> <li>• Risk of inadvertent information sharing groups on military forums and Facebook groups [P17]</li> </ul>

	<i>Overconfidence and complacency</i>	<ul style="list-style-type: none"> <li>• Potential arrogance of themselves and spouse thinking they know about vulnerabilities [P3]</li> <li>• Security through obscurity [P3]</li> <li>• Complacency due to amount of information online [P3]</li> <li>• Complacency with cyber hygiene and information sharing behaviours [P3]</li> <li>• F&amp;Rs don't think anyone is paying attention to their online information [P6]</li> <li>• Cyber medium provides confidence that people wouldn't experience in person [P8]</li> <li>• Perception that some online risk is okay as a one-off without realising significance of aggregation of one-offs [P12]</li> <li>• Overconfidence of snapchat only being viewed for limited time though can be screenshot [P14]</li> <li>• Once snapchat images are out there images can easily be viewed multiple times [P14]</li> <li>• Cyber risk from human laziness and complacency [P16]</li> <li>• Risk of confidence of sharing information on Facebook within trusted network with incorrect privacy settings [P17]</li> </ul>
	<i>Pride influences online behaviour</i>	<ul style="list-style-type: none"> <li>• Parents want to share information about military person when proud of them [P5]</li> <li>• Parents pride of children results in them posting online about them being in military [P9]</li> <li>• Mum doesn't actively post but proud so will talk about children if asked [P9]</li> <li>• F&amp;Rs post on social media when they're proud [P6]</li> <li>• Natural for F&amp;Rs to proud of military person [P6]</li> <li>• Families are proud of what their relatives do [P7]</li> </ul>
	<i>Increased cyber risk overseas</i>	<ul style="list-style-type: none"> <li>• Military targeted since the IRA and as a result of being in the middle east [P1]</li> <li>• Military person wants to share information with parents about experiences when working [P6]</li> <li>• Higher risk of information sharing when families visit military person on deployment [P6]</li> <li>• Frequent information sharing when military person is deployed as information is interesting [P6]</li> <li>• Before deployment parents post deployment location and leaving date [P7]</li> <li>• F&amp;Rs posting online about deployment indicates exact time and location of many military personnel [P7]</li> <li>• Potential difference of behaviours when military person is deployed or in UK based [P13]</li> <li>• When stationed overseas people want to update their friends and relatives about life [P14]</li> <li>• Online risk is exacerbated overseas [P15]</li> <li>• Increased risk from F&amp;Rs relocated overseas with military personnel [P16]</li> <li>• Deployment and relocation risk for personnel and F&amp;Rs is mobile devices [P16]</li> <li>• Deployment locations of interest to adversaries have cyber threat to F&amp;Rs and personnel [P16]</li> <li>• Welfare wi-fi on ships creates distraction personnel are still engaged in day-to-day family life [P17]</li> <li>• Challenging balance of staying connected to F&amp;Rs without them becoming a distraction to operations [P17]</li> <li>• Balancing risk of cybersecurity and physical security of using personal devices when ashore overseas [P17]</li> </ul>



	<p><i>Barriers to engaging in secure behaviours</i></p>	<ul style="list-style-type: none"> <li>• Colleagues secure until out drinking and then join open networks on pub crawl [P9]</li> <li>• Challenge for F&amp;Rs engaging with secure online behaviours due to busy lives [P13]</li> <li>• Non tech savvy F&amp;Rs may be unaware of children’s online behaviour [P13]</li> <li>• F&amp;Rs may have negative attitudes towards recommended safe ways to communicate with military person if they cannot communicate effectively [P12]</li> <li>• F&amp;Rs may revert back to insecure online behaviours if recommended methods don't work [P12]</li> <li>• Difficult to learn the process of security settings for some online platforms [P8]</li> <li>• Social media platforms want exposure so aren’t forthcoming with details about security settings [P8]</li> <li>• Different perception of risk sharing between individuals [P8]</li> <li>• F&amp;Rs not subject to service law so no repercussions for not engaging in secure online behaviours [P15]</li> <li>• Relying on military personnel to communicate information from educational briefs to F&amp;Rs [P16]</li> <li>• Difficult to protect data when mobile phone networks designed to work efficiently not protect anonymity [P17]</li> <li>• Need to understand the driving factor behind why F&amp;Rs feel the need to share information online to address risk behaviours [P17]</li> </ul>
<p>Individual differences</p>	<p>Risk behaviours from younger generation</p>	<ul style="list-style-type: none"> <li>• Children’s threat surface is wide due to plethora of technology [P3]</li> <li>• Difference in social behaviours between generations with children constantly connected online [P3]</li> <li>• Concern of educating children when threat experiences are different from own experiences [P3]</li> <li>• Pervasiveness of technology for children makes it difficult to switch off [P3]</li> <li>• Brother would post social media stories about visiting sibling on base [P6]</li> <li>• Younger generations blasé about app security settings and permissions [P6]</li> <li>• Much younger generations don't consider risk when using devices [P6]</li> <li>• Brother uses Instagram and snapchat [P6]</li> <li>• Parents of younger military personnel want to know location and activity [P6]</li> <li>• Younger generations attached to certain social media platforms [P6]</li> <li>• Snapchat is considered an app for teenagers [P8]</li> <li>• Teenagers are easily influenced to share discussion between family [P8]</li> <li>• Younger generation accept requests from anyone to achieve a higher follower account [P8]</li> <li>• Concern about Nephew’s gaming behaviour and online presence with everything being online [P11]</li> <li>• YouTube and Tiktok are main platforms used by children [P12]</li> <li>• Teenagers sharing online parents are going away for a certain amount of time [P13]</li> <li>• Younger generations spend a higher amount of time online across a multitude of platforms [P13]</li> <li>• Younger generation can become focussed on follower and like count [P14]</li> <li>• Younger generation use a plethora of social media platforms and voice their opinions [P16]</li> <li>• Risk of younger generations not understanding that information shared is permanently online [P16]</li> <li>• Younger generation pose risk of inadvertent sharing of information in background of picture [P16]</li> <li>• Challenge with younger generation posting online for instant access and gratification [P16]</li> </ul>

		<ul style="list-style-type: none"> <li>• When child is a teenager they'll have to consider the risks of their online behaviour [P17]</li> </ul>
	Risk behaviours from older generation	<ul style="list-style-type: none"> <li>• Parents behaviours online make them wince [P3]</li> <li>• Concern parents are agreeable when discussing online safety to get conversation over with [P3]</li> <li>• Parents, grandparents and auntie all use Facebook [P6]</li> <li>• Parents have Instagram accounts but they don't post [P6]</li> <li>• Parents would take pictures and post online later rather than a story post [P6]</li> <li>• Mum posts on Facebook as friends are on there so reaches a larger audience [P6]</li> <li>• Small generational gap in social media platforms used [P6]</li> <li>• Parents could censor grandparents but not brother due to using different platforms [P6]</li> <li>• Difficult to explain importance of secure online behaviours to boomer generation [P7]</li> <li>• Older generation easily influences when discovering new platforms and technology [P8]</li> <li>• Hard to explain security behaviours to older generation due to stubbornness [P8]</li> <li>• Frustrating to educate older generation unless previous job experience required them to be tech savvy [P8]</li> <li>• Mother in law requires in-person explanation rather than over the phone [P8]</li> <li>• Balance of respecting older generations knowledge and experience whilst helping them understand evolution of technology [P8]</li> <li>• Parents are of older generation and less tech savvy [P9]</li> <li>• Father in law technically minded but technology has accelerated away from him [P9]</li> <li>• Father in law is well connected with gadgets but can't get head around new stuff [P9]</li> <li>• Father in law can manage existing technology safely but would struggle if existing technology became obsolete [P9]</li> <li>• Parents mainly use Facebook [P9]</li> <li>• Mum has an Instagram account but doesn't post on it [P9]</li> <li>• Das is sceptical of technology's lifetime and stability [P9]</li> <li>• Age differences result in difference in online presence [P11]</li> <li>• Mum online for longer amount of time but engages less than the younger generation [P11]</li> <li>• Opinion that Facebook is for old people [P12]</li> <li>• Parents have less cybersecurity awareness but spend less time online [P13]</li> <li>• 40-60 year olds use Facebook to message friends and for reunion pages [P13]</li> <li>• Over 50s without a large amount of technological experience present more risk [P16]</li> <li>• Older generations present risk from lack of knowledge about using social media safely [P17]</li> <li>• Some individuals in older generation might only learn to communicate on new social media platforms when military person deployed [P17]</li> </ul>
	Generational behaviour differences reducing online risk	<ul style="list-style-type: none"> <li>• Secure behaviours can be taught to younger generation if they're made aware of risk [P6]</li> <li>• Parents know how to use social media platforms even though not frequently used [P6]</li> <li>• Grandparents would share information about military person in person [P6]</li> <li>• Grandparents are secure online due to lack of trust of technology [P6]</li> <li>• In-laws rarely post on Facebook and never about military family members' job information [P12]</li> </ul>

		<ul style="list-style-type: none"> <li>• Sibling has good security awareness due to growing up with technology [P13]</li> </ul>
	Personality differences	<ul style="list-style-type: none"> <li>• Dad is more risk averse compared to mum [P9]</li> <li>• Wife always been more risk averse and tech savvy [P9]</li> <li>• Dad's work life developed a hands on personality so technology frustrates him [P9]</li> <li>• Dad's lifestyle of living remotely puts technology security back of his mind [P9]</li> <li>• Character traits including gambling, adverse sexual behaviours, links to extremism and protest groups can be exploited [P15]</li> </ul>
	Differences in military job roles	<ul style="list-style-type: none"> <li>• Believes Navy personnel to be more secure due to requirement and communicate requirement to F&amp;Rs [P3]</li> <li>• Uptake of behaviours by dependents of personnel on units with extreme risk different to average service person [P5]</li> <li>• Friend with a parent in high risk military role is aware of requirements when posting about parent online [P6]</li> <li>• Level of online threat is not uniform to all F&amp;Rs [P17]</li> <li>• F&amp;Rs of higher command personnel are a more attractive target than F&amp;Rs or personnel lower in command [P17]</li> </ul>
	No existing training or education for F&Rs	<ul style="list-style-type: none"> <li>• Not actively aware of existing training for friends and relatives [P3]</li> <li>• Training might exist on family facing portals [P3]</li> <li>• Not aware of any existing training for friends and relatives [P9]</li> <li>• Reduced priority for cyber awareness for F&amp;RS due to lack of people available to devote time to the issue [P5]</li> <li>• Never actively signposted relatives to any cybersecurity materials [P13]</li> <li>• Not aware of existing cyber training and awareness for F&amp;Rs [P7]</li> <li>• F&amp;Rs cybersecurity is important but is a lesser degree of importance so not addressed [P15]</li> <li>• F&amp;Rs potentially indirectly pick up cyber messaging on military sites [P16]</li> <li>• Not aware of any existing cyber initiatives for F&amp;Rs [P17]</li> </ul>
	Existing training for F&RS	<ul style="list-style-type: none"> <li>• Previous contract with GSO provided visuals for monthly campaigns, posters, leaflets and webinars [P11]</li> <li>• Resource limit mean monthly campaigns are general military rather than branch specific [P11]</li> <li>• Current situation of posting materials on MODNET relies on service person delivering message to F&amp;Rs [P11]</li> <li>• Only direct outreach to F&amp;Rs is face to face events e.g. airshows and family days [P11]</li> <li>• QR code survey distributed at in person events to identify F&amp;Rs knowledge level and gaps to direct future initiatives [P11]</li> <li>• Current messaging focuses on general awareness of safety behaviours e.g. locked down accounts and secure passwords [P11]</li> </ul>

		<ul style="list-style-type: none"> <li>• Aim of Get Safe Online materials was to go through HIVEs so F&amp;Rs could access [P12]</li> <li>• Tailored cybersecurity briefs exist for various audiences including F&amp;Rs [P15]</li> <li>• Cybersecurity briefs are tailored to the risk behaviours and character traits of various audiences [P15]</li> <li>• Civilian cybersecurity briefs are toned down due to classifications and discouraging fear of threats [P15]</li> <li>• Cyber confident messaging is beneficial through consistent yet novel messages [P15]</li> </ul>
	Barriers to existing training	<ul style="list-style-type: none"> <li>• Budget cuts limit access to external companies like Get Safe Online to aid with materials for F&amp;Rs [P12]</li> <li>• F&amp;Rs aspect often forgotten as focus is on the service people [P12]</li> <li>• Difficult in reaching extended MOD community without a MODNET device [P14]</li> <li>• Requirement for military personnel to update all dependents and next of kin on JPA which is not a priority for them [P16]</li> <li>• Relying on military personnel to communicate information from educational briefs to F&amp;Rs [P16]</li> <li>• F&amp;Rs training and education is third-hand from personnel rather than first-hand [P17]</li> <li>• Cyber education for personnel includes examples of F&amp;Rs online risk behaviours for them to share with F&amp;Rs [P17]</li> </ul>
	Non-military training for Key Relations	<ul style="list-style-type: none"> <li>• Wife's previous role In defence provided some cyber training [P1]</li> <li>• Parents learnt about online scams through talking to friends, watching the news and reading the paper [P3]</li> <li>• Wife's role within technology increases her interest in cybersecurity [P9]</li> <li>• Wife has good level of cybersecurity knowledge due to role in tech industry [P9]</li> <li>• Generational difference of cyber education in schools higher level than at home [P13]</li> <li>• F&amp;Rs in technical role potentially receive better training than military [P13]</li> <li>• Education for children potentially more in-depth [P13]</li> <li>• Children receive cyber awareness from variety of avenues including home, school and cadets [P12]</li> </ul>
	External content accessible	<ul style="list-style-type: none"> <li>• Would google how to adjust settings on social media platforms [P8]</li> <li>• NCSC resources great for families with posters and printable materials [P12]</li> <li>• Would signpost F&amp;Rs to NCSC [P12]</li> <li>• NCSC materials are accessible to a range of knowledge levels [P13]</li> <li>• NCSC materials first point of call to signpost F&amp;Rs [P13]</li> <li>• Get Safe Online materials useful for dependents [P13]</li> <li>• Get Safe online materials colourful and use cartoons [P13]</li> <li>• Can easily adjust Get Safe Online materials to make them relatable to military population [P13]</li> <li>• NCSC and Get Safe Online provide good cyber content for F&amp;Rs [P14]</li> <li>• MOD Cyber Confident produce easy, digestible and eye catching content [P14]</li> </ul>
	Physical mitigations in place	<ul style="list-style-type: none"> <li>• Childrens' iPad and gaming devices lock down to reduce access similar to whitelist [P3]</li> <li>• MOD devices set up with VPN to protect device on home network [P3]</li> </ul>

		<ul style="list-style-type: none"> <li>• Actively attempt to disconnect children from technology to encourage cybersecurity but also to avoid mental health concerns [P3]</li> <li>• Limited risk for sharing devices or networks with F&amp;Rs as work is done on military issued devices [P7]</li> <li>• Devices are set up with VPN for protection when working remotely [P7]</li> <li>• Remote working low risk as long as cybersecurity policy is followed [P7]</li> <li>• Goes round to help in-laws with technology due to difficulty in explaining security [P9]</li> <li>• Widely known work devices should only be used for work [P14]</li> <li>• VPNs mandated on personnel devices [P16]</li> </ul>
<p>Training recommendations</p>	<p>Training content recommendations</p>	<ul style="list-style-type: none"> <li>• Training should teach people to be considerate of what they're posting online [P1]</li> <li>• Costa coffee cup example realistic of cyber risk [P1]</li> <li>• Hard hitting example of sitting in a room and someone at the back finding the details online of people in the room [P1]</li> <li>• Children should be taught information posted online can go wider than who originally posted to [P1]</li> <li>• Importance of educating children on cause an effect of posting information online that cannot be removed [P3]</li> <li>• 60 second cyber message videos on social media [P5]</li> <li>• Scenario based videos would be beneficial for educating F&amp;Rs [P5]</li> <li>• Importance of why F&amp;Rs shouldn't publish military person's activity and location [P11]</li> <li>• Impact statement explaining why F&amp;Rs should engage in behaviour, not just what the behaviour is [P11]</li> <li>• Can't stop progress of technology but children should be educated early to understand safe online behaviours [P11]</li> <li>• Basic threats and vulnerabilities for personal devices are valuable for F&amp;Rs to know [P13]</li> <li>• Basic security behaviours including secure application download and recognising phishing emails [P13]</li> <li>• Identifying differences in threats during deployment periods [P13]</li> <li>• Something is better than nothing [P13]</li> <li>• Relatability of training most important aspect [P13]</li> <li>• F&amp;Rs should be informed how to turn location settings off, information sharing advice and photo tagging requirements [P6]</li> <li>• F&amp;Rs require education on what they are and aren't allowed to post online [P6]</li> <li>• Importance of F&amp;Rs understanding the significance of engaging in secure online behaviours for military person [P7]</li> </ul>

		<ul style="list-style-type: none"> <li>• If F&amp;Rs post about military person's deployment online it should be vague rather than specific dates and locations [P7]</li> <li>• Providing guidance for families about deployment requirements [P7]</li> <li>• Materials should be broad and generic to encouraging accessibility [P7]</li> <li>• Encouragement to be aware of potential threat actors viewing online information and aggregating a picture [P12]</li> <li>• <b>Messaging to F&amp;Rs about understanding online risk behaviours and quick mitigations [P12]</b></li> <li>• Discourage WhatsApp usage due to over-reliance on end-to-end encryption, no password protection on app and vulnerabilities of image and link sharing [P12]</li> <li>• Signal recommended platform due to biometric access and ephemeral messaging to restrict access to classified information on lost or stolen devices [P12]</li> <li>• Could conduct a brief with F&amp;Rs where OSINT search conducted and information presented [P14]</li> <li>• Shock tactic can make people realise the relevance of existing dangers of posting online [P14]</li> <li>• Cybersecurity training, education and awareness materials should be fun and engaging as topic can be dull [P14]</li> <li>• <b>Cybersecurity videos and animations move people away from tick-box training [P14]</b></li> <li>• Cyber content should peak interest and be easily digestible [P14]</li> <li>• Threats should be shocking to encourage relevance but not scare people or instil fear [P14]</li> <li>• Cybersecurity materials are more palatable and easier to understand when the technical jargon is removed [P15]</li> <li>• Encouraging people to question whether they need to post certain information online [P15]</li> <li>• <b>Encouraging people to reduce online footprint, connections and information [P15]</b></li> <li>• Creation of cybersecurity materials can become iterative process based on concerns raised by F&amp;Rs [P15]</li> <li>• <b>Cyber experts should create materials that communicate technical understanding in accessible language [P16]</b></li> <li>• Key takeaway for F&amp;Rs is being mindful of what they post and ensuring profiles are locked down [P16]</li> <li>• Importance in educating why SIM cards and devices present risk overseas to personnel and F&amp;Rs [P17]</li> <li>• Importance of the risk of Facebook posting and snapchat location sharing should be highlighted within cybersecurity training [P17]</li> <li>• Challenge of cyber initiatives containing the right level of information for all age ranges and experiences [P17]</li> <li>• Cyber materials published online balance interesting to encourage engagement from F&amp;Rs without providing sensitive information to adversaries [P17]</li> </ul>
	<p>Importance of keeping up to date</p>	<ul style="list-style-type: none"> <li>• Important to keep updated on how personnel are behaving online and platforms used [P11]</li> <li>• Tinder as a way of monitoring if personnel are using their phones in an unsafe location for device usage [P11]</li> <li>• Balance of keeping up with newer technologies and new threats of existing platforms [P11]</li> <li>• Manageable to keep up with online trends if finger is on the pulse [P11]</li> <li>• Newer threats emerge as technology develops [P14]</li> </ul>

		<ul style="list-style-type: none"> <li>• Established provisions for personnel to feed back to Key Relations but emerging threats present risk [P15]</li> <li>• Cyber threat landscape is constantly changing but threats for military F&amp;Rs are the same just more pervasive as 10 years ago [P17]</li> <li>• Military organisations should be consistently analysing open source information about threats from online platforms [P17]</li> </ul>
		<ul style="list-style-type: none"> <li>• Standard guide for F&amp;Rs would be useful in reducing ambiguity or differences in what personnel communicate to F&amp;Rs [P7]</li> <li>• Would be beneficial for F&amp;Rs to receive same information about cyber vulnerabilities as station commanders [P12]</li> <li>• F&amp;Rs should be provided with an overview of online threats in deployment countries to understand why to engage in certain online behaviours [P12]</li> </ul>
	Training delivery recommendations	<ul style="list-style-type: none"> <li>• Use of SAFFA and other family associations to share information online and in leaflets [P5]</li> <li>• Use of Home Port Magazine to regularly share cyber information in an appealing way to a range of people [P5]</li> <li>• Easy to contact spouses and children directly as information is available from JPA [P5]</li> <li>• Creating videos and examples for cyber awareness is cheaper compared to implementing physical systems on ships [P5]</li> <li>• Sharing of a letter or leaflet to married quarter households [P5]</li> <li>• Sharing a letter/leaflet when ships deploy to pass along to families [P5]</li> <li>• Incorporating cyber survey in existing surveys with F&amp;Rs to identify behaviours and direct resources [P5]</li> <li>• Social media best way to disseminate materials as everyone spends so much time on there [P5]</li> <li>• Security risk having information in a letter that anyone could read [P6]</li> <li>• Good to have breadth of distribution formats of training, awareness &amp; education materials [P11]</li> <li>• Beneficial to provide F&amp;Rs with leaflets after in-person events to read information slowly [P11]</li> <li>• Benefit of having an outwardly facing website so F&amp;Rs can access materials by themselves [P11]</li> <li>• Potential to receive cybersecurity briefing upon joining military to disseminate to F&amp;Rs [P13]</li> <li>• Delivering materials to parents, siblings and children would be simplest way [P13]</li> <li>• Should cater for different family situations [P13]</li> <li>• Beneficial to have short cybersecurity presentation at passing out ceremony for F&amp;Rs [P6]</li> <li>• Present F&amp;Rs with materials at existing events F&amp;Rs attend [P6]</li> <li>• Pamphlet is quick and easy way to disseminate cybersecurity information directly to F&amp;Rs [P6]</li> <li>• Useful for F&amp;Rs to receive cyber materials when military person joins military [P7]</li> <li>• Website at government level for F&amp;Rs about deployment do's and don'ts online [P7]</li> <li>• Cyber materials could be conveyed in 30 second guide or poster [P7]</li> <li>• Open social media channels and FBS radio used to disseminate cyber messaging for F&amp;Rs [P14]</li> <li>• Cyber brief should be part of induction for F&amp;Rs living on military bases [P14]</li> </ul>

		<ul style="list-style-type: none"> <li>• F&amp;Rs training and education should be government led [P8]</li> <li>• Pamphlet about cybersecurity that is applicable for all generations [P8]</li> <li>• Cybersecurity messaging could be threaded into items already delivered to F&amp;Rs [P15]</li> <li>• Direct line or portal for Key Relations to feed cybersecurity concerns [P15]</li> <li>• Two way medium between defence and F&amp;Rs to provide guidance on security behaviours and a place to report incidents [P15]</li> <li>• Most military bases have family pages and social media sites to deliver cybersecurity messaging [P15]</li> <li>• F&amp;Rs cybersecurity portal would triage low level incidents and provide outputs to end user [P15]</li> <li>• Need to use existing link between welfare teams and families to access F&amp;Rs [P16]</li> <li>• Cyber initiatives should be set up through welfare teams and charities with an existing link to F&amp;Rs [P16]</li> <li>• Not a question of whether F&amp;Rs online behaviour needs to be addressed but a question of how [P17]</li> <li>• Distributing cyber messaging through families' federations with pre-established delivery methods [P17]</li> </ul>
	<p>Barriers to training engagement</p>	<ul style="list-style-type: none"> <li>• Training less beneficial for parents due to lack of online presence [P1]</li> <li>• People may not see benefit unless incentivised [P1]</li> <li>• Time gets in the way for training [P3]</li> <li>• Can't reach F&amp;Rs if unable to achieve secure cyber behaviours within military personnel [P3]</li> <li>• Challenging to monitor behaviours and behaviour change with F&amp;Rs due to lack of access [P5]</li> <li>• Behavioural change could be challenging with civilians with a less disciplined mindset than personnel [P5]</li> <li>• Resistance to conversations about cyber when saying you have to do something [P9]</li> <li>• Query over how information would be shared other than just telling people to look at something [P9]</li> <li>• Dad wouldn't get a lot from training &amp; awareness due to not paying attention [P9]</li> <li>• People outside the army won't see the big picture and so may not see benefit of training &amp; awareness [P9]</li> <li>• Lack of understanding from some people about different environments and that people are affected by online posting in different ways [P9]</li> <li>• People who have never had to worry about cybersecurity might struggle with understanding cyber concepts [P9]</li> <li>• Challenge within the military of people from a range of backgrounds and knowledge levels [P13]</li> <li>• Challenge with F&amp;Rs engaging initially as you can't order them to be anywhere [P13]</li> <li>• Training is only half the battle compared to initial buy-in [P13]</li> <li>• Talking about technical threats does not resonate with people outside of the IT worlds [P13]</li> <li>• Cybersecurity not appealing subject and people struggle to be interested [P13]</li> <li>• Letters don't always reach F&amp;Rs [P6]</li> <li>• Difficult for military organisations to access extended family directly [P6]</li> </ul>



		<ul style="list-style-type: none"> <li>• Challenge of messages getting through to F&amp;Rs via personnel [P12]</li> <li>• Behavioural change is very difficult when so many F&amp;Rs [P14]</li> <li>• Attempt to get social media and website channels for anyone to access is restricted and existing channels for MODNET devices encouraged [P14]</li> <li>• Easier to access F&amp;Rs living in vicinity of or on base compared to those located far away [P14]</li> <li>• Younger generation would dismiss a pamphlet [P8]</li> <li>• Cybersecurity language is direct and technical [P15]</li> <li>• Challenge of finding relevant cybersecurity case studies to share with F&amp;Rs due to classification of case study information [P17]</li> <li>• Physical magazines and pamphlets only read by a handful of people already engaged with military community [P17]</li> <li>• Challenge of how to get F&amp;Rs engaged rather than how to create content [P17]</li> <li>• Challenge of no existing method of directly engaging with F&amp;Rs themselves [P17]</li> <li>• Emails are not a good way to deliver content as people delete emails if they think content is irrelevant [P14]</li> <li>• Still a challenge of educating F&amp;Rs to understand technology even in digital age [P17]</li> </ul>
	Encouraging engagement with training	<ul style="list-style-type: none"> <li>• Cyber training initiatives would be beneficial for wife if online and in the evening [P1]</li> <li>• Training should highlight benefit for F&amp;Rs [P1]</li> <li>• Key Relations with an interest in cyber to become cyber champion for F&amp;Rs [P5]</li> <li>• Importance of monitoring and measuring behavioural shift [P5]</li> <li>• Explaining why a behaviour is bad is better than just stating it's bad [P9]</li> <li>• Dad would only get involved with training if he or someone close to him was a victim [P9]</li> <li>• Providing a hard-hitting example of a video where someone is hacked and then physical consequences could encourage security behaviours [P9]</li> <li>• Engagement at in person events encouraged with interactive games and freebies [P11]</li> <li>• Interaction with families has to be at a level for all family members [P11]</li> <li>• Explaining the why behind a behaviour encourages people to apply secure behaviours [P11]</li> <li>• Gamification could be beneficial in connecting with younger generation [P13]</li> <li>• Explaining the reason behind removing information online encourages understanding from F&amp;Rs [P6]</li> <li>• Passing-out day good opportunity for cybersecurity brief for F&amp;Rs as it is an enjoyable event [P6]</li> <li>• Materials should be accessible for everyone [P7]</li> <li>• Children aged as young as 8 should be able to access materials when they start going online [P7]</li> <li>• Consideration not to scare F&amp;Rs about cyber threats when already concerned about military person's physical safety [P12]</li> </ul>

		<ul style="list-style-type: none"> <li>• Cyber Champions mainly responsible for military personnel's cyber awareness but should also be engaging with extended community [P12]</li> <li>• Would be beneficial to have junior cyber champions who live in military patches [P12]</li> <li>• Beneficial to have cyber champions attend schools because they can take leaflets home to discuss information with parents [P12]</li> <li>• No reason why own F&amp;Rs wouldn't engage with training [P14]</li> <li>• Once secure behaviours become a routine they're easier to understand and apply [P8]</li> <li>• Older generation would read a cybersecurity pamphlet in down time [P8]</li> <li>• Military person would pass a pamphlet on to F&amp;Es and encourage them to read it [P8]</li> <li>• Potential reward for engaging in positive behaviours or helping others with their cybersecurity behaviours [P15]</li> <li>• Encouraging engagement with cybersecurity initiatives by sharing positive stories rather than negative behaviours [P15]</li> <li>• Buy-in is successful when phrased as a personal consequence for individuals rather than consequence for MOD [P15]</li> <li>• Importance of an approachable and open environment when engaging with F&amp;Rs [P15]</li> <li>• Can't enforce behaviours for F&amp;Rs but can offer guidance and advise engagement [P16]</li> <li>• Fear is a driver for encouraging people to engage in secure online behaviours [P17]</li> <li>• Case studies provide context for individuals interested in the why behind online security behaviours [P17]</li> <li>• Removal of military interface for F&amp;Rs to reduce barrier of apprehension towards approaching individual in uniform [P15]</li> </ul>
	<p>Extrapolating from existing military training</p>	<ul style="list-style-type: none"> <li>• Providing a reason not to do something rather than just saying not to do it [P9]</li> <li>• Build on shared experiences of military life [P13]</li> <li>• Ensuring real life examples are made relevant to military so people don't switch off [P13]</li> <li>• Gamified training with personnel useful to encourage discussions regardless of knowledge level [P13]</li> <li>• Introduction of more gamification and individually tailored approach to training [P14]</li> <li>• Attended briefing where attendees were searched online and public information was shared in brief to highlight their risk [P14]</li> <li>• Gamification of cybersecurity tools such as escape rooms and gameshows positively received by personnel [P14]</li> <li>• Advice focuses on having a locked down profile and limiting information in public domain [P15]</li> <li>• Statistics of amount of information social media platforms collect about you highlights the risk of oversharing online [P16]</li> <li>• Highlighting the importance of only sharing information online with people they trust [P16]</li> <li>• Case study examples of online risk behaviours that resulted in consequences for military are beneficial [P17]</li> <li>• Russia-Ukraine war has provided many open source examples of how F&amp;Rs have been used within cyber warfare [P17]</li> </ul>
	<p>Potential mitigations</p>	<ul style="list-style-type: none"> <li>• Deleting all social media would be successful if you don't know what you're missing [P1]</li> <li>• Safer option to not advertise they are in the RAF and where their family lives [P1]</li> </ul>

		<ul style="list-style-type: none"> <li>• Minimised information shared about job with wife even though both in similar roles [P11]</li> <li>• Technical solutions only effective if F&amp;Rs know solutions exist and how to implement them [P13]</li> <li>• Limits specifics about deployment to mum before arriving to reduce incidental information sharing [P7]</li> <li>• Limits sharing sensitive information with mother due to lack of trust she won't share onwards [P7]</li> <li>• All information shared with F&amp;Rs about potentially sensitive information is shared in person not online [P7]</li> <li>• Mitigating F&amp;Rs online risk behaviours by explaining what the impact is on the military person [P12]</li> <li>• Work devices should never be used by anyone apart from military person [P14]</li> <li>• Fitness tracking app profiles should be private or geo-location off [P14]</li> <li>• Reducing sharing pattern of life online that could be targeted by a threat actor [P14]</li> <li>• Deleting unused apps and downloading apps from reputable stores [P14]</li> <li>• Either locked down social media profile or extremely selective on content posted online [P14]</li> <li>• If work location is sensitive then limits detail shared with children [P8]</li> <li>• Can obfuscate more information to friends and extended family compared to spouse [P17]</li> </ul>
	Monitoring F&Rs online behaviour to reduce risk	<ul style="list-style-type: none"> <li>• Much more oversight of children's online behaviours when they were younger [P12]</li> <li>• Try to regulate children's time online but don't set up accounts [P12]</li> <li>• Discussion with children of a distorted view of reality and an echo chamber online [P12]</li> <li>• Recommends children to explore news outlets to corroborate information they see online [P12]</li> <li>• Parents provide children freedom online as they haven't shown any risk behaviours yet [P12]</li> <li>• Military personnel should encourage F&amp;Rs to lock down profiles [P14]</li> </ul>
	Challenges of measuring effectiveness of initiatives	<ul style="list-style-type: none"> <li>• Lack of metrics makes it difficult to measure effectiveness of initiatives on behaviour change [P11]</li> <li>• Challenging to ensure materials are reaching all personnel across workforce [P11]</li> <li>• Challenging to measure F&amp;Rs attendance for initiatives [P13]</li> <li>• Challenge of measuring impact of initiatives with metrics [P13]</li> <li>• Difficulty in measuring reception and effectiveness of cyber initiatives for F&amp;Rs [P12]</li> <li>• Metrics are important to explore effectiveness and behavioural patterns to address in future [P12]</li> <li>• Potential census to measure F&amp;Rs engagement with secure online behaviours before and after intervention [P14]</li> <li>• Challenging to measure effectiveness of cyber messaging with F&amp;Rs [P14]</li> </ul>
Military culture	Family experiences of military culture and lifestyle	<ul style="list-style-type: none"> <li>• Wife not posting sensitive information could be due to coming from a military family [P1]</li> <li>• Wife's father was in RAF [P1]</li> <li>• Wife has memories of looking under car for IRA bomb [P1]</li> <li>• Unsure whether wife's experience makes her approach to security different to the general population [P1]</li> <li>• Dad's experience of friends serving in NI increased his understanding of risk [P9]</li> </ul>

		<ul style="list-style-type: none"> <li>• Dual-serving household means extended family also have knowledge about military lifestyle [P11]</li> <li>• Hopes children have good cyber awareness due to dad talking about job frequently [P12]</li> <li>• Dual-serving household encourages discussions about cyber at home [P12]</li> <li>• Father in law is a cadet instructor and technically savvy [P12]</li> <li>• Wife has previous job role and family experience of military life [P8]</li> <li>• Dad's previous military career makes him tech savvy and doesn't need advising on social media behaviours [P8]</li> <li>• Military mindset that security is encouraged from onset and throughout career [P8]</li> </ul>
	Online risk is specific for military organisations	<ul style="list-style-type: none"> <li>• F&amp;Rs complaining on social media about communication difficulties with military person and unit exposes comms difficulties on operation [P12]</li> <li>• IT systems are important in supporting operations rather than system being main focus [P17] Focusing on cybersecurity can reduce reputational damage of people and organisation from media and press [P5]</li> <li>• Reputational damage occurs when something is posted online and taken out of context [P5]</li> <li>• Information about love triangles posted online can be damaging for organisation and individuals [P5]</li> <li>• Sensitive pictures online expose those in command to lack of respect from other personnel [P8]</li> <li>• Military laws focus on the reputational damage caused by adverse use of social media [P15]</li> <li>• Cyber-attack administered in modern warfare as it can be almost invisible [P5]</li> <li>• Individual personnel could be targeted and blackmailed due to information shared online [P15]</li> <li>• Threat actors can target military personnel but also leverage F&amp;Rs [P16]</li> <li>• Example in Afghanistan where threat actors found F&amp;Rs details and messaged serving personnel threatening F&amp;Rs [P17]</li> <li>• Reaching personnel through F&amp;RS is an extreme but potential during war or time of tension [P5]</li> </ul>
	Increased technological savvy due to military experiences	<ul style="list-style-type: none"> <li>• Living in bubble with wife's role in defence and friends being military, everyone is careful online [P3]</li> <li>• Friends behaviours also secure online as job either in military or role requires them to be secure [P3]</li> <li>• Wife's military cyber role means she understands the importance of secure information sharing behaviours [P11]</li> <li>• F&amp;Rs attend passing-out ceremony [P6]</li> <li>• Large number of friendship group are serving so can explain requirements to civilians [P7]</li> <li>• Wife is in the RAF and is considerate with online posts and connections [P12]</li> <li>• Living and breathing military culture equates to more conscious online choices about posting and friend requests [P12]</li> <li>• Dad is ex-military and understands online risk mitigations in place [P8]</li> <li>• Friends and colleagues engage in secure behaviours due to similar job roles and interests [P8]</li> </ul>
	Differences for civilians	<ul style="list-style-type: none"> <li>• People not in the military or a close relation don't understand consequences of online information sharing [P7]</li> </ul>

		<ul style="list-style-type: none"> <li>• Individuals with less military involvement except for serving relative are less aware online [P12]</li> <li>• Wife experiences challenges with balancing building online customer base for military-related business whilst remaining safe online [P8]</li> <li>• Importance of security is not as hard hitting for a civilian as it is for a military person [P8]</li> <li>• Difference in importance of cybersecurity for someone in military role compared to civilian role where success on social media is vital for job [P8]</li> <li>• Prior to engaging with military lifestyle wife would not be considerate of posting online content [P8]</li> <li>• Civilians have a different understanding of cybersecurity and resilience due to risk perception [P8]</li> <li>• F&amp;Rs are easier target than military personnel due to less cybersecurity training and education [P15]</li> <li>• Threat actor may target extended F&amp;Rs due to being a weak point in contacts [P15]</li> <li>• Challenging to educate F&amp;Rs on the importance of controlling sensitive information online [P17]</li> </ul>
	Current cultural approach for cybersecurity	<ul style="list-style-type: none"> <li>• Culture within military organisations of cyber being an unknown so lack confidence in providing guidance [P16]</li> <li>• Cultural approaches and problem solving is different between military branches [P16]</li> </ul>
	Existing training for personnel	<ul style="list-style-type: none"> <li>• Annual training and training every 3 years blur into one [P1]</li> <li>• Training is generic [P1]</li> <li>• Conflicting information about the use of social media profiles [P1]</li> <li>• Passive interaction with training to appease [P1]</li> <li>• Training that says don't even use social media is unrealistic [P1]</li> <li>• A lot of cyber information learnt through the job rather than formal training [P3]</li> <li>• Employer should encourage cyber training more by carving out time [P3]</li> <li>• Cyber training should be mandatory like diversity and inclusion training [P3]</li> <li>• Concern that defence is smaller with bigger problem so less time for training [P3]</li> <li>• Cyber resilience programme attempts to get breadth across workforce of understanding online behaviour [P3]</li> <li>• Cyber awareness, behaviour and culture is important across the Navy [P5]</li> <li>• Personnel who are reluctant to take cyber mindset would be unaware of a cyber attack [P5]</li> <li>• Importance of personnel adopting a cyber mindset [P5]</li> <li>• Barriers strengthened within organisation by operating with a cyber mindset [P5]</li> <li>• Main security for personnel is generic [P9]</li> <li>• Specific training provided for specific jobs and locations [P9]</li> </ul>

		<ul style="list-style-type: none"> <li>• Specific country training could be more specific about threats and how to genuinely mitigate against them [P9]</li> <li>• Own training consists of standard military cyber training and learning on the job [P11]</li> <li>• Picked up information by engaging with and administering cyber awareness briefs [P11]</li> <li>• Training mostly on the job through research [P13]</li> <li>• Those in a cyber role naturally more interested and seek out more information [P13]</li> <li>• Current threats made relatable to a military perspective [P13]</li> <li>• Existing mandatory training can be unrelatable and then people switch off [P13]</li> <li>• Cybersecurity training happened in phase 1 training [P6]</li> <li>• Training focussed on reducing online information through reduced information sharing [P6]</li> <li>• Further training for technology based role [P6]</li> <li>• Struggle to concentrate on cyber training because physical training is so demanding [P6]</li> <li>• Annual training about acceptable online behaviour [P7]</li> <li>• Additional training when working with higher classification information [P7]</li> <li>• Training should include more about only sharing information with F&amp;Rs you trust and they understand the importance of information [P7]</li> <li>• Unsure if limiting information to F&amp;Rs that might share is common sense or picked up in training [P7]</li> <li>• Existing cyber materials for personnel not necessarily appropriate for F&amp;Rs due to classification of threats highlighted [P12]</li> <li>• Defence contractors have MOD training and parent company training [P14]</li> <li>• Some cyber training modules overlap in content [P14]</li> <li>• Upskilled and learnt during role as well as cyber training [P14]</li> <li>• Annual mandated cybersecurity brief for personnel [P8]</li> <li>• Cybersecurity messages appear when MOD laptop switched on [P8]</li> <li>• Cybersecurity materials available for personnel to encourage secure online behaviours [P8]</li> <li>• Personnel educated that posting military information and holiday pictures online can result in exploitation [P8]</li> <li>• Experience in role of learning about new apps and risks to inform briefs [P8]</li> <li>• Military personnel receive cybersecurity pamphlets for social media settings and pre-deployment [P8]</li> <li>• Military personnel's cybersecurity training ticks the box for required criteria [P15]</li> <li>• Threat examples are based on global based cyber threats [P15]</li> <li>• Overseas locations provide training with local threat examples [P15]</li> <li>• Personnel briefed F&amp;Rs online behaviour is important as well as serving personnel [P16]</li> <li>• Personnel encouraged to set up F&amp;Rs devices with VPNs leftover from mandated account for own devices [P16]</li> </ul>
--	--	---

		<ul style="list-style-type: none"> <li>• Personnel receive cyber training and education yet still make mistakes [P17]</li> </ul>
	Perception of self in technology	<ul style="list-style-type: none"> <li>• Still views themselves as a cyber newbie whilst acknowledging their knowledge is still higher than average person [P11]</li> <li>• Always been interested in technology and considers themselves tech savvy [P8]</li> </ul>
	Encouraging positive Cybersecurity Culture	<ul style="list-style-type: none"> <li>• Focus on the benefits of secure online behaviours for F&amp;Rs rather than repercussions for not engaging [P15]</li> <li>• Importance of terminology reflecting that identifying risk behaviours is to protect rather than find fault [P15]</li> <li>• Encouraging a culture of lesson learning from cybersecurity incidents rather than punishment [P15]</li> </ul>
	Communicating requirements to F&Rs	<ul style="list-style-type: none"> <li>• Informed parents information about ship names and location cannot be shared online [P6]</li> <li>• Brother would ask why he had to remove post before doing it [P6]</li> <li>• Explained to mum why information about deployment is limited at times and she understands [P7]</li> <li>• Necessity of conversation would make it easy to communicate requirements to friends about online behaviours concerning military person [P12]</li> <li>• Military personnel should educate F&amp;Rs on not posting or tagging pictures of uniform or base [P14]</li> <li>• Highlighting importance to F&amp;Rs not to share military related information online about military person [P8]</li> <li>• Relying on military personnel to communicate information from educational briefs to F&amp;Rs [P16]</li> <li>• Service person is conduit for accessing cyber materials and communicating information to F&amp;Rs [P16]</li> <li>• Military levels of cyber knowledge assured with the hope information is passed along to F&amp;Rs [P16]</li> <li>• Personnel should encourage cybersecurity awareness and behaviours at home [P13]</li> <li>• Importance of materials should be reinforced by military person [P7]</li> <li>• Messaging at home discourages children from oversharing online [P12]</li> <li>• Concerns about social media would be communicated to F&amp;Rs without forcing them to engage and apply behaviour [P8]</li> </ul>
	Encouraging open dialogue	<ul style="list-style-type: none"> <li>• Encourages conversations with children about what they should be accessing online [P3]</li> <li>• Shares knowledge of basic online safety with others [P9]</li> <li>• Knowledge sharing in casual conversation [P9]</li> <li>• Wife would be understanding of conversations about security requirements [P9]</li> <li>• Feels they could discuss behaviour with friends openly [P9]</li> <li>• Family will ask for advice on whether emails or messages are suspicious [P13]</li> <li>• Military person should initiate open dialogues about cybersecurity with F&amp;Rs when deploying [P13]</li> <li>• Importance of open and honest dialogues with F&amp;Rs about online behaviours [P13]</li> <li>• Open dialogue and communication with family [P6]</li> <li>• Would ask family to remove risky online post but wouldn't hold them accountable for not knowing [P6]</li> <li>• Wife has a good understanding of requirements due to taking the time to explain why it's important [P7]</li> <li>• Explaining reasoning avoids sounding petty [P7]</li> </ul>

		<ul style="list-style-type: none"> <li>• Open discussions within the family about social media and the potential pitfalls [P12]</li> <li>• Encourages discussions at home about work topics including disinformation and misinformation [P12]</li> <li>• Encouraging conversations about online security to prepare them for any scenario they have to choose to make a safe decision online [P12]</li> <li>• If deployed would discuss privacy settings and risk of information sharing with in-laws [P12]</li> <li>• Friends would understand the reasoning behind limiting online presence [P12]</li> <li>• Friends would discuss and understand the importance of behavioural decisions for online security [P8]</li> <li>• Importance of explaining online risks to F&amp;Rs [P8]</li> <li>• Encourages open and honest discussions with F&amp;Rs to prevent regret of being evasive [P8]</li> <li>• Encouraging individuals to report online behaviour that appears suspicious to reduce potential threat [P15]</li> </ul>
	Barriers to open dialogue	<ul style="list-style-type: none"> <li>• Service person training families can lead to awkwardness and tension on relationships [P5]</li> <li>• General security behaviours not discussed to avoid tense conversations [P9]</li> <li>• Talking to dad about security is like talking to a brick wall [P9]</li> <li>• Can be painful to discuss security with dad [P9]</li> <li>• Would find it difficult to crowbar training/education materials for F&amp;Rs into a conversation [P9]</li> <li>• Awkwardness of calling people out on their behaviour [P9]</li> <li>• People chronically online struggle to understand military perspective as want to behave as they desire [P9]</li> <li>• Conversations about removing information online hurtful for some F&amp;Rs [P6]</li> <li>• Easier to have a conversation about cybersecurity with people who are IT literate and understand social media [P7]</li> <li>• Children questioning of parents' knowledge and experience even with dad in cyber role [P12]</li> <li>• F&amp;Rs may resist engaging in security behaviours when asked by military person as they want freedom to act how they want [P8]</li> <li>• More difficult to educate F&amp;Rs you don't know very well on cybersecurity [P8]</li> </ul>
	Knowledge sharing behaviours	<ul style="list-style-type: none"> <li>• Parents learnt about online scams through talking to friends, watching the news and reading the paper [P3]</li> <li>• Daughter tells friends information parents have told her about why it's important to engage in safe online behaviours [P12]</li> <li>• Children reaffirming knowledge by sharing within their circle is powerful [P12]</li> <li>• Will share information about social media settings with F&amp;Rs if perceived benefit [P8]</li> <li>• A focal point portal for F&amp;Rs should be connected to other organisations to provide data on potential threats [P15]</li> <li>• Effective cybersecurity knowledge sharing between organisations is key to address cyber resilience across MOD [P15]</li> </ul>



	Family and friends coming together to help	<ul style="list-style-type: none"> <li>• Brother also helps with basic technology behaviours with parents [P9]</li> <li>• Close family members can communicate requirements to extended family members [P6]</li> <li>• Dad would tell extended family members to remove concerning post when military person deployed [P6]</li> <li>• Family members would censor each other if military person was unable to [P6]</li> <li>• Friendship group including other military personnel helps explain it's not one individual being difficult [P7]</li> <li>• Other family and friends should support the older generation in keeping them tech savvy [P8]</li> </ul>
Responsibility	Responsibility of military person	<ul style="list-style-type: none"> <li>• Military person responsible for not sharing anything unsharable [P1]</li> <li>• Military person should have conversation with F&amp;Rs about their security requirements [P9]</li> <li>• Responsibility higher for individuals with children as they don't know how behaviours influence military [P13]</li> <li>• Military personnel expected to understand detail available to them about operations and exercises are not for general public [P11]</li> <li>• Service personnel should pass on cyber hygiene basics for F&amp;Rs to protect personnel and assets [P11]</li> <li>• Military person responsible for monitoring F&amp;Rs online behaviours in relation to military information [P6]</li> <li>• Responsibility of military person to know requirements for posting online as it's their job [P6]</li> <li>• Military person's responsibility to know when to (not) share information with F&amp;Rs [P7]</li> <li>• Responsibility is 99% the military person [P7]</li> <li>• Military person sharing information with F&amp;Rs should be dependent on trust that F&amp;R won't share online [P7]</li> <li>• Proportion of personnel not following online safety criteria indicates proportion of personnel not communicating criteria to F&amp;Rs [P12]</li> <li>• If personnel haven't got recommended communication platform installed on device, F&amp;Rs probably don't either [P12]</li> <li>• Responsibility of military person to educate F&amp;Rs when F&amp;Rs lack interest [P14]</li> <li>• Military person responsible for ensuring security settings control what other people can see [P8]</li> <li>• Military person should monitor F&amp;Rs online behaviour to ensure it's not inappropriate [P8]</li> <li>• Personnel responsible for sharing information from cybersecurity briefs with F&amp;Rs [P15]</li> </ul>
	Responsibility of the military organisation	<ul style="list-style-type: none"> <li>• Vicarious liability for any organisation for cybersecurity including defence [P3]</li> <li>• Cyber interest should come from leadership to encourage culture of acceptance and support [P5]</li> <li>• Importance of policy and strategy for incorporating F&amp;Rs in awareness and behaviour change [P5]</li> <li>• Organisation has the responsibility to protect service person and their Key Relations [P5]</li> <li>• Generally personnel follow rules once importance is highlighted [P5]</li> </ul>

		<ul style="list-style-type: none"> <li>• Cyber awareness is not role specific as everyone has access to knowledge that could be used by adversary [P11]</li> <li>• Responsibility for cyber initiative should come from cyber experts and communicated throughout personnel [P12]</li> <li>• Encouraging identifying vulnerabilities to keep personnel safe rather than blame culture [P12]</li> <li>• Air command should be interested in success of awareness briefs trickling down to F&amp;Rs [P12]</li> <li>• Creating a norm of cybersecurity awareness [P12]</li> <li>• Responsibility of line managers to ensure personnel are applying cybersecurity best practice [P8]</li> <li>• Next step for defence cybersecurity is to engage the wider military community [P15]</li> <li>• Work contributes to military aligning with civilian business practices rather than distinct military rules and regulations [P15]</li> <li>• Beneficial for F&amp;Rs but also as workforce moves to a more civilianised workforce [P15]</li> <li>• Breaking down barriers with F&amp;Rs in one aspect can encourage positive view of military [P15]</li> <li>• Leadership should engage in secure online behaviours to demonstrate exemplary behaviour [P16]</li> <li>• Materials could be joint effort across the branches as online security behaviours the same [P17]</li> <li>• Obligation from organisations to be responsible for F&amp;Rs online behaviours as they're the reason personnel are at risk and will experience majority of impact [P17]</li> <li>• Military organisations have an obligation to educate F&amp;Rs on cybersecurity to provide option of them to engage in behaviours [P17]</li> </ul>
	Responsibility of online platforms	<ul style="list-style-type: none"> <li>• Social media would be better with easy option to be more secure [P8]</li> <li>• Positive opinion towards tiktok introducing time limit for children on app [P12]</li> <li>• Would like to see platforms taking responsibility for monitoring children's platform usage [P12]</li> <li>• Positive opinion towards Instagram providing option to hide like count on posts [P14]</li> <li>• Pinned help bar on social media platforms to help identify how to set security settings safely [P8]</li> <li>• A help icon on social media pages for additional assistance when you reach a certain age [P8]</li> </ul>
	Shared responsibility	<ul style="list-style-type: none"> <li>• Responsibility is three-way split between the organisation, the service person and F&amp;Rs [P5]</li> <li>• Responsibility shouldn't fall to service person to train F&amp;RS due to lack of knowledge [P5]</li> <li>• F&amp;Rs not accountable for not knowing military requirements for online behaviours [P6]</li> <li>• Everyone who is online should be responsible for being aware of the dangers and seeking out safety information [P11]</li> <li>• During day-to-day life responsibility shouldn't solely be on serving person [P13]</li> <li>• Responsibility from perspective of personnel and F&amp;Rs should be covered [P12]</li> <li>• Reliance on personnel and F&amp;Rs setting up signal correctly to be secure [P12]</li> <li>• F&amp;Rs aren't solely responsible due to limited cyber education in relation to military [P12]</li> <li>• Responsibility is a 50/50 split where F&amp;RS need to take ownership of behaviour but correct message should be enforced by personnel [P14]</li> <li>• If information is passed on it is then up to F&amp;Rs to apply information [P8]</li> </ul>

		<ul style="list-style-type: none"> <li>• Should approach military personnel and F&amp;Rs as a package rather than separate entities [P15]</li> <li>• Military person acts on behalf of F&amp;R if consequence from F&amp;Rs behaviour [P15]</li> <li>• Responsibility of an individual household or family to secure their own online behaviours [P15]</li> <li>• Defence terminology move to whole force to reflect that employees come from military personnel, defence contractors and civilians [P15]</li> <li>• Responsibility for F&amp;Rs online behaviour is shared between military person and their F&amp;Rs [P15]</li> <li>• Everyone in the chain with access to information has a responsibility to keep it safe [P17]</li> </ul>
	Situational responsibility	<ul style="list-style-type: none"> <li>• Deployed military person cannot frequently monitor F&amp;Rs online behaviours [P6]</li> <li>• Deployment delays communication with F&amp;Rs presenting risk of information sharing behaviours going unnoticed longer [P6]</li> <li>• Responsibility of military person to communicate requirements to F&amp;Rs when deploying [P13]</li> <li>• F&amp;Rs aren't aware of risks when individual is deployed and how to mitigate against risks [P13]</li> <li>• Responsibility dependent on the knowledge and training F&amp;Rs receive professionally or at school [P13]</li> <li>• F&amp;Rs with professional cyber experience should have more behavioural responsibility [P13]</li> <li>• If F&amp;Rs want to protect loved one's responsibility to behave securely online is on them [P14]</li> </ul>

## Appendix J: MODREC Letter of Favourable Opinion for Phases 3 & 4



**MODREC Secretariat  
Defence Science and Technology**

Dstl Portsdown West, Fareham, PO17 6AD  
Telephone: 0300 153 5372  
E-mail: [DST-MODRECTeam@mod.gov.uk](mailto:DST-MODRECTeam@mod.gov.uk)

Our Reference: 2256/MODREC/23

Date: 18 Oct 2023

Dear Miss Kooner-Evans,

***Exploring the role of service personnel's key relationships in military cyber resilience***

Thank you for submitting your revised application (2256/MODREC/23) with tracked changes and the covering letter with detailed responses to the MODREC letter. I can confirm that the revised protocol has been given a favourable opinion ex-Committee. **Please only use the definitive, clean file version of the protocol from now on, which is attached (V3.3, dated 16 Oct 2023).**

This favourable opinion is valid for the duration of the research and is conditional upon adherence to the protocol – please inform the Secretariat if any amendments become necessary.

Please note that under the terms of JSP 536 you are required to notify the Secretariat of the commencement date of the research and submit annual and final/termination reports to the Secretariat on completion of the research.

## Appendix K: Bournemouth University Letter of Ethical Approval for Phases 3 & 4



Dear Francesca Kooner-Evans,

Your checklist (Exploring the role of service personnel's key relationships in military cyber resilience) has now been reviewed and **APPROVED** in line with [BU's Research Ethics Code of Practice](#).

The reviewer provided the following comments:

No additional comments provided

You can now save and/or print off a hard copy of the checklist at <https://ethics.bournemouth.ac.uk>.

This approval relates to the ethical context of the work. Specific aspects of the implementation of the research project remain your professional responsibility.

It is your responsibility to ensure that where the scope of the research project changes, such changes are evaluated to ensure that the ethical approval you have been granted remains appropriate.

Should you need to make any modifications to your project e.g. request an extension, increase the number participants (recruitment), submit an Amendment Request via the online ethics checklist. Requests will be considered by the original Approver. Changes cannot be implemented until relevant approvals are in place. See 'Amendments' for further guidance.

*Students – if the scope of your research changes, please discuss with your Tutors/Supervisors before submitting a new checklist or an Amendment Request.*

Many thanks

For UG/PGT enquiries – please contact your Supervisor in the first instance

For general enquiries – please email [researchethics@bournemouth.ac.uk](mailto:researchethics@bournemouth.ac.uk)