Recruiting and Training the Defence Forces' Cyber Capability

Comdt Eoin Scanlon

BSc MSc

5th Joint Command and Staff Course

Submitted in part fulfilment of the requirements for the
MA (LMDS)
Maynooth University
2022-2023

Supervisors: Dr. Laura Brown, Maynooth University

Comdt Stephen Molumphy, Defence Forces

MA (LMDS)

Student Declaration

1. I certify that this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.

2. Permission is given for the Military College Library and the NUI Library Maynooth to lend or copy this dissertation upon request.

3. The views and conclusions expressed herein are those of the student author and do not necessarily represent the views of the Military College, the Defence Forces or Maynooth University.

Signed: Eoin Scanlon **Rank:** Commandant

Name: Eoin Scanlon **Date:** 26 May 2023

Acknowledgements

I am extremely grateful for the guidance, feedback and motivation I have received from my supervisors Dr. Laura Servilan Brown and Comdt Stephen Molumphy throughout this journey. Their advice has been invaluable to me, encouraging me to pursue my interests whilst ultimately helping me believe in the utility of this research. I also wish to thank the School Commandant and Chief Instructor of the Command and Staff School, Col Dermot Hanifin and Lt Col Robert Kearney, for facilitating and encouraging this research during a very demanding yet equally rewarding course.

Furthermore, I am profoundly grateful to my friends, whose unwavering friendship, support, and guidance were indispensable in helping me complete this thesis. In particular, I would like to express my appreciation to my fellow students of the 5th JCSC, from whom I learned so much. My colleagues in the CIS Corps were always there to offer advice, and I am grateful for their expertise and wisdom.

I would particularly like to acknowledge the example set by my father, Lt Col (retired) Eddie Scanlon, without whom I would never have gotten this far in the Defence Forces. In fact, I couldn’t have joined if it weren’t for his help. His thesis (Scanlon, 2004) on this same course – written while I was a cadet on the other side of the square in 2004 – was the first I read last year. Despite a few spelling mistakes, it inspired me to give this course a solid effort and follow his example. My dad and my mam, Bernie, have been a rock of support for me and my own family, and I am forever grateful.

Finally, my wife Claire has put up with *a lot* over the past year. She selflessly took from her free time and gave it to me, encouraging me to try harder and pursue my academic goals. My two children Sophie and Ted didn’t help at all, but that’s their job – and I wouldn’t change it for the world. Thank you especially, Claire, Sophie and Ted. I owe you all some time back!

Abstract

(Word Count: 15,868)

The cyber domain presents many challenges for all aspects of national defence and security. Cyber threats today loom persistently in the background of all systems connected to the internet, and all forecasts for the predictable future amount to the progressive increase of cyber activities ‘below the threshold of war’ punctuated by periodic catastrophic cyber incidents. As a key component of Ireland’s national defence, the onus is on the DF to prepare itself adequately to fulfil its roles in the cyber domain, specified or otherwise.

The DF must examine ways to boost cyber recruitment, technical training and general military education in order to ensure its responses to cyber incidents – at home and overseas – are appropriate to the threat. The cyber domain is ubiquitous at this point, and its presence has been forced upon the DF without the appropriate time to prepare and adjust. The CIS Corps – the DF’s de facto cyber force – does not systematically train its personnel for cyber; nor does it recruit specifically for cyber. More broadly, the DF does not systematically educate the average soldier or officer in cyber until far too late in their career.

To assess these gaps in DF cyber efforts, inferences are drawn from the cyber initiatives of the US, Canadian and British Armed Forces. Each military is unique in the context of cyber, with their various recruitment mechanisms, training pathways and Professional Military Education (PME) courses differing significantly, depending largely on the roles and functions required. In addition to providing recommendations to address the various challenges, this research puts forward a finding of significance: a DF Cyber Strategy must explicitly define the functions and outcomes expected from its cyber workforce, as there evidently does not exist such thing as a standard cyber technician or operator.

This research also demonstrates the utility of the Cyber Security Body of Knowledge (CyBOK) mapping framework – with novel adjustments uniquely applicable to the DF – as a tool to benchmark and assess cyber training and education. It is demonstrated that the current scheme of DF-sponsored postgraduate cyber education is not meeting to the desired learning outcomes of cyber security experts in the DF, introducing potential vulnerabilities and inefficiencies.

Table of Contents

Table of Figures

Table of Tables

Glossary of Acronyms and Terms

CAF	Canadian Armed Forces
CIS Corps	Communication and Information Services Corps
CIST	Communication and Information Services Technician
CGSC	Command and General Staff Course (US)
CO	Cyberspace Operations
CoDF	The Commission on the Defence Forces
CyBOK	Cyber Security Body of Knowledge
DoD	Department of Defence (Ireland)
DOD	Department of Defence (US)
DF	Defence Forces
FCCI	Forensic Computing and Cybercrime Investigation (UCD MSc)
IT/ICT	Information Technology / Information and Communications Technology
JCSC	Joint Command and Staff Course (Ireland)
KA	Knowledge Area (CyBOK)
KWoP	Key Word or Phrase (CyBOK)
MOD	Ministry of Defence (UK)
MSc	Master of Science Degree
NCO	Non-commissioned Officer
NCSC	National Cyber Security Centre (Ireland)
NCSS	National Cyber Security Strategy (Ireland)
PDF	Permanent Defence Forces
PME	Professional Military Education
RDF	Reserve Defence Forces
Signalman/woman	Enlisted rank of the CIS Corps; equivalent of Private rank
SME	Subject Matter Expert

Introduction

How does the Defence Forces (DF) rise to the opportunities and challenges posed by one of the most significant developments in modern military history – the cyber domain? This research will demonstrate that when it comes to training the people charged with cyber-technical and leadership roles, the DF is preparing for the cyber domain sub-optimally. The Corps with primary responsibility for cyber – the Communications and Information Services (CIS) Corps – does not *systematically* train its technicians for cyber. Furthermore, cyber workforce recruitment is almost exclusively restricted to the DF's pool of enlisted soldiers, introducing important practical concerns and being at odds with other Western militaries. To meet the demands placed on the DF both militarily and in a national context, particularly in the wake of the Health Service Executive (HSE) ransomware attack of May 2021, all cyber efforts must be primarily rooted in people. Good recruitment pathways and coherent, systematic training should therefore be important – if not vital – to DF cyber resilience.

This research will compare the cyber-recruitment and training pathways of other militaries with the DF's. Pragmatic recommendations are formulated to guide future decisions when addressing the well-known challenges of shortages of specialist CIS technicians (CIST), the less-well-known challenges of ill-defined technical cyber training, and the possible challenges of sub-optimal cyber-leadership training.

Literature Review

The literature pertaining to cyber-military matters tends to converge at the strategic level, given that it is there where some of the most significant implications reside. At the practitioner level, there is a wealth of information in the form of technical books, peer-reviewed articles, and a trove of material online aimed at teaching and progressing new ideas and technologies. A number of key sources were identified in the research of this topic, and a brief overview is given here.

The selected sources focus on (1) the recruitment pathway of the cyber workforce in the Canadian Armed Forces (CAF), (2) the analytical and knowledge-based mapping of technical cyber skills, and (3) the importance and mechanisms of introducing meaningful and coherent cyber training to non-technical military leaders. These sources ultimately provide the research justification, as well as foundational ideas for the integration of such practices into the DF.

The first source is the recruitment website of the CAF (Canadian Armed Forces, 2022a). The CAF recruits its technical CIS-related roles directly into the Royal Canadian Corps of Signals (RCCS) once basic educational requirements are met. There are six technical roles within the RCCS, including the addition of the newly created Cyber Operator role (Government of Canada, 2017). Cyber Operators however are recruited exclusively from within existing ranks of the CAF – without any third-level education requirements – and undergo a 72-week period of cyber-specific training. This case study is relevant to the DF CIS Corps via similarities of scale and scope, and qualified inferences may be drawn. It should be noted however that such institutional websites are likely to carry certain biases, contain outdated or incomplete information, and may be aspirational rather than descriptive – factors treated accordingly in Chapter One.

The second source is the 'Cyber Security Body of Knowledge' (CyBOK, 2021a), an ongoing effort to establish a solid foundation for technical cyber skills. The CyBOK project is a collaboration involving academics, industry experts, and government organizations worldwide, sponsored by the UK Government's National Cyber Security Programme. Its goal is to standardize cybersecurity knowledge and skills using "Knowledge Areas" (KAs) as broad topics that encompass learning for all cyber roles. KAs are further divided into indicative training content. The project also evaluates certifications and courses, generating maps of strengths and weaknesses (see Fig. 1). This mapping will be considered in Chapter Two when analysing current DF cyber training.

One danger when using methodologies as presented in the CyBOK is the potential for information overload and reduction of a clear and coherent ‘result’. The authors went to great lengths to capture everything relating to the current state of cyber skills[1], and essentially *everything* made the final product (Rashid, A. et al., 2018). A work that may be fairly described as an honest and detailed assessment of contemporary cybersecurity, may also be described as complicated and practically unwieldy. Nevertheless, with suitable rigour and a clearly defined research question, the CyBOK should aggregate to a useful methodology.

[1] Focus groups, workshops and interviews were conducted with academics, practitioners, primary and secondary educators, authors and the public over a period of more than two years.

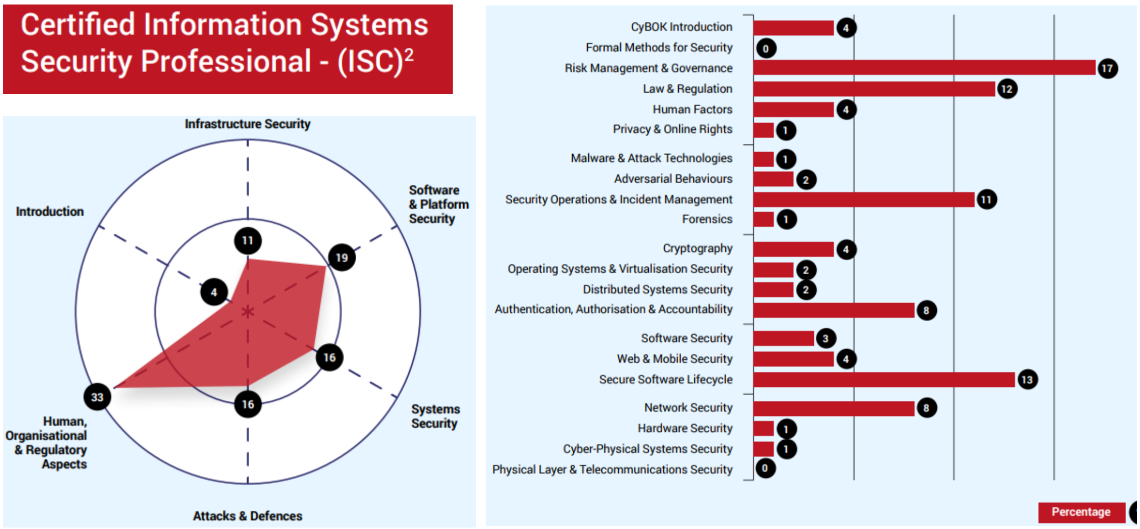


Figure 1: *A CyBOK 'map' for the Certified Information Systems Security Professional accreditation (CyBOK - Cyber Body of Knowledge, 2021a, pg. 6). Note the significant emphasis placed on human, organisational and regulatory aspects.*

The third source is "Cyber Security as a Field of Military Education and Study" (Tikk-Ringas et al., 2014). The authors, drawing on their diverse backgrounds in legal, technical, and social aspects of cybersecurity, propose a holistic reflection based on their experience designing workshops and courses for military and civilian audiences. They argue that cyber principles should be included in general leadership training for all military officers. The article highlights different focuses at various levels, from basic technical foundations for cadets and junior officers to service-specific capabilities at operational levels, and strategy and policy at senior levels. The authors advocate for aligning military cyber curricula with rank and role, which may also be relevant for the DF. However, it's worth noting that the article's observations were primarily based on senior military education courses *up to* 2014, thus some findings may not be applicable in the contemporary context.

Research Lacunae

Having critically examined the available and relevant literature on the recruitment and development of cyber personnel in the military, it is apparent that a number of lacunae exist. The first is that there exists an emerging consensus among Western militaries that cyber roles should be stratified and filled by specialised recruitment[2], yet the DF has not formally examined this in the context of cyber. Furthermore, cyber training in the DF has not been critically assessed, for example against a framework such as the CyBOK. Current CIS cyber-related training has ostensibly evolved from other technical requirements, such as electronic engineering or IT, without being meaningfully defined first. Finally, the literature generally makes a strong case for the universal integration of cyber at all levels of military leadership training. It is certainly far from clear how the DF should, or could, adopt such an aspiration. This research aims to synthesise the available material on the subject and indicate a new path forward for the DF in each of these thematic areas.

Research Questions

This research proposes the following three research questions, which follow a certain chronological flow of 'recruitment to development' for cyber-technical and leadership expertise in the context of the DF.

1. Recognising both the current roles within the CIS Corps and the 'real-world' constraints placed on human resources, how does the DF recruit an appropriate cyber workforce?
2. Given the DF's IT infrastructure, its communications technologies and recent events such as the HSE ransomware attack, what skills should cyber technicians possess, and what are the pathways to attain these skills?
3. To what extent should general cyber education be integrated into Professional Military Education (PME) in the DF, in line with other militaries?

Sources

Primary documents and sources are the main subject of analysis for the first research question. The published websites and documents of other militaries contain in some cases much indicative material in relation to how specialists are recruited and trained into cyber roles, and very little in other cases. Further research may reveal more detail, or even peer-reviewed research, but it is likely that inferences must be made from the correlation of primary sources before applying them to the DF context.

[2] Recruitment of those people with skills or education prior to enlistment, as opposed to general enlistment.

Secondary sources become more relevant and available for the next two research questions, with primary sources also informing where available. The CyBOK, for example, is a primary document that has generated peer-reviewed work, enhancing the potential for a more balanced understanding of its domain of applicability and usefulness. Finally, there are relevant secondary sources exploring the topic of cyber education in a non-technical and leadership context. Synthesising common findings and conceptually applying these to the DF is the primary analytical goal of Chapter Three, and will form an important part of the final recommendations.

Methodology

A qualitative research methodology is adopted, with a significant focus on document-based data collection and analysis. This methodology helps ensure two key research priorities are achieved throughout. The first is to identify and qualify potential biases or matters of contextual relevance, since the majority of the literature emanates from other countries and markedly different circumstances. The idea is to minimise the dangers of drawing erroneous conclusions, or trying to fit a 'square peg in a round hole'. Thus, a Systematic Literature Review (SLR) is chosen as the tool for analysing the mainly primary sources available. Such methodology is in theory a "replicable, scientific and transparent process" that explicitly aims to minimise bias (Tranfield et al., 2003, p.209) and generate a logical sequence of reasoning between the research questions and findings.

The second priority is the construction of a practical and *reasonable* model that best addresses the functional requirements of a cyber-workforce in the DF. The recommendations must be tenable. While retaining some degree of aspiration, simply developing theoretical models for recruitment and training of specialist cyber personnel without practical considerations would damage the utility of this research. Elements of Grounded Theory (GT) will thus be used to inductively reason solutions that might suit the DF, qualified by the SLR. Developed by Glaser and Strauss (1967), GT ensures that the theory fits the unique circumstances under investigation, having been informed by the data.

Thesis Outline

While the challenges and opportunities identified in this research will likely neither be fully addressed nor realised respectively, a methodological examination of available best-practices should nevertheless provide a reasonable and pragmatic indicative path towards obtaining a well-defined and resourced DF cyber function. The research herein is bespoke to the DF, concerned only with the contemporary and functional requirements of similar cyber functions and – to the best of the author’s knowledge – has not been academically assessed before.

Chapter One will consider the differences between the cyber-recruitment of selected Western militaries and the DF. A qualitative exploration of alternative mechanisms may provide some justification for decision makers seeking to boost the CIS Corps’ cyber workforce.

Chapter Two will assess CIST training from a cyber-perspective, using the CyBOK, and research realistic pathways to achieve improved standards and function. The DF is a relatively small organisation with resourcing difficulties, and care will be taken to propose tenable recommendations.

Chapter Three will examine the literature on the topic of general cyber training for military leaders, the benefits yielded and how such a concept may work for the DF. The extent to which this may be both justified and achievable will be assessed.

Finally, the concluding chapter will generate a synthesis of the complete research, summarising the key recommendations and discussing recommendations for future research.

Chapter One – Recruiting a DF Cyber Workforce

"If you think it's expensive to hire a professional, wait until you hire an amateur."

- Red Adair

1.1 Introduction

This chapter analyses and discusses some of the relevant and contemporary issues relating to the recruitment of personnel for military roles in cyber. The DF's de facto recruitment of cyber practitioners is discussed, highlighting some of the key difficulties and deficits of the current mechanism. Two case studies – the British Army and the Canadian Armed Forces – are examined to help qualify elements of an indicative, pragmatic solution. Although these militaries are markedly different in scale and role to the DF, they are doctrinally similar and share similar values; so making qualified inferences is a reasonable task. It is important to note that this research will not address the important aspects of recruitment such as pay, conditions of service, pensions and so on. While any indicative solutions must consider these factors, they belong to a more suitable form of analysis, with direct access to accurate information.

Many factors contribute to the difficult position that the DF is in, and there is no off-the-shelf solution to 'fix' the problems outlined herein. It does appear that most militaries are struggling with the recruitment and retention of cyber specialists; and the hope is that the DF can learn from their experiences. Prior to suitable analysis, it is necessary to first summarise the situation the DF finds itself in with respect to cyber.

1.2 Cyber and the Defence Forces

'Cyber' itself is a relatively meaningless term[3], so being granular and precise is quite important. A succinct, if oversimplified, summation of military cyber functions may include:

- Cyber Security – focusing on the computer network security to ensure confidentiality, integrity and availability of key resources;

[3] From the perspective that it is just too broad. Having said that, the term will be used throughout this work for simplicity.

- Defensive Cyber Operations – detecting and mitigating adversarial cyber activities, with a focus on the operational aspects;
- Offensive Cyber Operations – achieving mission-oriented effects on adversarial networks and systems.

These broad definitions matter, as they directly imply the type of recruitment and training required. It is also important to state at the outset that the DF does not strictly have a cyber function, outside of a small incident response team, nor does it purport to recruit specifically for cyber. Rather than write most of this thesis off as a straw man argument, two important factors should be considered. First, CIS Corps personnel are increasingly working within cyber, despite their actual appointments. Thus, the CIS Corps' roles are expanding into cyberspace regardless of Defence Forces Regulation (DFR) CS4[4]. The establishment of the DF is highly regulated, requiring layers of bureaucratic approval for most changes, notably including the Department of Defence (DoD) and the Department of Public Expenditure and Reform (DPER). DFR CS4 prescribes the roles of CIS technicians as they pertain to the 'classical' roles of military communications. Changing this to include cyber may require newly defined roles, people and ultimately more money.

The second factor is that recent publications, i.e. the Report of the Commission on the Defence Forces (CoDF) (Commission on the Defence Forces, 2022), the associated government decisions of the High Level Action Plan (Government of Ireland, 2022) and the National Cyber Security Strategy (NCSS) (Government of Ireland, 2019a), indicate that the DF is now required to do more in the cyber domain. Furthermore, the DF played a critical role in reacting to the 2021 cyber attack on Ireland's Health Service Executive (HSE, 2021) – described as the "largest known attack against a health service computer system in history" (US Department of Health and Human Services, 2022). However, similar to arguments about the DF more broadly[5], what exactly the DF should be doing in cyber is not clear.

The NCSS is not clear on the role of the DF, other than as a key supporting agency. The DF Cyber Defence Strategy, although light on detail, lists the strategic objectives as: (1) "Defend the Defence Forces Communications and Information Networks & [sic] Management Information Framework at home and overseas"; (2) "Develop Cyber

[4] This regulation provides the numbers, roles and qualifications of all ranks and appointments in the DF.
[5] Usually in the context of an absent National Security Strategy or political direction, it is often assessed that the DF does not have a clearly defined defence role.

Security awareness amongst members of the Defence Forces", and; (3) "Enhance strategic relations with other State Bodies/Organisations and International Organisations […]" (Defence Forces, 2013). This should inform the skills, training and outputs required of the DF's cyber workforce, but it evidently does not.

1.3 The Problem

There are two primary enlisted roles in the DF's CIS Corps – the Communications Operative and the CIST. A concise description of these roles is that the former is the trained operator of military communications systems, and the latter is the electronic engineer responsible for installation, maintenance and development of these systems. Neither have cyber as a core competency.

In 2006, the CIS Corps amalgamated the previous roles of IT Support Technician (ITST), Software Engineer Technician (SET) and Electronic Engineer Technician (EET) into one – the CIST – partly in an effort to standardise management and operational issues, such as promotion and overseas deployment criteria. Now the de facto educational pathway of the CIS Corps to develop its cyber-capability has become University College Dublin's (UCD) MSc in Forensic Computing and Cybercrime Investigation[6] (UCD, 2022), and via relatively small numbers of personnel on a periodic basis. Consider then the indicative timeline for a CIST to complete this MSc, as shown in Figure 1.

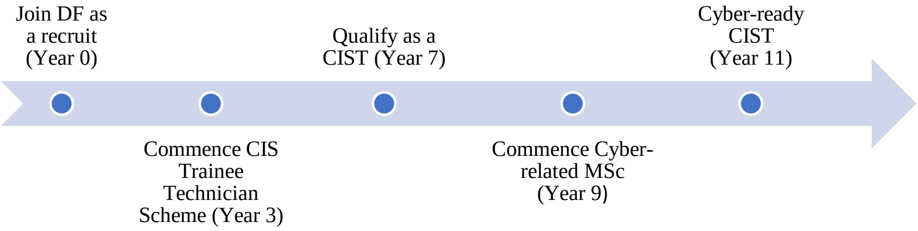

Join DF as a recruit (Year 0)
Commence CIS Trainee Technician Scheme (Year 3)
Qualify as a CIST (Year 7)
Commence Cyber-related MSc (Year 9)
Cyber-ready CIST (Year 11)

Figure 2: *Indicative timeline for qualification of a cyber-ready CIST.*

This demonstrates one fundamental issue with training a cyber-qualified CIST – the duration. This may of course vary, but usually upwards[7]. Thus the first assertion is that

[6] Applicants require an undergraduate degree, which they achieve on completion of the CIS Trainee Technician Scheme. The MSc usually takes between 2-3 years to complete.

[7] The only assumptions on this timeline are 3 years from recruit training to entry to CIS TT Scheme, and 2 years from completion of scheme until commencing the MSc. These estimates would be on the lower end of typical.

eleven years to train a cyber-technician is not ideal, particularly since this is the *only* pathway in the DF[8]. Furthermore, a compounding factor with this sequence of training is that those cyber-qualified CISTs who now work in cyber roles then necessarily stop doing CIST-related tasks they were trained for – such as maintaining radios and equipment, research and development, IT networking and so on. The second assertion is that given the significance of the cyber domain in contemporary defence and security, merging the roles of CIST and cyber is inefficient[9], expensive, leaves important gaps in other CIS functions and realistically reduces the individuals' remaining length of service[10] in cyber roles, if not the DF.

Another problem – and the third assertion, supported by aspects of the following case studies – is the false dichotomy the DF has presented itself. There is no particular reason DF cyber roles must be filled from the ranks of CISTs. The current justification includes contemporary issues around technical pay in the DF, and the requirement for an undergraduate degree to study for a cyber MSc. The former is out of scope of this work, and the latter is somewhat of an arbitrary problem[11], as the following case studies will show.

Military leadership often expresses concerns about retaining specialised personnel, viewing it as a problem that requires financial solutions. However, the US Department of Defense (DOD) found that despite "retention bonuses and special pays, [the armed forces] continue to experience challenges retaining qualified cyber personnel" (Graham, E., 2022). This challenge is consistently highlighted in the literature. Additionally, recruitment is seen as an even more challenging task. Gregg Kendrick, Executive Director of the US Marine Corps Forces Cyberspace Command, stated that "[r]etaining a force is tough but it is doable. Recruiting the force is significant" (Lynch, J., 2018). It is commonly believed that many specialists will leave the military when better opportunities arise, making recruitment and maximizing their service time crucial. While retention measures are important, relying solely on them may not be the most effective strategy.

[8] Some initial work has been done to permit 'Advanced Entry' to the CIS TT Scheme for those with suitable civilian qualifications, but details are unclear and it has not yet materialised.

[9] Chapter 2 will break down CIST training in the context of cyber and suggest educational gaps.

[10] The general consensus is that the military can't compete with the private cybersecurity sector in terms of remuneration.

[11] In that the more typical requirements are undergraduate cyber-related degrees, or alternative, relevant qualifications, including professional certifications.

The final contextual piece that must be highlighted is that the DF currently has an establishment for one officer, two NCOs and two Signalmen/Signalwomen in its only de facto cyber unit[12]. Recent developments and documents have significantly driven the cyber agenda forward as described earlier, however at the time of writing, the DF's official establishment is five personnel. An important caveat is therefore placed on the conclusions herein; if the DF wishes to retain the status quo, then some of the recommendations may not be valid.

1.4 British Military

This section provides an overview of the British Army's cyber workforce generation and the various pathways available. The UK's defence organization offers a range of cyber recruitment mechanisms tailored to different cyber units and services. The Royal Signals Corps technicians in the British Army are recruited into specific cyber roles such as Cyber Engineer, Electronic Warfare Signals Intelligence Specialist, Supply Chain Operative, Power Engineer, and Communications Troop Officer (British Army, 2022a). Civilians with relevant qualifications can join as specialist 'direct entry' officers and work within their field after basic military training. Selection for these roles involves customised assessments, including the Cyber Aptitude Assessment (Military Fitness, 2022). New recruits interested in technical trades, including Royal Signals and Cyber, are required to take a technical selection test, although it is unclear if the Cyber Aptitude Assessment is part of this process. Rigorous aptitude assessments are also increasingly emphasized in the civilian cyber sector.

Although financial considerations are beyond the scope of this research, they are important and should be alluded to where relevant. In 2020 the UK's Armed Forces Pay Review Body (AFPRB) published its annual review of military pay, allowances and charges, concluding that

> […] with the future skill requirements of Cyber […] MOD will face a major challenge unless they change their traditional approach to Terms and Conditions of Service […]. We think that MOD should think outside the box of the existing pay and career structure and give serious consideration to the use of a bespoke pay spine for this critical group. (AFPRB, 2020, p.55)

[12] A Cyber Incident Response Team (CIRT), part of the establishment of a CIS Company

The point was made again in the next report in 2021 (AFPRB, 2021, p.58). Since then, the MOD introduced 'Unified Career Management' (UCM) for cyber specialists[13], a "new approach to career management for select groups of military personnel" (UK Government, 2021b). UCM centralises the management of cyber-specialists defence-wide under Strategic Command in an effort to address career progression difficulties and obstacles experienced by cyber personnel as they compete against the rest of the military. It also affords cyber specialists the opportunities to deepen their expertise[14] and offers improved job security (UK Government, 2021b). The 2022 AFPRB report lauds the UCM and its potential to "deliver benefits to individuals and Defence and, potentially in areas of skills shortage, reduce the reliance of Defence on remuneration packages" (AFPRB, 2022, p.95).

In terms of flexibility in recruitment, the UK stands out in the literature. Importantly, consider that "the UK military has now officially moved to relax its recruitment rules to allow cyber specialists from the private sector to enter the military laterally" (Nawrat, A., 2021). On this point, then Head of Strategic Command[15] (now Chief of the General Staff) General Sir Patrick Sanders in 2021 stated

> I'm interested in people who may want to come in and spend a bit of time in defence, gain their credentials, their credibility and then move in and out, […] [a]nd so that idea of a much more flexible approach to a career in defence, encouraging 'lateral' entry, and also looking at people with very different entry standards to what we traditionally expect. (Warrell, H., 2021).

Furthermore, to generate diversity[16] in the British military's cyber efforts, the MOD and Army's Strategic Command engage in outreach programmes, including "Cyber First", "Code First Girls" and "Black Codher" (Nawrat, A., 2021). These are interesting and relevant strategies that may boost recruitment further down the strategic road. In fact, "more than 8,700 girls from across the UK" took part in the 2023 'CyberFirst Girls' competition (National Cyber Security Centre, 2023) for example.

[13] Although UCM is exclusively cyber, MOD's website reports that it is also "being considered for other groups of specialists" (UK Government, 2021b).

[14] A feature of the literature is that cyber specialists generally tend to want to remain specialists, deepening their knowledge of an area they enjoy. Most armies tend to penalise this, with increasing pressure to periodically change roles and 'tick boxes' for their personal file.

[15] Strategic Command has command authority over British military cyber functions.

[16] Diversity is a key component of the British Army's People Strategy, but also the main argument of the Army's *Diversity and Inclusivity Strategy*.

Within the wider MOD, civilian graduates of cyber degrees can consider an apprenticeship through the Defence Engineering and Science Group (DESG) Graduate Scheme. The scheme is a program offered by the MOD to recruit and train recent graduates in engineering, science and technology disciplines, including cyber (Ministry of Defence, 2022c). The scheme provides on-the-job training and development opportunities to help graduates gain practical experience and skills in their field, with the goal of producing future leaders and experts in the MOD's defence engineering and science community. Cyber graduates remain in the MOD and work on cyber projects for, and with, the military.

For prospective military cyber specialists, all of this amounts to a significant revision of career management in their favour, fairer remuneration over time and increased opportunities for further specialisation. For their civilian counterparts in the MOD, it means better opportunities on defence-related projects, flexible and attractive working conditions[17], and opportunities for further professional and academic development (UK Government, 2020).

The UK's approach to cyber defence thus champions a "Whole Force concept […] including civilians, armed personnel, reservists and contractors" (King's College London, 2021, p.19). Time will tell of course how successful these strategies become, but on paper they purport to be flexible and creative solutions to the difficult problem of military cyber recruitment. The UK is quite clear in its defence strategy "Defence in a Competitive Age" (Ministry of Defence, 2021c) that cyber is critical to national defence, and it has taken many tangible measures to address the shortages in its cyber defence workforce.

1.5 Canadian Armed Forces

In 2017, the CAF established their Cyber Forces, following the Strong, Secure, Engaged defence policy (Government of Canada, 2017). The CAF nominally grew by 5% to include new roles, including the Cyber Operator. The first batch of eleven Cyber Operators graduated in September 2021 (Government of Canada, 2021b), after undergoing a 60-week foundational cyber analyst course in a civilian third-level institution and 12 weeks in the Canadian Forces School of Communications and Electronics for the military aspects of cyber. The Cyber Operators are recruited exclusively from the CAF and require the equivalent of a Leaving Certificate in

[17] When compared with the civilian cybersecurity sector, except (for the most part) remuneration.

mathematics or computer science. This entry standard of education has been criticised for being too low, especially when compared to other Canadian governmental departments (Alibhai, A., 2022).

The Royal Canadian Corps of Signals (RCCS) has functionally separated its technicians into various roles, including Telecommunication and Information Systems Technicians, Information Systems Technicians, Signal Operators, Signal Technicians, Signals Intelligence Specialists, and more recently Cyber Operators (Canadian Armed Forces, 2022a). Prior to this development, cyber tasks were taken on by elements of the RCCS – analogous to the present situation in the DF and CIS Corps. Concerns exist about the functions of the Cyber Forces and the potential need for assistance from Canada's Communications Security Establishment (Canadian Global Affairs Institute, 2021). Some experts propose retraining officers with relevant education for key cyber-leadership positions instead of investing in small groups of Cyber Operators (Lunn, L., 2021).

The CAF's cyber program implementation has faced many difficulties, including slow procurement processes, personnel development, and delays in security clearances (Government of Canada, 2021a). Furthermore, the Cyber Force is not yet operational, and the RCCS currently takes the lead for training. The CAF has advertised a "Future Entry Plan," intending to accept applications from individuals who have already completed a CAF-endorsed college program in a relevant field (Canadian Armed Forces, 2022b). This may shorten the training period to 12 weeks for those with relevant degrees.

It has been suggested that the CAF "is more than a decade behind its key allies" in the development and integration of cyber (Canadian Global Affairs Institute, 2021), but the concepts above are "robust in theory" (Government of Canada, 2021a) and are suitably derived from defence policy. The CAF is subject to many constraints that are hampering its ability to recruit enough Cyber Operators and of the right standard, but it is quite plausible this will improve over time.

1.6 An Indicative Solution

The British Army and CAF are not unique in their difficulties attracting, recruiting and retaining suitable cyber skills. The trends of growing shortages and increasing pay in civilian-cyber is ubiquitous, and although the dynamic may vary over time, it is likely that there will exist a significant majority who wish to maximise their remuneration by working in the civilian sector. With the usual public-sector constraints placed on the DF and other militaries, flexibility and creative thinking appear to be very important in resolving the most pressing issues in cyber recruitment and retention.

Both the Canadian and UK military generally rely on two strategies of recruitment to strengthen cybersecurity capabilities and build their expertise:

- The direct recruitment of cyber-trained personnel, for which the military needs to recruit civilians who possess relevant cyber skills via direct commission or enlistment, and;
- The development of cyber skills internally via bespoke education and training schemes, for which the military need to identify and retain capable personnel, training them appropriately for cyber roles.

The latter is the case for the DF and cyber. The DF does have limited direct entry mechanisms (Irish Defence Forces, 2022) however these are limited[18] and do not include CIS. Research demonstrates that for the former mechanism, it is important not to be overly prescriptive in terms of required education. While "research suggests that technical backgrounds should be preferred", a useful concurrent strategy is to "also support opportunities for candidates to demonstrate cyber potential in other ways, such as cyber competitions" and rigorous aptitude tests[19], with follow on training as appropriate (Hardison, C.M, et al., 2019, p.65). For example, from 2021, "all existing members of the [UK] armed forces will be offered a cyber aptitude test: those found to have the relevant skills will be offered further training and a career path into a cyber job" (Warrell, H., 2021). The first recommendation is thus to introduce a degree of flexibility in requirements to a potential direct recruitment mechanism, and the selection for a potential 'Advanced Entry' scheme of the current CIS TTS. It is not yet clear however the extent to which such flexibility can apply to the DF case, and further analysis is required.

The second recommendation is that – in considering the risks associated with the de facto merging of CIST and cyber roles – the CIS Corps should recognise the pragmatic advantages of creating separate cyber roles and disadvantages of merging them. Not only does the current situation arguably lead to a poorly defined role overall, but it diverges

[18] Army Motor Technician Fitters, Naval Service Engine Room, Entry Hull and Electrical Artificers as well as Chefs.

[19] The British Army outsource cyber assessment testing to IBM, where assessment is to the same degree as civilian cybersecurity firms (IBM, 2018).

with modern practices, increases training time and cost, and likely increases the probability that these personnel will seek better remuneration outside the military.

Thirdly, and although strictly a retention-based initiative, the British Army's UCM must be acknowledged. Of course, the DF is much smaller in scale, but the concept may have validity. It is a decisive step away from remuneration as the primary focus, emphasising the removal of some obstacles that otherwise encourage some cyber specialists to exit the military. Its application exclusively to cyber roles is evidence of the need for – and utility of – new ways to prioritise cyber-retention. The scale of the CIS Corps is significantly different to its British Army counterpart, however there is enough merit to the initiative that further analysis should be pursued. Moreover, an indirect effect is that the generation of favourable, separate career and promotion prospects for cyber may also promote increased interest from prospective recruits.

The fourth recommendation is that the DF should consider – in line with suitable terms and conditions of service[20] – adjusting the physical standards for some of the cyber workforce. For example, "specific military demands such as physical demands could also be lowered if they are not necessary for the job" (Orye, E. and Faith-Ell, G., 2020, p.14). Inclusive of people with disabilities or otherwise unable to typically serve in the military, the RAND Corporation found that;

> […] the Armed Forces could therefore consider an expanded use of recruitment waivers to enable the organisation to harness diversity, particularly for specialist roles and functions in which the US military are likely to face stiff competition from other employers (including the private sector) for skills (Slapakova, L. et al., 2022).

Finally, the above is a non-exhaustive analysis and puts forward some of the useful concepts derived from the British Army and the CAF, but firmly focused on permanent forces. As civilian cybersecurity grows exponentially, military reservists with cyber skills could be a credible source of skills. The RAND Corporation assessed the cyber power potential of the US Army's reserve and found that most cyber skills required for operations could be acquired from civilians (Porche III, I.R. et al, 2017). The UK's Joint Cyber Reserve Force (British Army, 2022c) and Canada's (Government of Canada, 2017) use of reservists with specialised skills have been successful in utilising civilian-acquired skills. However, Ireland's Reserve Defence Forces face significant recruitment and

[20] For example, cyber technicians and operators that are not required to use weapons or deploy overseas.

retention issues. If addressed, the RDF could serve as a solution to the DF's difficulties with cybersecurity. RDF personnel could provide practical cybersecurity considerations and advise the PDF at operational and strategic levels.

1.7 Conclusion

The unconventional and dynamic nature of the cyber domain is reflected in the variation and difficulties with cyber recruitment across the sample of militaries within this chapter. The dynamic nature of the cyber domain is also reflected in some of the recurring criticisms found in the literature and elsewhere – that most cyber training is never exactly fit for purpose. It is very difficult to keep up with the changing requirements of the roles, as a typical three or four year period of training is quite a long time in the cyber domain. Thus, overly-prescriptive or 'one-size-fits-all' entry and training requirements will necessarily contain gaps, and will likely lag behind modern cybersecurity practices – providing further justification for a the primary finding: a flexible approach, via several parallel mechanisms is the only pragmatic solution.

Military cyber units will essentially always compete with other government agencies and the private sector for talent. For the DF, flexibility in terms of establishment, pay or recruitment may not transpire to a degree comparable to those militaries studied above, but the recently proposed Joint Cyber Defence Command (Commission on the Defence Forces, 2022, iv) is a unique and timely opportunity to implement an *improved* recruitment pathway for cyber technicians and operators. Recent and significant job losses in Ireland's tech sector signal a potential opportunity for the DF, should it wish to seize it (The Irish Times, 2023). Despite difficulties with establishment figures, pay and broader retention difficulties, the DF should take the initiative in cyber and learn from other militaries, particularly with respect to being more flexible in its recruitment of a cyber workforce. Chapter Two will examine in detail the actual training and education of the DF's cyber workforce, generating further recommendations for elevating its cyber capability.

Chapter Two – Training a DF Cyber Workforce

"One of the tests of leadership is the ability to recognize a problem before it becomes an emergency."

- Arnold H. Glasow

2.1 Introduction

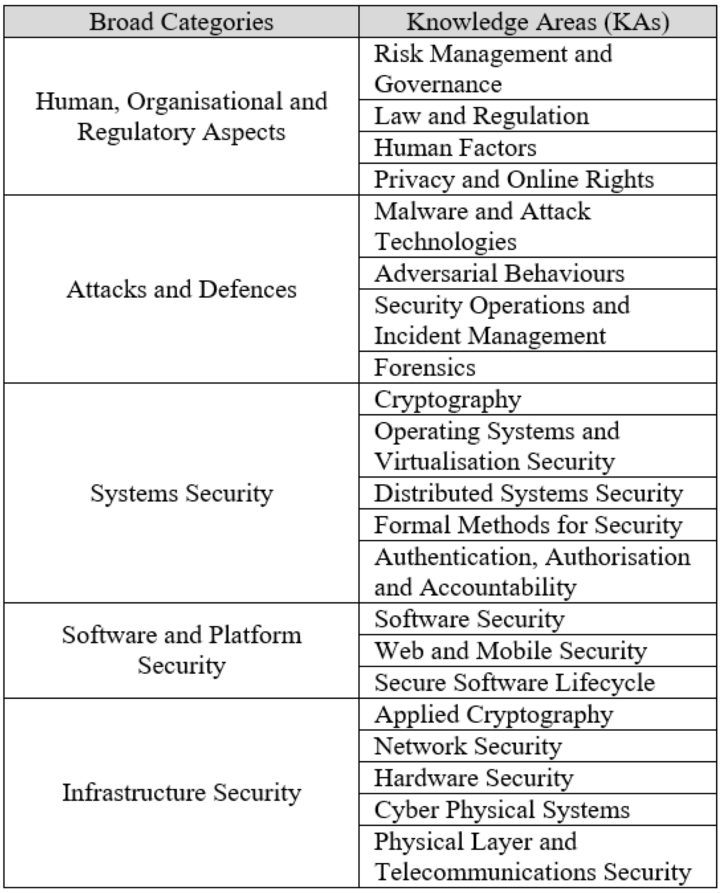
The DF has been charged by Irish Government to "effectively defend Defence Forces' networks from cyber attacks" (Government of Ireland, 2015, p.63) and to "provide support to the CSIRT-IE[21] team […] in any emergency/crisis situation" (Government of Ireland, 2019a, p.22). Thus, the importance of developing technically skilled cyber personnel in the DF is clear and worthy of further research. This chapter will deal exclusively with the cybersecurity training and associated skills of those enlisted DF personnel on the technical-end of the cyber spectrum, eschewing the less technical and management functions of cybersecurity. This is justifiable since the associated training is more complex, evidently difficult to develop and tends to be more visible in the available literature. Furthermore, it serves as a good starting point for further analysis since much of the related cyber training will likely be designed to complement the technical.

One assumption was required at the outset of this research however – that cyber functions and roles would remain the domain of the CIS Corps. It is assumed to be unlikely that the DF will soon separate the functions, as some militaries have, and so cyber technical-training inevitably competes with CIST training and resources. The term 'cyber-technician' is henceforth adopted to delineate between the current CIST, and to encapsulate the expected functions of a cyber-role. The analysis within this chapter inevitably possesses some degree of subjectivity – albeit subject matter expert (SME) qualified, and a detailed mapping framework known as the 'Cyber Security Body of Knowledge' (CyBOK) is employed extensively.

[21] The Computer Security Incident Response Team is an important component of Ireland's National Cyber Security Centre.

2.2 The Cyber Security Body of Knowledge

The CyBOK project is aimed at providing a comprehensive and highly-descriptive guide to the key areas of skills and knowledge required for the contemporary field of cybersecurity. It is an active and iterative project, developed by an international consortium of leading academic institutions, industry experts and professional bodies (CyBOK, 2021a). The CyBOK is comprised of 22 cyber knowledge areas (KAs), grouped into 'broad categories' (see Table 1) that have been classified as fundamental[22], from which skills, training and functions are developed upon.



Broad Categories	Knowledge Areas (KAs)
Human, Organisational and Regulatory Aspects	Risk Management and Governance
	Law and Regulation
	Human Factors
	Privacy and Online Rights
Attacks and Defences	Malware and Attack Technologies
	Adversarial Behaviours
	Security Operations and Incident Management
	Forensics
Systems Security	Cryptography
	Operating Systems and Virtualisation Security
	Distributed Systems Security
	Formal Methods for Security
	Authentication, Authorisation and Accountability
Software and Platform Security	Software Security
	Web and Mobile Security
	Secure Software Lifecycle
Infrastructure Security	Applied Cryptography
	Network Security
	Hardware Security
	Cyber Physical Systems
	Physical Layer and Telecommunications Security

Table 1: *CyBOK Broad Categories and Knowledge Areas (KAs) (CyBOK, 2021b).*

Detailed mapping frameworks are a key CyBOK resource that enable the analysis of education and training programmes, and will be used in Sections 2.4 and 2.5. These 'maps' permit the classification of modules, assessments, research elements and so on in

[22] This thesis will consider 21, since one is "Introduction to CyBOK", and would not be relevant to this analysis.

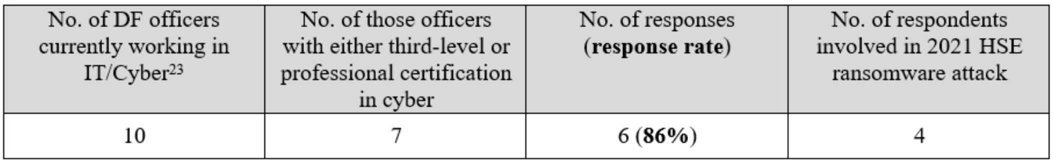
terms of KAs, allowing aggregation and analysis (CyBOK, 2021c). Comparison is the selected methodology of this chapter.

Limitations of the CyBOK include; the rapid rate of change of cyber technologies, processes and threats out-pacing its incremental evolution; a uniquely UK-focus (evident in the span of mostly British-based education analysed online), potentially introducing bias and regional discrepancies; and a distinct focus on technical skills, perhaps playing down important soft skills such as communication, teamwork and leadership. Notwithstanding these limitations, the CyBOK's breadth and depth provide an excellent tool from which a contextually relevant methodology can be employed, provided the findings and recommendations take them into account. Prior to the application of the CyBOK methodology, it is important that pertinent information is obtained to attempt to identify the skills required of a cyber-technician in the DF.

2.3 Identifying the Cyber Skills Required by the Defence Forces

The US military groups its cybersecurity roles – across all domains of war – into "Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC)" (Careers in the Military, 2022). Depending on the source or context, there may be further or alternative subgroups – but the important point here is that COMPUSEC is the primary focus of this chapter. This is the category that broadly aligns with 'civilian cybersecurity' and meets the primary concerns of the DF, since "the most prevalent threats facing [it] include Cyber Exploitation, Data Leakage, Human Factor, Hactivism, Mobile Malware and threats to the Critical National Infrastructure" (Defence Forces, 2013, p.5). Inevitably, some aspects of the other categories will overlap, especially those concerning encryption and human factors. Having established this assumption about DF cybersecurity, comparison with the general literature and practices of civilian cybersecurity broadly is reasonable. Even if this logic was imperfect, and the CIS Corps was tasked with defensive cyber operations say, 'civilian cybersecurity' is sufficiently broad that the findings herein would remain relevant to a sufficient degree.

Nevertheless, more detail should be obtained before further analysis to increase validity. Defining the functions required of potential cyber-technicians is – in the absence of formal guidance or specification – addressed here through a CyBOK-based questionnaire. The questionnaire was sent to seven SMEs in the CIS Corps, requesting their expert opinion on the relative importance of each of the CyBOK KAs. The personnel were selected according to the following criteria; (1) are currently working in the field of IT or cyber in the DF; (2) possess either a third-level degree or professional certification in cyber and; (3) and are commissioned officers – since their role includes the identification of functional and personnel gaps. Of the six respondents, four worked extensively with the HSE during the 2021 ransomware attack (HSE, 2021), providing a unique opportunity to capture well-informed, expert opinions. Table 2 details the statistics associated with this survey.

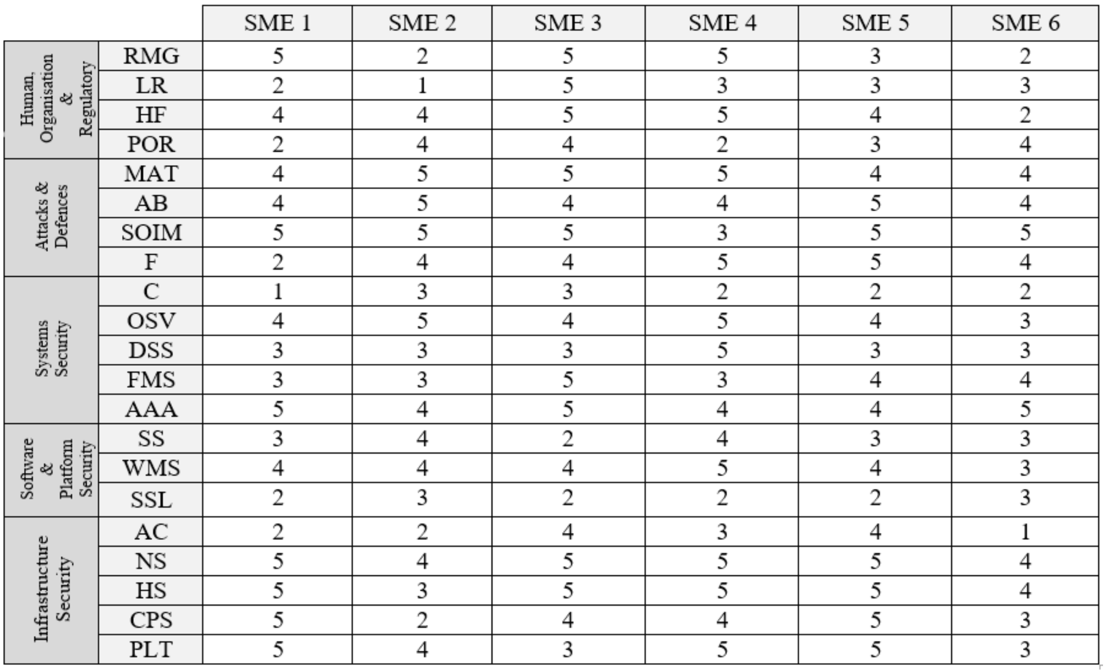


No. of DF officers currently working in IT/Cyber[23]	No. of those officers with either third-level or professional certification in cyber	No. of responses (**response rate**)	No. of respondents involved in 2021 HSE ransomware attack
10	7	6 (**86%**)	4

Table 2: *DF CyBOK-based survey response rates.*

Respondents were asked to rate from 1 (not important) to 5 (very important) each of the CyBOK KAs as they pertain to the actual and expected role of a cyber-technician in the CIS Corps. As a grounded theoretical-approach to dealing with subjective data, the questionnaire's purpose was to quantify those CyBOK broad categories most important to the CIS Corps, and provide a metric against which training could be measured. Labelled anonymously as "SME" 1 through 6, responses are recorded in Table 2. Abbreviations (consistent with the CyBOK) are detailed in Appendix 1. Figure 2 visualises and compares the aggregate of each broad category per SME – i.e. the sum total of the respective KA emphases. It can be concluded that within the broad categories of *Attacks and Defences*, *Software and Platform Security* and *Systems Security* in particular, there is general consensus with respect to their relevance. Within *Human, Organisational and Regulatory Aspects* and *Infrastructure Security*, there is more variance in the responses but it is still clear that the latter is relatively most important overall. Further analysis of these data will follow in the succeeding sections.

[23] As per Defence Forces Regulation (DFR) CS4.



		SME 1	SME 2	SME 3	SME 4	SME 5	SME 6
Human, Organisation & Regulatory	RMG	5	2	5	5	3	2
	LR	2	1	5	3	3	3
	HF	4	4	5	5	4	2
	POR	2	4	4	2	3	4
Attacks & Defences	MAT	4	5	5	5	4	4
	AB	4	5	4	4	5	4
	SOIM	5	5	5	3	5	5
	F	2	4	4	5	5	4
Systems Security	C	1	3	3	2	2	2
	OSV	4	5	4	5	4	3
	DSS	3	3	3	5	3	3
	FMS	3	3	5	3	4	4
	AAA	5	4	5	4	4	5
Software & Platform Security	SS	3	4	2	4	3	3
	WMS	4	4	4	5	4	3
	SSL	2	3	2	2	2	3
Infrastructure Security	AC	2	2	4	3	4	1
	NS	5	4	5	5	5	4
	HS	5	3	5	5	5	4
	CPS	5	2	4	4	5	3
	PLT	5	4	3	5	5	3

Table 3: *CyBOK KA opinion-based ratings of CIS Corps SMEs (1 least important, 5 most important).*

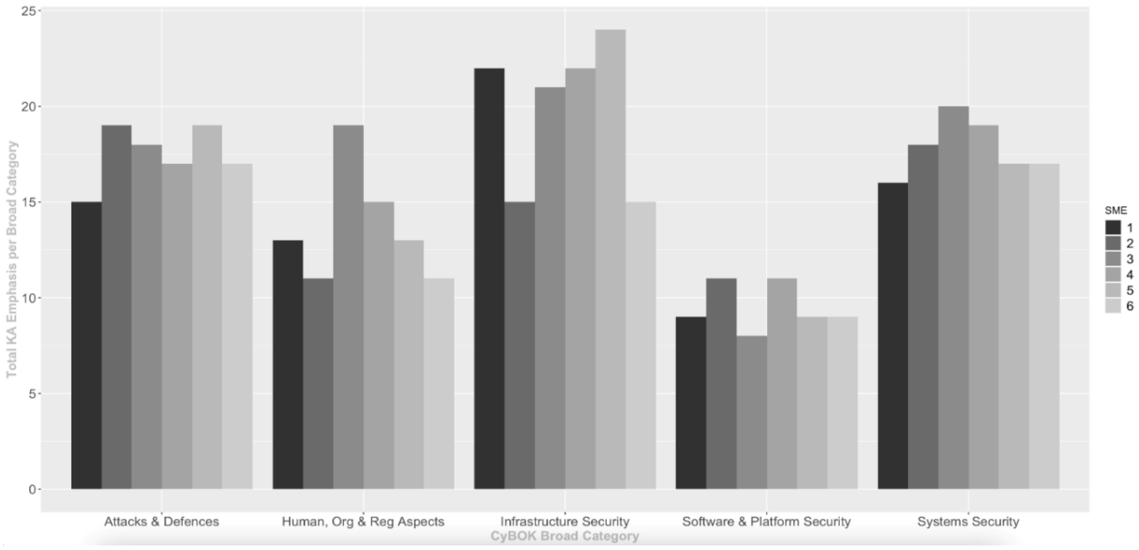


Figure 3: *Comparison of total CyBOK broad category emphasis per SME questionnaire.*

Application of the CyBOK methodology to relevant schemes of training and education – in particular the CIS TT Scheme – is one of the primary research components of this chapter; however a more holistic analysis first requires some qualitative and contextual information. It is useful at this point to compare the CIS TT Scheme with the cyber training identified in Chapter One – namely the British Army and CAF.

2.4 Comparing the CIS TT Scheme with British and Canadian Cyber Training

In Chapter One, the recruitment of cyber-personnel was considered, and the DF case was broadly compared with the British Army and CAF. In this section, the CIS TT Scheme will be compared with its cyber-equivalent[24] in both militaries to further understand the problem, and to qualify any succeeding recommendations. Two metrics will be used in this section to do so – time and CyBOK KAs. These metrics are then used to calculate an analytical heuristic – its so-called *cyber utility* – defined herein as

$$\text{cyber utility} := \frac{(\text{No. of CyBOK KAs})(\text{No. of IT related modules } \times \ 0.5)}{(\text{Total No. of Modules})(\text{Expected duration in years})}$$

A weight of 0.5 was assigned to IT-related, non-cyber specific modules, since these are generally important to cyber[25]. A fair time comparison was deemed possible only from the commencement of functionally-relevant training, disregarding basic training or time previously served for example. A limitation of this analysis is that the information regarding timelines and course duration for non-DF training is confined to online sources – primarily recruitment or institutional websites. In particular, it may be the case that in reality the time between courses and modules vary, so overall estimates have been 'rounded up' to account for such estimation errors. Furthermore, while not strictly correct that KAs be considered as a proportion of modules (a module may contain one or many KAs), the fact that this is a heuristic intended only for relative comparison means it should remain numerically sufficient, although limited to this context.

Assessing the KAs within each module is a source of potential bias, since judgement is required given limited information. To minimise this, analysis was kept at the module-level, rather than learning outcomes (unlike in Section 2.5, where more information was available). Tables 4-6 detail the modules, CyBOK KAs and duration of each respective

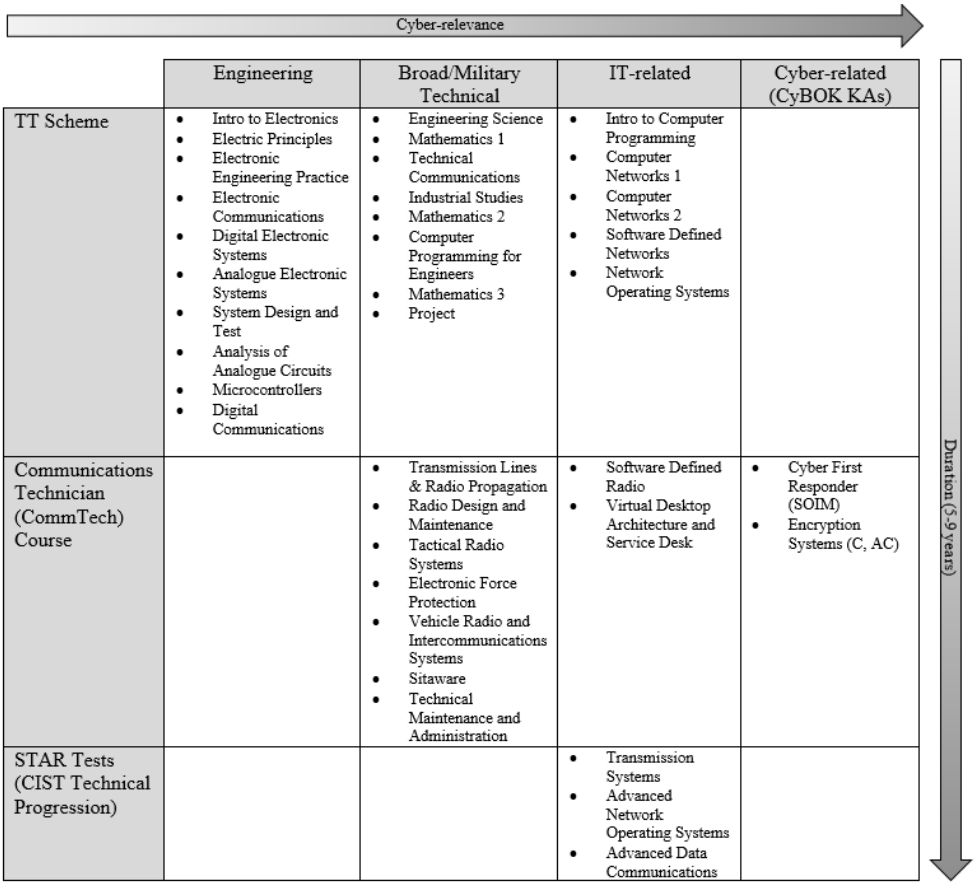
[24] It should be reiterated at this point that although cyber is not one of the formal aims of the CIS TT Scheme, the personnel qualifying from it are increasingly being required to do cyber tasks, and are the de facto cyber workforce of the DF.

[25] The choice of 0.5 is admittedly arbitrary, however as this analysis is concerned with comparison then effectively any value may be entered here.

training scheme. Table 7 calculates the cyber utility of each scheme, enabling comparison. The following subsections detail this process in tabular form.

2.4.1 DF CIS Trainee Technician Scheme

The primary source of information for this analysis was the current, 2021 update of the DF CIS TT Scheme Syllabus of Training (DF CIS Corps Training Syllabus 28, 2011) – the most significant document available in terms of detail.



Cyber-relevance
Duration (5-9 years)

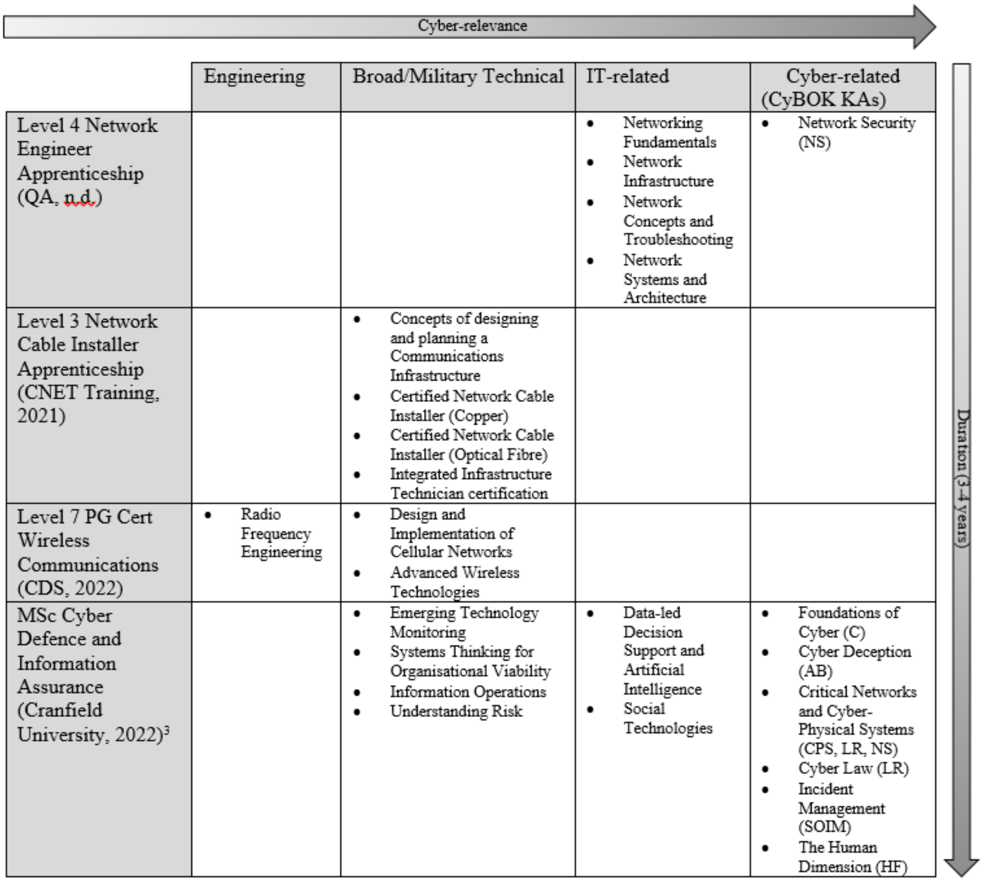
	Engineering	Broad/Military Technical	IT-related	Cyber-related (CyBOK KAs)
TT Scheme	• Intro to Electronics • Electric Principles • Electronic Engineering Practice • Electronic Communications • Digital Electronic Systems • Analogue Electronic Systems • System Design and Test • Analysis of Analogue Circuits • Microcontrollers • Digital Communications	• Engineering Science • Mathematics 1 • Technical Communications • Industrial Studies • Mathematics 2 • Computer Programming for Engineers • Mathematics 3 • Project	• Intro to Computer Programming • Computer Networks 1 • Computer Networks 2 • Software Defined Networks • Network Operating Systems	
Communications Technician (CommTech) Course		• Transmission Lines & Radio Propagation • Radio Design and Maintenance • Tactical Radio Systems • Electronic Force Protection • Vehicle Radio and Intercommunications Systems • Sitaware • Technical Maintenance and Administration	• Software Defined Radio • Virtual Desktop Architecture and Service Desk	• Cyber First Responder (SOIM) • Encryption Systems (C, AC)
STAR Tests (CIST Technical Progression)			• Transmission Systems • Advanced Network Operating Systems • Advanced Data Communications	

Table 4: *Detailed modular and CyBOK breakdown of the CIS TT Scheme (DF CIS Corps Training Syllabus 28, 2011).*

2.4.2 British Army Cyber Engineer

The primary sources for this analysis include the British Army's Cyber Engineer recruitment website (British Army, 2022a) and those sources listed in Table 5. For each course encompassed in the overall scheme, an external supplier of the relevant education or training has been identified, given that the majority takes place outside the military. It should be noted that this path is not necessarily consecutive or correctly time-ordered.

The available sources suggest that this sequence is possible, and thus will be treated as a reasonable estimate of Cyber Engineer training.

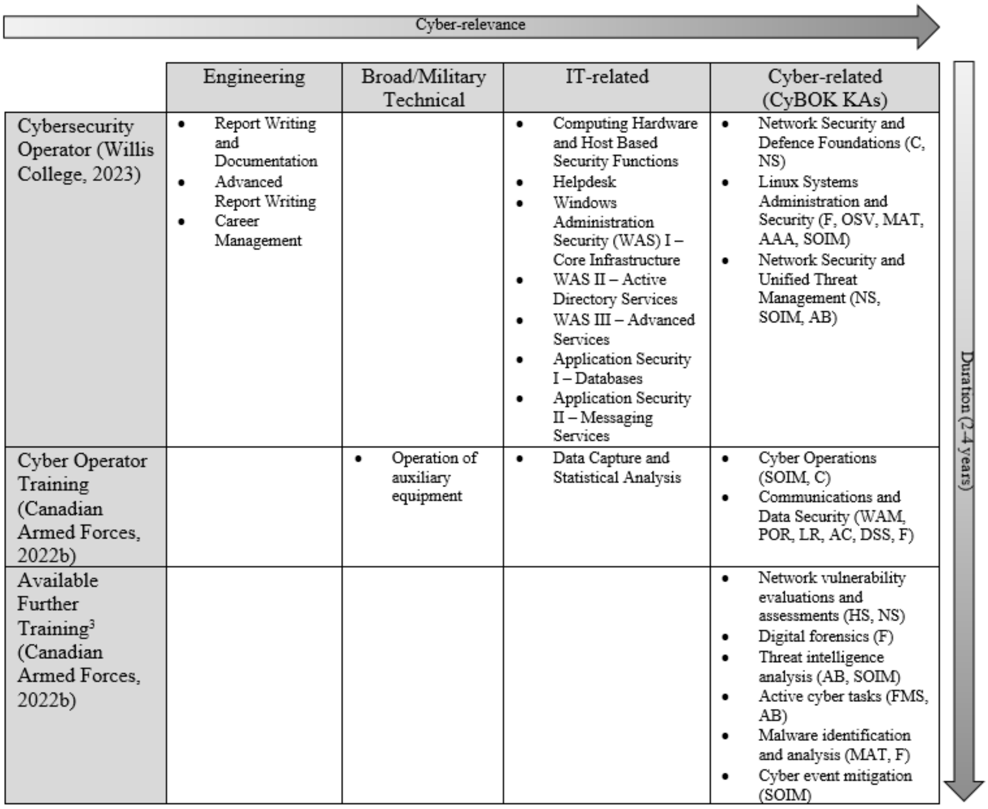

Cyber-relevance
Duration (3-4 years)

	Engineering	Broad/Military Technical	IT-related	Cyber-related (CyBOK KAs)
Level 4 Network Engineer Apprenticeship (QA, n.d.)			• Networking Fundamentals • Network Infrastructure • Network Concepts and Troubleshooting • Network Systems and Architecture	• Network Security (NS)
Level 3 Network Cable Installer Apprenticeship (CNET Training, 2021)		• Concepts of designing and planning a Communications Infrastructure • Certified Network Cable Installer (Copper) • Certified Network Cable Installer (Optical Fibre) • Integrated Infrastructure Technician certification		
Level 7 PG Cert Wireless Communications (CDS, 2022)	• Radio Frequency Engineering	• Design and Implementation of Cellular Networks • Advanced Wireless Technologies		
MSc Cyber Defence and Information Assurance (Cranfield University, 2022)[3]		• Emerging Technology Monitoring • Systems Thinking for Organisational Viability • Information Operations • Understanding Risk	• Data-led Decision Support and Artificial Intelligence • Social Technologies	• Foundations of Cyber (C) • Cyber Deception (AB) • Critical Networks and Cyber-Physical Systems (CPS, LR, NS) • Cyber Law (LR) • Incident Management (SOIM) • The Human Dimension (HF)

***Table 5:** Detailed modular and CyBOK breakdown of the British Army Cyber Engineer programme of training (British Army, 2022a).*

2.4.3 CAF Cyber Operator

The primary sources for the CAF Cyber Operator analysis again were the recruitment website (Canadian Armed Forces, 2022b) and the external education provider’s website. Compared to the British Army Cyber Engineer case, this sequence of training is more certain, although detail is unfortunately somewhat more opaque.


Cyber-relevance
Duration (2-4 years)

	Engineering	Broad/Military Technical	IT-related	Cyber-related (CyBOK KAs)
Cybersecurity Operator (Willis College, 2023)	• Report Writing and Documentation • Advanced Report Writing • Career Management		• Computing Hardware and Host Based Security Functions • Helpdesk • Windows Administration Security (WAS) I – Core Infrastructure • WAS II – Active Directory Services • WAS III – Advanced Services • Application Security I – Databases • Application Security II – Messaging Services	• Network Security and Defence Foundations (C, NS) • Linux Systems Administration and Security (F, OSV, MAT, AAA, SOIM) • Network Security and Unified Threat Management (NS, SOIM, AB)
Cyber Operator Training (Canadian Armed Forces, 2022b)		• Operation of auxiliary equipment	• Data Capture and Statistical Analysis	• Cyber Operations (SOIM, C) • Communications and Data Security (WAM, POR, LR, AC, DSS, F)
Available Further Training[3] (Canadian Armed Forces, 2022b)				• Network vulnerability evaluations and assessments (HS, NS) • Digital forensics (F) • Threat intelligence analysis (AB, SOIM) • Active cyber tasks (FMS, AB) • Malware identification and analysis (MAT, F) • Cyber event mitigation (SOIM)

Table 6: *Detailed modular and CyBOK breakdown of the CAF Cyber Operator programme of training (Canadian Armed Forces, 2022b).*

2.4.4 Cyber Utility

The cyber utility of each training programme in Tables 4-6, and the contributing numerical factors to its calculation, are represented in Table 7.

Training Scheme	Total No. of Modules	No. of IT-related modules	No. of CyBOK KAs identified	Expected (mean) duration (years)	**Cyber Utility**
CIS TT Scheme	37	10	2	7	**0.06**
British Army Cyber Engineer	26	6	9	3.5	**0.86**
CAF Cyber Operator	23	8	28	3	**1.62**

Table 7: *Calculation of cyber utility for CIS TT Scheme and selected cyber training (Scanlon, 2023).*

Considering the time to achieve CyBOK KAs as a function of overall content, the CAF Cyber Operator achieves the most cyber utility, with the British Army's Cyber Engineer at approximately half of that score. The two most significant factors contributing to higher cyber utility is the number of CyBOK KAs addressed during the training and the duration of the training. The CIS TT Scheme scores quite poorly, but this is to be expected – after all its purpose is not to train cyber-technicians. In addition to being a comparative tool, cyber utility could be used to aid the development of new or existing training programmes – a task dependent on a properly defined role.

The role of the British Cyber Engineer includes; (1) to engineer, maintain and repair a range of communications equipment, and; (2) to install, service and repair telecommunications data cable networks, data centres and associated technologies (British Army, 2022b). Given the focus of the MOD's strategy "Defence in a Competitive Age" on rapidly deployable land forces and multi-domain operations requiring centralised data networks in potential overseas environments (Ministry of Defence, 2021c), it is evident that there is a clear link between the stated requirements of a Cyber Engineer and the training delivered.

CAF Cyber Forces are "those military and civilian personnel that force generate, force employ and force develop Cyber Operations, Network Operations and Cyber Mission Assurance" (Government of Canada, 2021a). Focused on the operational level, it is not strictly fair to compare this operator with the British Cyber Engineer. The equivalent role instead may be conducted by the CAF Information Systems Technician, or Signal Operator[26] (Canadian Armed Forces, 2022a). A key lesson then may be discerned in the course of this analysis – there is no one type of cyber engineer or operator. The role, and hence training, depends on operational requirements.

After initial cyber training, most militaries promote some form of postgraduate education, likely to encourage specialisation, promote retention and to maintain relevant cyber-skills in a fast changing domain. The following section will use the CyBOK mapping framework to analyse and compare selected postgraduate courses, providing the basis for a more complete argument.

2.5 CyBOK Analysis of Cyber Postgraduate Education

The CyBOK is not the only comprehensive effort to standardise cybersecurity education and training. Other programmes include the Chartered Institute of Informational Security (CIISec) skills framework (Chartered Institute of Information Security, 2023); the

[26] These are not mutually exclusive roles.

ACM/IEEE/IFIP Joint Task Force guidelines for Cybersecurity Curriculum (CyberEd, 2017); or professional certifications like (ISC)2 Certified Information Systems Security Professional (CISSP) ((ISC)^2 ,2023). However, the CyBOK takes a unique approach by identifying the foundational components of knowledge areas (KAs) that can be used as a basis for different curricular frameworks or programmes to build upon. It also permits analytical measurement cybersecurity course content and the assessment of learning outcomes.

In this section, the broad categories and KAs identified by the CyBOK are applied to the learning and skills outcomes of selected third-level education. This work deviates from the majority of the analysis in the literature, where the analysis of given programmes compared to industry is usually the primary goal; for example Catal, C. et al (2022), Hallett, J. et al (2018) and Mead, N.R. and Tenbergen, B. (2021). In this chapter, some measure of comparison *between* courses is desired, and so a bespoke analysis is proposed and detailed in the following subsection.

2.5.1 The CyBOK Mapping Methodology

Assessing academic or professional programmes via the CyBOK first requires the identification of ‘key words or phrases’ (KWoPs) in either the learning outcomes or content of each of the taught modules[27], or both. The process follows the flowchart in Figure 4 (CyBOK, 2021c) and while tedious, is relatively straightforward. Note that the CyBOK ‘Knowledge Trees’ are not included here diagrammatically due to their significant size and scope, but they are indispensable in actually converting KWoPs to KAs (CyBOK, 2021b).

[27] Research components are not considered, since learning outcomes tend to vary with chosen research project and cannot be controlled for here.

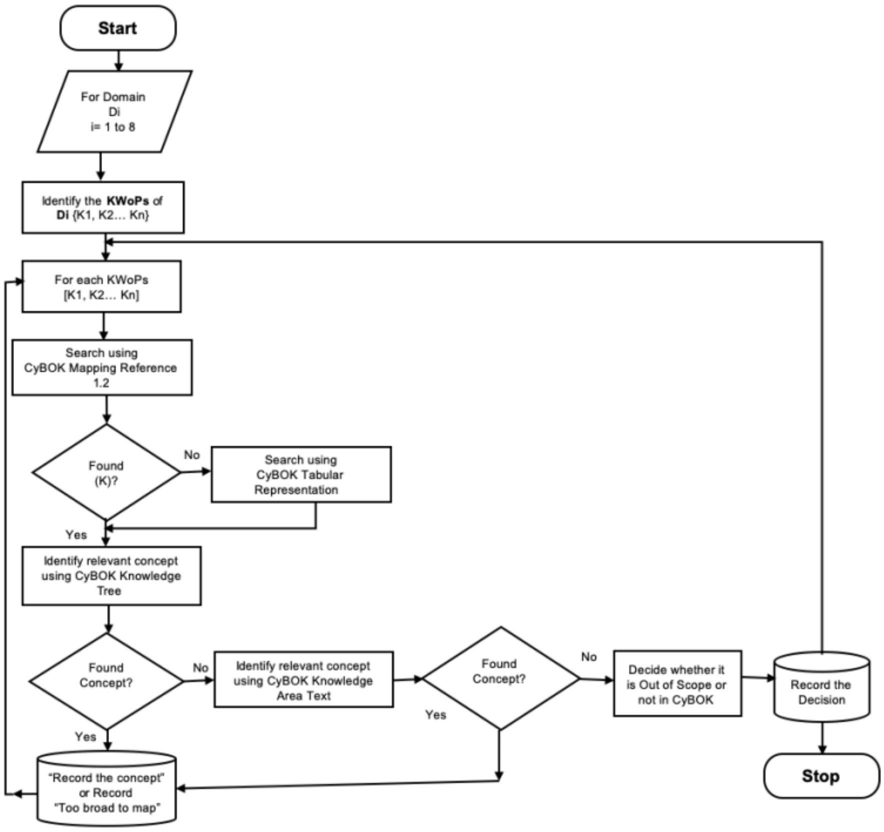


Figure 4: *"How to map concepts in academic and professional programmes to the [CyBOK]" (CyBOK, 2021c, p.7).*

This research diverges from the standard CyBOK methodology in that multiple peer researchers did not perform the KWoP mapping, establish consensus or independently validate mappings (CyBOK, 2021c). The justification for this lies in the exploratory nature and scope of the research. The findings herein though must take such limitations into account, and replication (or otherwise) of results could be followed by closer alignment to the prescribed CyBOK method.

Three postgraduate cybersecurity programmes were mapped. The analytical goal was to compare the overall CyBOK broad category emphasis per programme, with those that CIS Corps SMEs decided were most important in Section 2.3. Ultimately, does the CIS Corps-sponsored MSc in Forensic Computing and Cybercrime Investigation (FCCI) via University College Dublin (UCD, 2022) address the KAs required of a technician working in DF cyber? UCD's MSc in Cybersecurity was also assessed, as was the British Army Cyber Engineer's MSc in Cyber Defence and Information Assurance (CDIA) via Cranfield University – primarily for further comparison, but additionally to demonstrate the utility of the CyBOK's mapping methodology for the CIS Corps. Appendices 1 through 4 detail the mapping and tabularised results for each of the three programmes.

Owing to the multiple ways of counting KAs across learning outcomes, questionnaires and indicative module content, it is necessary to standardise the results in order to permit numerical comparison. The following formula was devised in the course of this research in order to retain the relative significance of each CyBOK broad category. The so-called 'standardised emphasis' $\overline{e_j}$ for each broad knowledge category j is herein defined as

$$\overline{e_j} = \frac{5e_j}{\max[e_j]} = \frac{5}{\max[e_j]}\sum_{i=1}^{n_j} x_{ij}$$

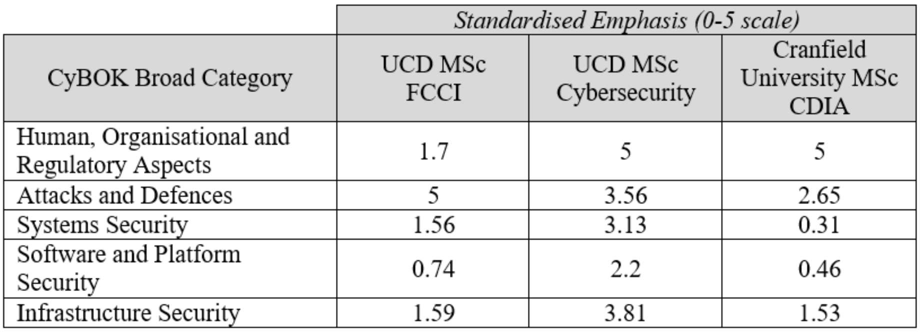
where x_{ij} are the respective scores for each KA, in each broad category, and n_j is the number of KAs in each. This measure therefore permits direct comparison between the SME questionnaire results of Section 2.3 and the CyBOK analysis of different programmes; where a scale of 0-5 has been chosen rather arbitrarily, although analogous to the Likert scale. Although other analyses have used similar quantitative methods for comparison, to the author's knowledge this is the first use of a method of numerical standardisation that retains the relative significance of each broad category. Consider as a comparator, the measure used by Catal, C. et al (2022, p.1818):

$$\text{Importance} \mid \text{Learning Level} = \frac{\text{No. of subjects scoring more than zero}}{\text{Total no. of subjects}}$$

This measure is a function of sum of KAs only, failing to take broad category emphasis into account. Furthermore, a simpler method – the arithmetic average – was ruled out since this (by definition) fails for the same reason. Having established the unit of measure, the CyBOK mapping process may now be outlined in detail.

2.5.2 Results of CyBOK Mapping

The application of the standardised emphasis measure results in a standardised emphasis for each broad category and for each of the three selected postgraduate cyber courses. Table 8 details the numerical results of this computation for each course.



	Standardised Emphasis (0-5 scale)		
CyBOK Broad Category	UCD MSc FCCI	UCD MSc Cybersecurity	Cranfield University MSc CDIA
Human, Organisational and Regulatory Aspects	1.7	5	5
Attacks and Defences	5	3.56	2.65
Systems Security	1.56	3.13	0.31
Software and Platform Security	0.74	2.2	0.46
Infrastructure Security	1.59	3.81	1.53

Table 8: *Standardised emphasis scores per CyBOK broad category, by postgraduate course (Scanlon, 2023).*

2.5.3 Analysis

There were two components to this analysis. The first was a comparison of the standardised broad category emphasis for each of the SME questionnaires, with the CIS Corps-sponsored UCD MSc in FCCI – the de facto cyber postgraduate programme for DF cyber personnel. Of particular interest is the question of whether the MSc is addressing the CyBOK KAs proportionally to the opinions of CIS Corps SMEs. If not, which KAs not being addressed sufficiently? Figure 5 plots each of the SME's standardised broad category emphasis (line plot) against the MSc in FCCI (grey shaded region) as a visual comparison.

It is relatively clear to see that the broad category *Attacks and Defences* is being addressed quite well, relative to SME opinion. This is not surprising given the programme's general emphasis on forensics, malware and adversarial behaviour. However, the categories generally deemed of high importance by SMEs (*Infrastructure Security*, *Systems Security* and *Human, Organisational and Regulatory Aspects*) receive poor coverage. This effectively introduces skills gaps to the DF's cyber defences. Once again, the similarities between the SME's opinions is evident – a good starting point for further identification of the skills required of a DF cyber technician.

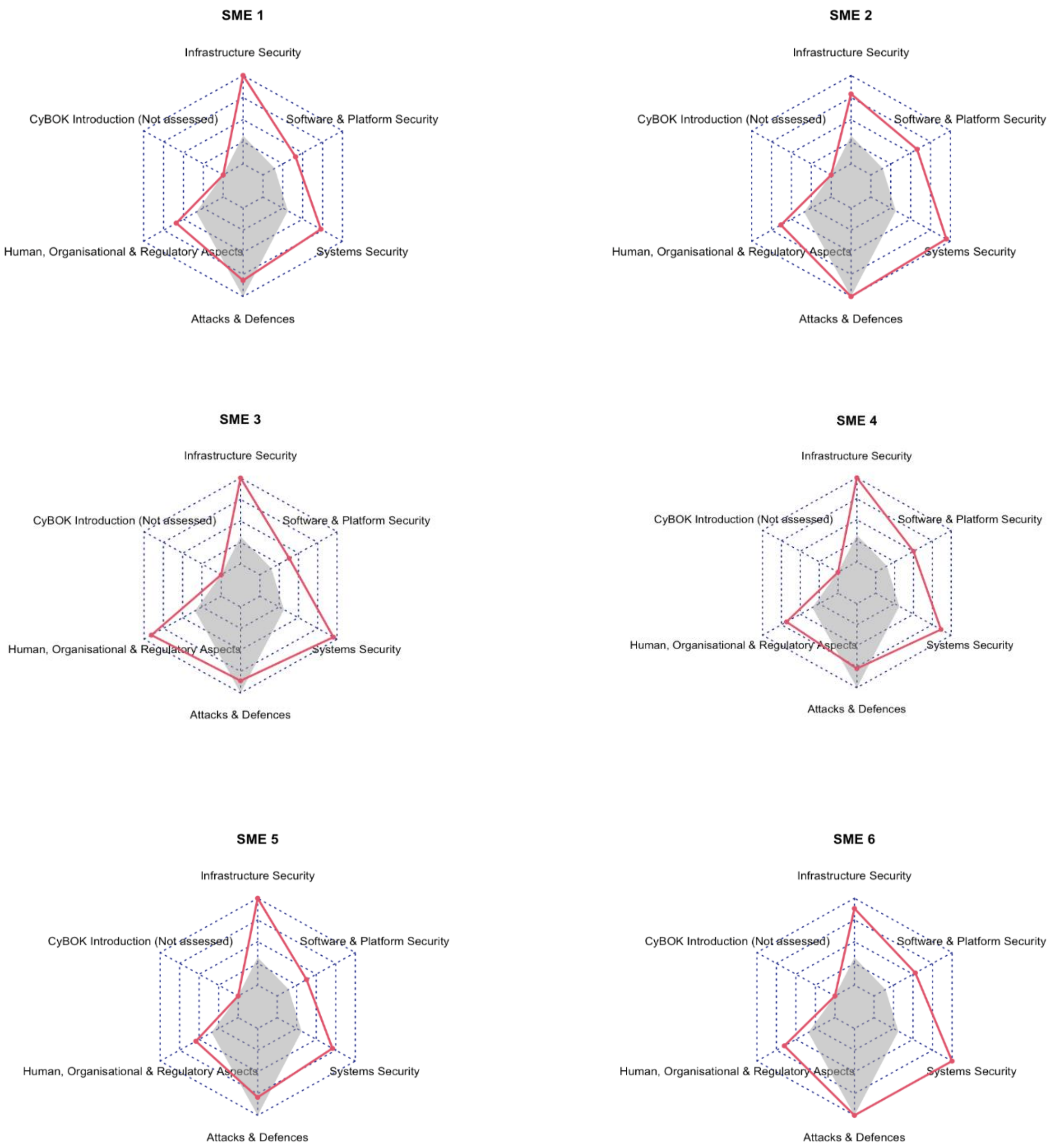


Figure 5: *Mapping and comparing standardised SME CyBOK broad category emphasis (line) with UCD's MSC in FCCI broad category emphasis (grey area) (Scanlon, 2023).*

The second component of this analysis is the comparison of each of the selected postgraduate courses with SME opinion. An average of the six SMEs' quantified opinions relating to CyBOK KAs and broad categories was first calculated using the data in Table 3. This is reasonable since – as seen in Figure 3 – there was somewhat of a consensus in terms of broad categories, although with greater variability within broad categories. The 'averaged SME opinion' could then be plotted and compared directly to the broad category emphasis for each programme calculated with the results from the CyBOK mapping procedure described earlier. Figure 6 plots these results and permits an initial comparison.

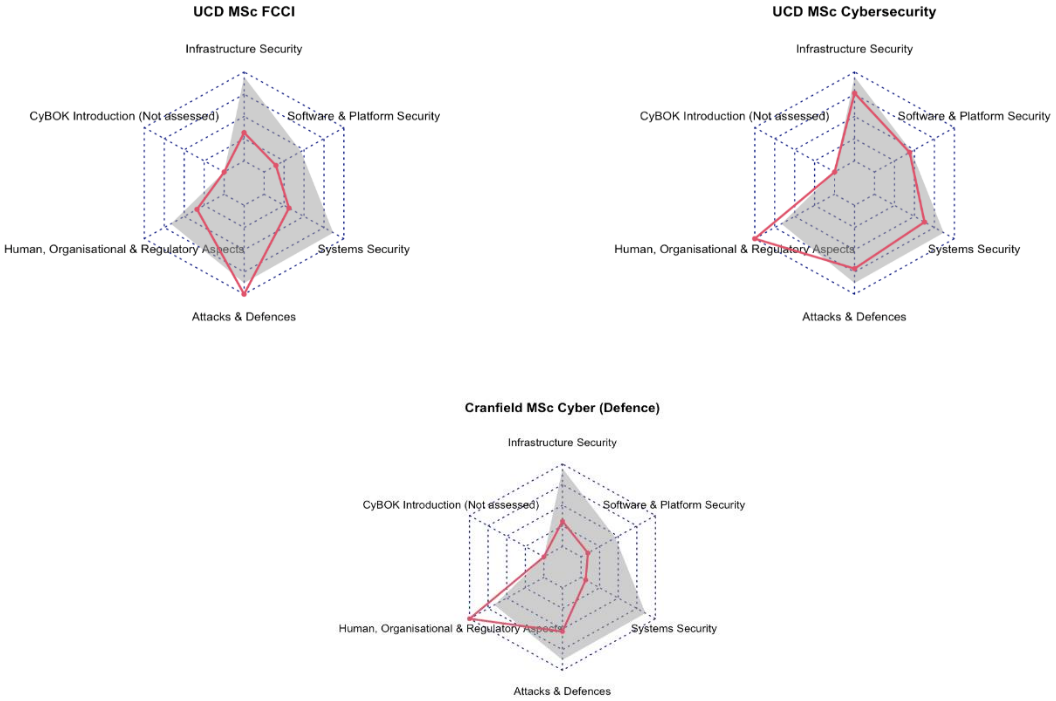


Figure 6: *Mapping and comparing postgraduate cyber education (line) with averaged, standardised SME CyBOK broad category emphasis (grey area) (Scanlon, 2023).*

Within the parameters and definitions discussed above, it is reasonable to suggest again that the UCD MSc in FCCI addresses a narrow proportion of the CIS Corps' requirements well, but not others. The UCD MSc in Cybersecurity appears a more comprehensive fit, offering more in terms of KAs relating to *Infrastructure Security* and *Systems Security* in particular, although perhaps too much in *Human, Organisational and Regulatory Aspects*. Cranfield University's MSc in Cyber Defence and Information Assurance (Defence) evidently prioritises this latter broad category, but is relatively light in terms of most of the other categories. This may be just one possible pathway for a British Army Cyber Engineer; other courses may prioritise different CyBOK broad categories.

This analysis provides a quantitative basis to the finding that current postgraduate cyber training does not meet the requirements of those working in cyber in the DF. Most importantly, applying the CyBOK analysis methodology to other postgraduate courses is a demonstrably useful way to identify those courses that do. An example is UCD's MSc in Cybersecurity, an offering which has here been tentatively shown to be more suitable than the FCCI MSc. The next section will summarise the outcomes of the previous sections and suggest potentially more suitable training pathways for cyber CISTs.

2.6 Potential DF Training Pathways

Recommendations are proposed here within two contexts, following the analysis of Sections 2.4 and 2.5 respectively. First, what training measures can be implemented to improve initial cyber training in the DF CIS Corps? Section 2.4 provided evidence that the cyber utility of the current CIS TT Scheme is significantly lower that both the British Army Cyber Engineer and CAF Cyber Operator schemes, particularly the latter. To increase cyber utility, the most useful adjustment would be to increase the number of CyBOK KAs addressed. However adding more modules to an otherwise well-defined, 5-9 year, non-cyber CIS TT Scheme may compound the original problems, as outlined in Chapter One. The resulting recommendations are that the DF should:

1. Recognise that military cyber operators and engineers are evidently a well-defined class of military capability. Notwithstanding the administrative and organisational difficulties within the DF, an appropriate class of cyber practitioner should be established and trained independent of current CISTs.
2. Define the functions required of DF cyber practitioners. Formally, a new DF cyber strategy could identify this, and the policies of the Directorates of CIS and Training should address the delivery of this capability.
3. Consideration should be given to adopting a model similar to the CAF's Cyber Operator scheme, in particular. Maximising cyber utility is most usefully achieved through increasing CyBOK KAs. Apprenticeship schemes such as 'Fastrack into Information Technology' (Fast Track into IT, 2022) may cover many of the desirable CyBOK KAs, for example. Cyber education does not necessarily need to be several years of undergraduate education, as is evident in both the British and Canadian cases. Similar research in the CAF suggested that gaps in Cyber Operator education could be significantly addressed by "incorporat[ing] industry approved courses/certifications into the foundation qualifications" (Alibhai, A., 2022, p.11).

Secondly, what changes to the postgraduate component of cyber training would reduce the skills gap identified in Section 2.5? In terms of postgraduate or further education and training, the CyBOK mapping methodology provides a good starting point to identify suitable certifications or degrees. Particular recommendations are that the DF should:

1. Consider professional certifications as an effective method of reducing skills gaps. Figure 7 demonstrates, for example, that the Systems Security Certified Practitioner (SSCP) certification is quite tailored to the CIS Corps' current cyber requirements, with a significant relative emphasis on Infrastructure Security and Systems Security.
2. Examine the feasibility of expanding postgraduate education to a wider array of suitable courses, most notably UCD's MSc in Cybersecurity. There are many offerings within Ireland's third level institutions, and an over-reliance on any one is evidently problematic.

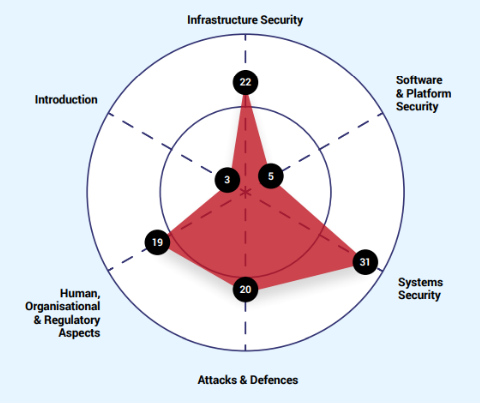


Figure 7: *CyBOK mapping of SSCP (ISC)2 certification (CyBOK, 2022, p.5).*

2.7 Conclusion

This chapter sought to identify the skills required of those DF personnel working in cyber, and propose improved training pathways to minimise the most significant skills gaps. Two research elements were thus introduced. The first was a CIS Corps cyber-SME questionnaire, relying on expert opinion in the context of the CyBOK KAs. The result of this analysis showed a general consensus in terms of broad categories, with some variance at the KA-level, and provided the metric from which training could be compared: a novel numerical standardisation that encodes the relative significance of each CyBOK broad category, known herein as the *standardised broad category emphasis*. The second element was the CyBOK mapping of three relevant military programmes; (1) the CIS TT Scheme, (2) British Army Cyber Engineer training and (3) CAF Cyber Operator training; followed by the CyBOK mapping of selected postgraduate courses.

The overall finding of this chapter was that the DF's cyber personnel are not appropriately trained for their roles – which are in turn poorly defined – however there exist practical ways to address this situation. Both the British and Canadian cases offer some useful insight, and maximising the cyber utility of the next generation of cyber training programmes is a reasonable metric. Further research could consider a more detailed examination of cyber-requirements in the DF, coupled with a broader examination of available training options. The CyBOK methodology is sufficiently rigorous and suited to this problem, however a separate analysis is recommended for both completeness and to further minimise any intrinsic biases in these findings.

Finally, it is recognised that KA coverage is just one measure of cyber training and that other factors must be considered, such as educator and institutional expertise, quality of assessment, student participation and so on. While these findings addressed mostly technical cyber subject matter, Chapter Three will examine another important component of a military's cyber capability – general cyber knowledge with respect to Professional Military Education (PME).

Chapter Three – Cyber PME in the Defence Forces

“*The great aim of education is not knowledge, but action*”

- Herbert Spencer

3.1 Introduction

To what extent should cyber education be integrated into Professional Military Education (PME) in the DF, in line with other militaries? The literature review revealed a substantial body of literature describing a clear requirement for structured and meaningful cyber PME for non-technical military leaders – those officers in general command, operations or planning roles in any service, corps or formation. The growing consensus that “[c]yber power is critically important in joint warfare” (Bonner, E.L., 2014) pushes today’s militaries to generally train more of their leaders in cyber, and requires its integration into joint operations planning and execution.

This chapter will make the case that an increased significance on cyber does not only require those with technical skills (as in the preceding chapters) but cyber-competent leadership too. Military leadership in general must consider cyber organically; an integrated domain as ubiquitous as the land, sea, air and space domains. It is not a task just issued to technicians. Despite notable efforts to increase *awareness*, there are significant gaps between how the DF’s leaders are meaningfully educated in cyber, relative to their peers elsewhere. The most salient and apparent case in the literature is the US Armed Forces, primarily since it is a world leader in cyber. Hence most of the analysis herein is based on the US Armed Forces, so inferences will be scaled down usefully through grounded reasoning to a magnitude and scope more suitable to the DF. The next section will assess military cyber operations from the perspective of PME, ultimately establishing the context for recommendations at the end of this chapter.

3.2 Military Cyber Operations

This section aims to justify the need for non-technical cyber PME, i.e. cyber without using Information and Communication Technology (ICT). Figure 8 illustrates where cyber defence sits within the context of national defence, information security and cyber security. The latter is treated in Chapter 2, but a more complete DF cyber capability thus requires organisational competence in the cyber components of information security and national defence in addition. While the literature emphasises the significance of non-technical cyber PME at all levels, the primary focus of this chapter will be on the operational level owing to research constraints, but with suitable references to the tactical and strategic levels throughout. Rather than attempting to summarise or analyse the growing breadth of cyber considerations at each level, this section will concentrate just on distilling some of the fundamentals that ultimately should be taught to officers as they progress through their PME.

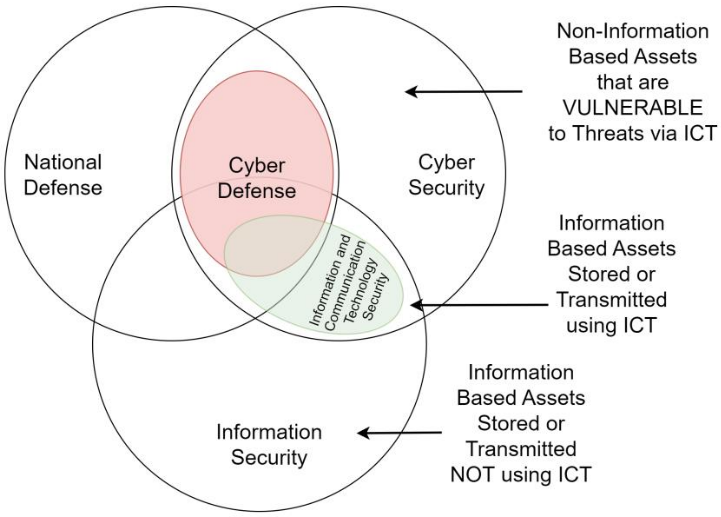

National Defense
Cyber Defense
Cyber Security
Information and Communication Technology Security
Information Security
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Based Assets Stored or Transmitted using ICT
Information Based Assets Stored or Transmitted NOT using ICT

Figure 8: *The relationship between information security, cyber security, and national defence (Lee, S. and Kim, S., 2021, p.4).*

Cyber now forms a critical component of many militaries' strategies and doctrines, as is evidenced by the relatively recent formation of major cyber units and commands[28]. There are some important distinctions between the cyber and 'traditional' domains of warfare that general officers must be familiar with. One key and immediate distinction between cyber and those traditional land, sea, maritime and space domains is that lines are blurred between military and civilian. Once connected to the internet, military operations using cyber-means must pay close attention to the consequences and implications of the presence of civilian actors. Modern military operations insist that cyber must be

[28] For example, the US Cyber Command (USA), Cyber and Information Domain Command (Germany), C4I and Cyber Defense Directorate (Israel), Cyber Defense (Norway).

integrated out of sheer necessity into planning, employing or mitigating those operational effects and actions that overlap with the newest domain of warfare.

The cyber domain poses challenges and opportunities for military planning and operations. Cyber specialists handle the deployment and conduct of cyber operations, but it is military leaders and planners who are responsible for integrating effects and achieving synchronisation across domains. Coherently integrating the cyber domain will have the "additional benefit of informing the greater operational community as war fighters in the land, maritime, and air domains continue to become increasingly dependent upon cyberspace" (Babcock, C., 2015). Even though it is not a 'warfighting force', the DF still stands to gain within its own sphere of cybersecurity.

Identifying the components of cyber-PME required a systematic review of the available literature. While general awareness of cyber and its strategic and operational implications are certainly important, the literature review revealed some practical and necessary considerations required on the part of the joint planner. Consider the following illustrative points taken from the United States Army War College's Strategic Cyberspace Operations Guide (Leitzel, B. and Hillebrand, G., 2022, p.32), highlighting the uniqueness of planning military operations in cyberspace:

1. Cyberspace operations (CO) likely require more branch and sequel planning, since the higher-order effects of cyber actions and events are notoriously more difficult to predict than in the physical domains;
2. Although one aspect of cyberspace can be mapped onto the physical layer of the battlespace – i.e. the command and control structures, the transmission media or even the technologies – there are the cyber-critical logical network and cyber-persona layers to be considered. An adversary network's topology[29] or the profiles of system users and administrators should be familiar concepts to operational planners in contemporary conflicts;
3. In terms of defence, "planners require a clear understanding of which friendly forces or capabilities might be targeted by an adversary". This is a fundamentally complex issue, since an adversary may seek to achieve effects in or through cyberspace.

[29] The *arrangement* of nodes and connections in a network, a component of adversary analysis that is typically unfamiliar to 'traditional' operations planning.

The Strategic Cyberspace Operations Guide effectively recommends a separate concurrent and integrated CO analysis and planning process. Planning for CO is sufficiently different to the physical domains of air, land, sea and space that many of the ‘products’ of joint planning are replicated specifically for cyber considerations, including a unique cyberspace mission analysis, a continuously updated “CO scheme including objectives and effects” and its own annexes in Operational Orders – for example. Many important details have been omitted here, however the main assertion is that the US Armed Forces are leading the way in terms of comprehensive integration of CO into the joint planning process, and its Strategic Cyberspace Operations Guide is an excellent reference for how the DF should consider integrating its own cyberspace concerns into joint operations planning. Cyberspace has been elevated to ubiquity, and plans must follow.

While the scale of DF cyber activities will remain significantly less – in terms of both capability and intent – to those of the US, cooperation with other nations through NATO PfP, EU Battle Groups, overseas deployments and so on will increasingly require cyber-ready capabilities and planning processes. Of direct importance to this chapter are those elements of knowledge, experience and leadership in the cyber domain that the DF requires to do so. The next section will examine the literature from the perspective of generally non-technical cyber-PME, with a focus on the particular benefits derived.

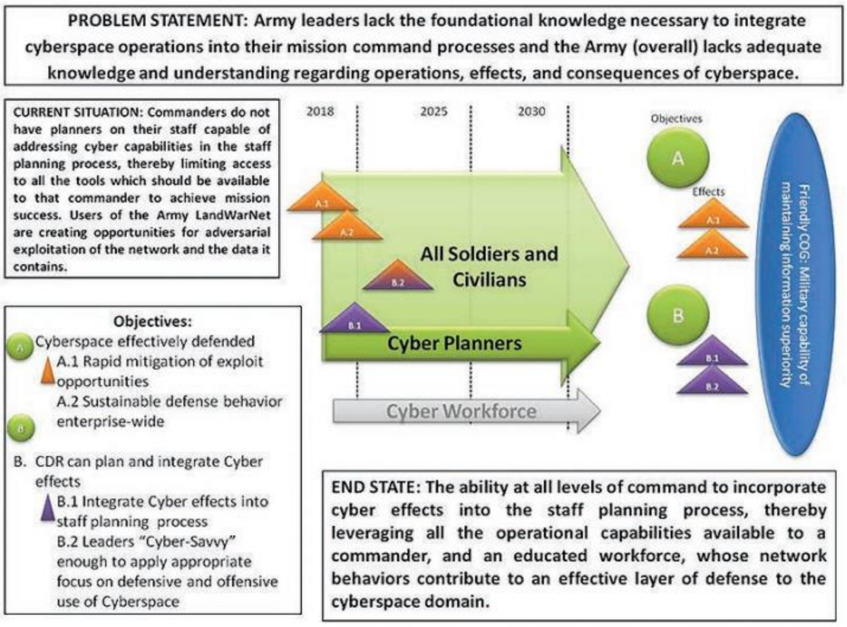
3.3 Non-technical Military Cyber Education

While the US Armed Forces puts significant resources, research and effort into developing the elements of a leading technical cyber workforce, it is also evidently a champion of general cyber training. An illustrative and simple example of this is the ‘Cyber Awareness Challenge’, a unique initiative of the US Armed Forces that *all* enlisted and commissioned ranks must complete each year (Information and Communication Technologies Defense Division, n.d.). Although limited in scope and open to fair criticism[30], it is nevertheless a reasonable and demonstrably achievable – being a requirement across all services since at least 2016 (US Marine Corps, 2016).

A broad emphasis on cyber training for US Armed Forces commanders and planners is quite apparent in the literature. Consider first the succinct summary of R. L. Collins (2014), who first highlights the US Army Cyber Center of Excellence’s mission to

[30] The primary criticisms include that it is too short, easy to cheat and is not very challenging.

integrate "cyber LDE&T[31] into Army PME to increase Army-wide knowledge of cyberspace and commander's ability to integrate into the unit's operations" (Collins, R. L., 2014, p.15). He then details some of the specific courses that are designed to achieve this, and reiterates military cyber-functions based on role and experience. Borrowing from operational design concepts, Collins further illustrates a conceptual 'operation' where the end state is the complete integration of cyber into the staff planning process – see Figure 9.



PROBLEM STATEMENT: Army leaders lack the foundational knowledge necessary to integrate cyberspace operations into their mission command processes and the Army (overall) lacks adequate knowledge and understanding regarding operations, effects, and consequences of cyberspace.

CURRENT SITUATION: Commanders do not have planners on their staff capable of addressing cyber capabilities in the staff planning process, thereby limiting access to all the tools which should be available to that commander to achieve mission success. Users of the Army LandWarNet are creating opportunities for adversarial exploitation of the network and the data it contains.

Objectives:

A Cyberspace effectively defended

A.1 Rapid mitigation of exploit opportunities

A.2 Sustainable defense behavior enterprise-wide

B. CDR can plan and integrate Cyber effects

B.1 Integrate Cyber effects into staff planning process

B.2 Leaders "Cyber-Savvy" enough to apply appropriate focus on defensive and offensive use of Cyberspace

END STATE: The ability at all levels of command to incorporate cyber effects into the staff planning process, thereby leveraging all the operational capabilities available to a commander, and an educated workforce, whose network behaviors contribute to an effective layer of defense to the cyberspace domain.

2018
2025
2030
A.1
A.2
B.2
B.1
All Soldiers and Civilians
Cyber Planners
Cyber Workforce
Objectives
A
Effects
A.1
A.2
B
B.1
B.2
Friendly COG: Military capability of maintaining information superiority
B

Figure 9: *A conceptual operation design to integrate general cyber training to PME in the US Armed Forces (Collins, R. L., 2014, p.15).*

Although published nine years ago, the summary in Collins' article broadly reflects the current state of so-called cyber LDE&T in the US Army as evidenced in US Army Regulation 350-1 – Army Training and Leader Development – which prescribes the sequencing and high-level content of leadership training in the US Army (US Army, 2017). At the Brigade level, the regulation outlines that electronic warfare and cyber be taught as part of "Branch-specific Command Preparation Program" in conjunction with other, 'more traditional' functions of leadership.

[31] Leaders Development, Education, and Training

Importantly, Collins suggests that US Army Regulation 350-1 will be successful[32] when; (1) all soldiers and civilians understand and mitigate the cyberspace threat; (2) Army leaders at all levels understand effects and consequences of use; (3) Army staffs fully understand and have the ability to plan for the full spectrum use of all cyberspace capabilities within the MDMP; and (4) Commanders "have a baseline understanding of their unit's cyber-related vulnerabilities and are able to integrate cyberspace operations […] to achieve effective cyber-related effects on the enemy". Heatherly, J. C. and Melendez, I. (2019, p.70) further propose that all soldiers must be continually educated on cyber threats throughout their careers to achieve this, including multifaceted instruction on the improper use of technology, cyberattacks during military operations, and security classification regulations.

A workshop led by the Cyberspace Operations Group of the Center for Strategic Leadership, U.S. Army War College, was conducted in 2011. Senior leaders and academics across a wide range of relevant institutions (including from within the US DoD) were involved, with the study contributing towards a contemporary understanding of the implications of the cyber domain for general military officers. Of particular relevance is the opening assertion that "senior military leaders need to consider cyberspace issues in Commanders Critical Information Requirements (CCIRs) as they can significantly impact the effectiveness of military organizations" (Waddell, W. et al, 2011, p.3). Despite the many significant advances in military cyberspace since publication – including the creation of the joint US Cyber Command and the service cyber components it comprises[33] – the recommendations appear equally applicable 12 years later. The study's recommendations in terms of PME were:

1. "Emphasize cyberspace in the context of traditional military theory, planning, and operations, that is, as an integral part of the profession of arms.
2. Better integration among existing cyberspace centers of excellence (such as the Air Force Institute of Technology, Naval Postgraduate School, National Defense University, etc). Consider the development of a standing working group on cyberspace.

[32] Strictly speaking, Collins was addressing the 2013 version of US Army Regulation 350-1. However, there were insignificant changes in the 2017 in terms of cyber, and his point stands.

[33] US Army Cyber Command, Marine Corps Cyberspace Command, US Fleet Cyber Command, Air Force Cyber and US Space Force

3. Emphasise the role of senior and strategic leaders as potential advisors with respect to cyberspace events (as opposed to tactical practitioners)" (Waddell, W. et al, 2011, p.21-22).

These are actionable recommendations that can be translated into content for PME, and will be referred to in the recommendations for the DF later in the chapter. More recently, Rodriguez, A. (2022) – a retired Signals Corps lieutenant colonel and senior cyber analyst for the US Marine Corps – called for senior-level PME to achieve five objectives, ensuring that senior military leadership can: (1) evaluate the impact of cyberspace operations on the national security environment; (2) integrate joint doctrine perspectives into cyberspace operations and strategy; (3) analyse cyberspace operations, technologies and policies in the context of DoD activities; (4) evaluate and mitigate potential vulnerabilities threatening joint operations; and finally (5) "apply principles of strategic leadership, decision-making, and ethical conduct to cyber capability employment" (Rodriguez, A., 2022). Although the author stops short of detailing how such a curricula would be written and delivered, his primary assertion is that military PME is behind its civilian analogue in terms of national defence, a situation in which Ireland too finds itself. The objectives listed by Rodriguez, A. (2022) above are firm starting points for potential learning outcomes for PME in the DF.

Prior to making any recommendations for the DF, the next section will give an overview of the cyber PME in the US Armed Forces so that a comparison may then be drawn – albeit appropriately scaled and contextualised.

3.4 Cyber PME in the US Armed Forces

The current military instruction on officer PME in the US Armed Forces is the Officer Professional Military Education Policy (Joint Chiefs of Staff, 2020). It places a particular emphasis on Joint PME (JPME) and prescribes the objectives for all accredited PME education in the US Armed Forces, nominating entities responsible for component-level and thematic education. The cyber component of US Armed Forces JPME is the responsibility of the College of Information and Cyberspace, part of the broader US National Defense University (NDU). In terms of general cyber PME, as evident in the Officer Professional Military Education Policy, cadet training and the Command and General Staff Course (CGSC) are where the main effort evidently lies.

The US Military Academy (USMA) Cadets of West Point are offered a wide array of academic electives and majors in both technical and non-technical studies in their formal education, spanning the arts, history, sciences, law and information technology, including cyber (US Military Academy, n.d. a). During the ‘summer military training’ periods, all USMA cadets – regardless of degree choice – study the cyber domain (US Military Academy, n.d. b). Most significant however is the deliberate culture and environment that pervades West Point, and “facilitates cadets’ growth into professionals and leaders who possess the character and competence required to succeed in and adapt to the Cyber Domain and Multi-Domain Battle” (Hall, A. and Sobiesk, E., 2017, p.5). This environment comprises optional activities such as cyber clubs, conferences, internships, work experience with US Army Cyber units and even competitions. For particularly interested cadets, the Cyber Leader Development Program (CLDP) of the US Army permits them to “pursue opportunities to attend advanced cyber training”, potentially leading to advanced cyber career paths (Hall, A. and Sobiesk, E., 2017, p.6). This culture reflects the strong, cyber-centric language of US Military strategies and doctrines.

On the other end of the PME spectrum is the US Army’s equivalent of the DF’s Joint Command and Staff Course (JCSC); the CGSC. As with the JCSC, the CGSC is also accredited at postgraduate level[34]. The US Army Command and General Staff College’s catalogue of courses “Cyberspace Operations” as one of the 14 topics within the 41-hour “Unified Action” block of instruction, focussing on “the conditions or effects provided by the capabilities of the joint services and unified action partners” (US Army Command and General Staff College, 2020, p.7-6). Outside of the CGSC, the US Armed Forces integrates general cyber competence in two ways; by requiring general leaders to be familiar and competent, and through the availability of professional development courses.

Such short courses are frequently conducted from Fort Leavenworth for the general purpose of preparing officers and NCOs for their next appointment. Two such courses stand out in terms of professional development in terms of cyber, namely the Brigade Command Tactical Commanders Development Course (BCTCDC) and Brigade Functional Command Development Course (BFCDC). The former cites understanding how a Brigade employs “cyber warfighting” (U.S. Army Command and General Staff College, 2020, p.10-8), while the latter emphasises the graduating student’s “ability to

[34] Master of Military Art and Science, or Masters in Operational Studies; it depends on the student’s existing enrolments or professional goals.

leverage the Cyber and Space domains in LSCO[35]" (U.S. Army Command and General Staff College, 2020, p.10-9). Most leaders in the US Armed Forces appear to be required to spend at least some time studying and practicing the employment of cyber, notwithstanding the various assertions in the literature calling for (much) more. The next section will compare the DF with the preceding examples, and infer reasonable recommendations.

3.5 Recommendations for the DF

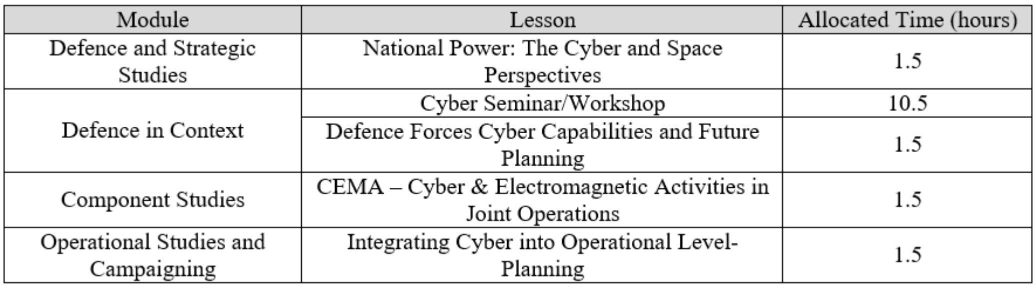
Spidalieri, F. and McArdle, J. (2016, p.143) claimed that "the next generation of military leaders must also be cyber-strategic leaders", since the domain has become ubiquitous at the strategic level. Although US-centric and writing in the context of its US Military institutions and services, the authors' analysis should retain relevance for the DF. Since the stated high-level training objective of the DF's JCSC includes "incorporating relevant academic, critical thinking, operational-level, defence management and leadership skills, in order to prepare officers for command and higher defence management roles, nationally and internationally" (Defence Forces, 2022, p.6), it is clear that the development of Spidalieri and McArdle's cyber-strategic leaders is an implied and necessary task for the DF.

An examination of the most operationally-oriented PME courses in the DF permits comparison with some of the salient principles emerging from the assessed literature. Considering first DF's Land Command and Staff Course (LCSC), which aims to "equip officers to hold a Commandant's command and to acquire a knowledge of handling commands normally allotted to a Lieutenant Colonel" (Defence Forces, 2019, p.3). Although this career course is aimed at the land component, it includes a small block of instruction on 'joint studies', with one hour dedicated to "Introduction to Cyber Defence at the Strategic Level" (Defence Forces, 2019a, p.20).

The DF's JCSC – the exemplar of operational and strategic level PME in the DF – is aimed at training officers of all services to "command formations of all components of the Defence Forces; and to perform the higher staff work involved in the handling of such

[35] Large-Scale Combat Operations (LSCO).

formations" (Defence Forces, 2022, p.6) – including cyber[36]. The learning outcomes and details relating to cyber education on the JCSC are presented in Table 9.



Module	Lesson	Allocated Time (hours)
Defence and Strategic Studies	National Power: The Cyber and Space Perspectives	1.5
Defence in Context	Cyber Seminar/Workshop	10.5
	Defence Forces Cyber Capabilities and Future Planning	1.5
Component Studies	CEMA – Cyber & Electromagnetic Activities in Joint Operations	1.5
Operational Studies and Campaigning	Integrating Cyber into Operational Level-Planning	1.5

Table 9: *Cyber-related education on the DF JCSC (Defence Forces, 2022).*

The US CGSC (US Army Command and General Staff College, 2020) – includes "a two-hour block on cyberspace with additional cyber instruction as part of the lessons on Command and Control and Fires Integration" and "includes some cyber play in the various student war game exercises conducted at the end of each major block of instruction" (Heatherly, J. C. and Melendez, I., 2019, p.69). Additionally, student officers have the choice of taking a cyber-elective. It is difficult to draw a direct comparison between both courses, however it does appear that the DF JCSC has developed a suitable approach to cyber at the joint operational level. The idea of "cyber play" at the end of each major block of instruction is worthy of further investigation, pending the identification of learning outcomes linked to DF cyber doctrine. As asserted in previous chapters, a more prescriptive DF cyber strategy too would help further align the JCSC with the functions ultimately required of senior DF officers.

Given that the standard cadet training syllabus (Defence Forces, 2019b) contains no cyber-related education whatsoever, a one-hour lecture on cyber defence at the strategic level[37] on the LCSC is the total education a typical DF officer formally receives prior to the JCSC, approximately 20 years into their military service. Comparison to the USMA in West Point, detailed in the previous section, creates a significant contrast in this respect. The effective lack of any cyber-related PME in the DF prior to the JCSC is dramatically

[36] Recall however that Chapter Two assessed the DF's cyber strategy as effectively oriented on cybersecurity only, rather than military cyber offence or defence.

[37] Notwithstanding the very limited time made available to cyber, the operational level would be more appropriate to this particular course.

out of step with the emerging consensus in the literature and – most importantly – generates a significant vulnerability for the DF in the cyber domain, offering adversaries or malicious actors a position of relative advantage.

To address this gap, the DF should follow the recommendations of the previous section and integrate cyber training for all officers at the appropriate levels. A desirable end state may replicate that of Collins (referenced in Figure 7); the ability for all levels of command "to incorporate cyber effects into the staff planning process" and leverage all the operational cyber capabilities available to a commander (Collins, 2014, p.15). In addition to this decidedly operations-focused end state, all leaders should be competent to enforce "proper communication procedures and cyber OPSEC in all aspects of a unit's daily duties whether in garrison or in the field" (Heatherly, J. C. and Melendez, I., 2019, p.71) – this is not just a task for CIS personnel.

Tikk-Ringas, E., Kerttunen, M. and Spirito, C. (2014) recommend that at cadet and corps level, the cyber "focus is on hands-on, in-depth technical and tactical skills" that teach students "how these [cyber] capabilities have been or can be used in the core functions of military operations such as command and control, intelligence, maneuver, interdiction, targeting and fire, logistics, and sustainment". At the joint and senior levels of PME, the authors recommend developing in the students an "understanding of concepts, knowledge of the use of cyber capabilities in military operations, and the ability to design and define strategies, policies, and future capabilities". It is clear from Table 8 that the JCSC has established a relatively strong foundation to achieve this, however the earlier courses of a DF officer's PME are significantly lacking.

Further recommendations can be distilled from Waddell, W. et al's second and third recommendations (2011, p.21-22); in that the DF should "[c]onsider the development of a standing working group on cyberspace" and "[e]mphasize the role of senior and *strategic* [emphasis added] leaders as potential advisors with respect to cyberspace events". In the context of PME, a strategic working group or leader could assist with the development and integration of the cyber domain into the 'products', plans and orders PME students frequently work with. Creating doctrine in this respect would be a logical first step, perhaps using the United States Army War College's Strategic Cyberspace Operations Guide (Leitzel, B. and Hillebrand, G., 2022) as a reference point.

Finally, established US initiatives such as the Armed Forces' Cyber Awareness Challenge would be a good starting point to address the requirement for ubiquitous cyber-education in the DF, provided it is improved upon and aligned with the DF context. Perhaps coupling this with the suggestions of Heatherly, J. C. and Melendez, I. (2019) would be wise, i.e. to regularly educate all ranks on; (1) their role in military cybersecurity; (2) improper use of internet and computing devices; (3) operational security (OPSEC); and (4) using relevant case studies to educate.

3.1 Conclusion

These recommendations are a subset of broader recommendations originally intended for the US Armed Forces. While the DF's cyber infrastructure and aspirations may skew their prioritisation and implementation in practice, most are sufficiently broad and fundamental across all of the reviewed literature that they should retain applicability. Significant detail remains to be analysed, but this chapter outlines the essentials for improved cyber-PME in the DF. Sipper, J. (2021) concludes his article on multidisciplinary cyber education by charging both military and civilian educational institutions to "keep pace" and generate the interoperability and cross-domain cyber-leadership that is demonstrably now required. The DF too should recognise its deficits in this respect, continue developing 'jointness' by examining PME and ensuring the cyber domain is elevated appropriately.

Compared with the other military domains, cyber is the fastest-changing and therefore the most difficult to keep up with. For PME this presents a difficult situation, where significant effort is required to remain relevant, while the risk of not doing so increases with time and technological advances. In any given year, operations within the land or air domains realistically change very little, whereas significant changes to material may be required within *months* for cyber (Office of the Army Chief Information Officer, 2021). Rather than an obstacle, the DF should view this as an opportunity to enhance its relevance in the national cyber defence context, and increase its interoperability and robustness in the context of deploying overseas.

As the world continues to grow in social, political and technological complexity, and contemporary conflicts continue to simmer beneath the threshold of war, the cost of not pursuing military competence in the cyber domain will ultimately outweigh any reasonable investment. Ireland continues to protect its public and private networks from cyber attacks through the National Cyber Security Strategy via the NCSC, but empowering and educating the DF in cyber should be treated as a central tenet of its modern national defence.

Conclusion

"If we have someone who is a genius in cybersecurity, but who is unfit, we should find a way to make that person a member of the Defence Forces."

- Micheál Martin[38]

In its preamble introducing the 2015 White Paper on Defence, the Irish Government discusses the need for a flexible policy framework that is "responsive […] to the dynamic nature of the security environment and the key role that Defence plays in the State's security architecture" (Government of Ireland, 2019b). With the unanimous international recognition of the importance of the cyber domain to national defence and security, and the demonstrably persistent cyber threat Ireland faces, the DF must therefore implement change and enable improvements to its cyber workforce and capability. While some of these changes may require government or department-level decisions or action, this thesis has shown that some important changes can be instigated at DF-level. Recruiting, revising syllabi, creating new roles or re-thinking postgraduate cyber-education are meaningful actions that can be driven from within existing DF-resources; so they should be.

Key Findings and Recommendations

This thesis was formed around three quite distinct research questions that cumulatively sought to investigate the DF's shortcomings in terms of recruitment, training and education for cyber. In the process it proposed several key concepts and mechanisms that may address some of those gaps, summarised here under the respective research questions.

Recognising both the current roles within the CIS Corps and the 'real-world' constraints placed on human resources, how does the DF recruit an appropriate cyber workforce?

Chapter One drew lessons from both the CAF and British Army cyber-recruitment efforts and found that flexible recruitment strategies, such as supporting candidates to demonstrate their cyber potential in various ways, cyber-aptitude tests, and follow-up

[38] Speaking as Tánaiste of Ireland and Minister for Defence in a statement to Seanad Éireann on the Report of the Independent Review Group on Dignity and Equality Issues in the Defence Forces on 25 April 2023 (Seanad Éireann, 2023).

training as appropriate are converging on a new best-practice. Importantly, both militaries achieve their cyber capability via several cyber-related roles, permitting individual specialisation and enhancing organisational resilience. The British Army's UCM (Unified Career Management) mechanism for cyber specialists is an ambitious yet appropriate initiative that emphasises the removal of obstacles that evidently encourage cyber specialists to exit the military. Ultimately, the unconventional and dynamic nature of the cyber domain calls for a flexible approach to recruitment and training.

The CIS Corps should therefore remain flexible and innovative in the recruitment, selection and training of personnel for cyber-related roles. Narrow policies in these respects evidently diverge from the emerging international consensus and erect artificial barriers to the development of a cyber workforce. Mechanisms such as Advanced Entry, Direct Entry and apprenticeships should be examined in more detail to better assess feasibility, and due consideration given to the potential reassessment of academic, medical and physical standards for prospective military cyber technicians or operators.

Given the DF's IT infrastructure, its communications technologies and recent events such as the HSE ransomware attack, what skills should cyber technicians possess, and what are the pathways to attain these skills?

Chapter Two was immediately forced to contend with the vacuum created by the lack of a well-defined role for DF CIS technicians and was forced to consider SME-qualified opinion as a baseline. Founded on experience and intimate knowledge of DF IT systems and policies, these opinions converged on a reasonable 'average' and thus permitted useful CyBOK comparison. Compounding the problem, the literature pertaining to the CAF, UK Armed Forces and US Army suggest that there is no single type of cyber engineer or operator. Roles are evidently defined in line with current operational and strategically-oriented requirements, naturally varying between militaries – so the DF cannot rely on 'borrowing' the roles (reword). Assessing the CIS TT Scheme and UCD MSc FCCI, it was found that the *cyber utility* of the former, and the CyBOK KA coverage of the latter are far from optimal.

The CIS Corps and future DF Cyber Strategies should be clearer about the roles and skills required of those working directly in the cyber domain, since this is the largest missing piece in terms of training. As it stands, this is a significant gap for the DF. Furthermore, and while acknowledging the benefits of a well-defined and common scheme of initial cyber-training, the value of varied professional and post-graduate education is also clear. The current UCD MSc in FCCI does not sufficiently meet the learning outcomes recommended by CIS Corps SMEs. Such considerations should be integral to the further development of appropriate training.

To what extent should general cyber education be integrated into Professional Military Education (PME) in the DF, in line with other militaries?

Chapter Three argued that the development of cyber-strategic leaders is a necessary task for the DF to prepare officers for command and higher defence management roles, nationally and internationally. By comparing the existing DF PME courses to US standards, a *significant* relative gap was revealed, persisting for most officers until attendance on the JCSC twenty or so years into their careers. The integration of the cyber domain is therefore not currently achieved by the DF, nor will it be until its leaders are competent enough to plan and act within or through it.

A standing working group on cyberspace and the emphasis of senior and strategic leaders as potential advisors with respect to cyber could further strengthen the DF's cyber strategy. Furthermore, cyber PME should focus on hands-on, in-depth technical and tactical skills, along with the understanding of concepts, knowledge of the use of cyber capabilities in military operations, and the ability to design and define strategies, policies, and future capabilities. More broadly, a DF version of the US Armed Forces' annual Cyber Awareness training could be considered, provided the learning outcomes are suitable and certain improvements are implemented.

Further Research

Further research may enhance the recommendations of this thesis. In particular, concerted effort is required to move from the present state of CIST (i.e. electronic engineering) training and education to a state that provides for a separate CIS Corps cyber-technician, and research may identify ways to overcome the associated challenges. The CoDF highlighted the need for "any enhanced capabilities in the cyber domain" to be developed only in "extremely close co-ordination" with relevant national agencies and national security policy (Commission on the Defence Forces, 2022, vii); therefore any new cyber roles must be deliberately defined in this context.

A similar assertion may be made in the case of progressing PME in the DF – further research could identify exactly what aspects of cyber security and defence should be taught to the general DF officer, and at what point in their careers. Finally, the imperative for improving PME in the DF with respect to cyber is clear. The vast majority of officers in the DF with less than twenty years' service have no formal military cyber training, introducing dangerous vulnerabilities to both national defence and DF operations.

While the CyBOK methodology is not the only tool to assess cyber training and education, it is both practical and rigorous. Fine tuning the CyBOK methodology with this research's novel *standardised broad category emphasis* permitted congruency with SME opinion, and perhaps further consideration could be given to adopting this as a standard tool to assess various cyber courses against DF requirements.

Concluding Remarks

In its High Level Action Plan for the Report of the CoDF, the Government accepted that in order to enhance DF structures in the cyber domain, the DF should "publish a cyber defence strategy in line with best practice" and "incorporate[e] practical lessons identified from comparator countries" (Government of Ireland, 2022, p.20). Lessons and insights from this thesis may serve as a reliable and useful starting point. While recruitment is an ongoing challenge for the contemporary DF, thoughtful consideration of the opportunities brought by the cyber domain is instead the more insightful perspective for recruitment, potentially opening national defence up to those who may otherwise not be suitable, or interested. At a time when ICT job stability in the private sector appears to be uncertain (The Irish Times, 2023), there is an opportunity for the DF to act decisively.

References

Alibhai, A. (2022). CAF Cyber Capability is M.I.A., Exercise Solo Flight, *JCSP 47*, Canadian Forces College, Canada.

Armed Forces Pay Review Body (2020). *Armed Forces' Pay Review Body, Forty-Ninth Report 2020*. Available at: https://www.gov.uk/government/publications/armed-forces-pay-review-body-forty-ninth-report-2020. (Accessed: 01 February 2023).

Armed Forces Pay Review Body (2021). *Armed Forces' Pay Review Body, Fiftieth Report 2021*. Available at: https://www.gov.uk/government/publications/armed-forces-pay-review-body-fiftieth-report-2021. (Accessed: 01 February 2023).

Armed Forces Pay Review Body (2022). *Armed Forces' Pay Review Body, Fifty-First Report 2022*. Available at: https://www.gov.uk/government/publications/armed-forces-pay-review-body-fifty-first-report-2022. (Accessed: 01 February 2023).

Army Cyber Institute (2018). *Army Cyber Institute (ACI) Home*. Available at: https://cyber.army.mil/. (Accessed: 22 August 2022).

Arney, C., Vanatta, N., and Nelson, T. (2016). Cyber Education via Mathematical Education. *Cyber Defense Review*, 1, no. 2 (Fall 2016): 49–59.

Babcock, C. (2015). Preparing for the Cyber Battleground of the Future. *Air & Space Power Journal*, 29(6), pp.61-74.

Blair, J.R., Hall, A.O. and Sobiesk, E. (2020). Holistic cyber education. *Cyber Security Education* (pp. 160-172). Routledge.

Bonner, E.L. (2014). Cyber power in 21st-century joint warfare. *Joint Force Quarterly*, 74(3), pp.102-109.

British Army (2021a). *Army's Only Cyber Regiment Celebrates First Birthday*. Available at: https://www.army.mod.uk/news-and-events/news/2021/06/cyber-regiment-birthday/. (Accessed: 02 February 2023).

British Army (2021b). *Future Soldier – Transforming the British Army*. Available at: https://www.army.mod.uk/media/11826/20210322-army-future_soldier-publication-final.pdf. (Accessed: 01 February 2023).

British Army (2022a). *Cyber Engineer - British Army Jobs*. British Army Roles. Available at: https://apply.army.mod.uk/roles/royal-signals/cyber-engineer. (Accessed: 18 August 2022).

British Army (2022b). *Royal Signals - British Army Jobs*. Available at: https://apply.army.mod.uk/roles/royal-signals?cid=refe5174135742. (Accessed: 09 August 2022).

British Army (2022c). *Joint Service Signals Unit (Volunteers).* Available at: https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-corps-of-signals/joint-service-signals-unit-volunteers/. (Accessed: 21 August 2022).

British Army (2022d). *Assessment Centre: Soldiers*. Available at: https://jobs.army.mod.uk/how-to-join/army-assessment/soldier/. (Accessed: 02 February 2023).

Canadian Armed Forces (2022a). *Careers | Canadian Armed Forces*. Available at: https://forces.ca/en/careers (Accessed: 08 August 2022).

Canadian Armed Forces (2022b). *Cyber Operator | Careers | Canadian Armed Forces*. Available at: https://forces.ca/en/career/cyber-operator/. (Accessed 30 January 2023).

Canadian Global Affairs Institute (2021). *Canada's Active Cyber Defence is Anything But Active*. Available at: https://www.cgai.ca/canadas_active_cyber-_defence_is_anything_but_active. (Accessed 30 January 2023).

Careers in the Military (2022). Cyber Security Specialists | Careers in the Military. Available at: https://www.careersinthemilitary.com/career-detail/cyber-security-specialists (Accessed: 21 February 2023).

Catal, Cagatay, Alper Ozcan, Emrah Donmez, and Ahmet Kasif (2022). Analysis of Cyber Security Knowledge Gaps Based on Cyber Security Body of Knowledge. *Education and Information Technologies*. https://doi.org/10.1007/s10639-022-11261-8.

CDS (2022). *Post Graduate Certificate in Wireless Communications*. Available at: https://www.cdsds.uk/training-learning-development/ubi-tech-programmes-courses/post-graduate-certificate-in-wireless-communications. (Accessed: 03 March 2023).

Chartered Institute of Information Security (2023). CIISec | The home of cyber. Available at: https://www.ciisec.org/. (Accessed: 05 March 2023).

CNET Training (2021). *Network Cable Installer Apprenticeship*. Available at: https://www.cnet-training.com/programs/nciapprenticeship/. (Accessed: 03 March 2023).

Collins, R. L. (2014). Cyberspace training permeates professional military education. *Army Communicator, (Spring),* pp.14-16.

Commission on the Defence Forces (2022). *Report of the Commission on the Defence Forces*. https://www.gov.ie/en/publication/eb4c0-report-of-the-commission-on-defence-forces/. (Accessed 12 July 2022).

Cranfield University (2022). *Cyber Defence and Information Assurance MSc (Defence)*. Available at: https://www.cranfield.ac.uk/courses/taught/cyber-defence-and-information-assurance. (Accessed: 03 March 2023).

CyberEd (2017). Cybersecurity Curricular Guidelines | CSEC 2017. Available at: https://cybered.hosting.acm.org/wp/. (Accessed: 05 March 2023).

CyBOK (2021a). *CyBOK - Cyber Body of Knowledge*. Available at: https://www.cybok.org/. (Accessed: 28 February 2022).

CyBOK (2021b). *Knowledgebase – CyBOK v1.1*. Available at: https://www.cybok.org/knowledgebase1_1/. (Accessed: 28 February 2023).

CyBOK (2021c). *CyBOK Mapping Framework*. Available at: https://www.cybok.org/media/downloads/CyBOK_Mapping_Framework_academic_professional_progs_Feb21.pdf. (Accessed: 28 February 2023).

CyBOK (2022). *Use Cases*. Available at: https://www.cybok.org/usecases/. (Accessed: 22 February 2023).

Defence Academy of the United Kingdom (2022). *Commander UK Strategic Command opens Defence Cyber Academy*. Available at: https://www.da.mod.uk/news-and-events/news/2022/commander-uk-strategic-command-opens-defence-cyber-academy. (Accessed: 02 February 2023).

Defence Forces (2013). *Defence Forces Cyber Defence Strategy*. Available on DF Intranet. (Accessed: 03 February 2023).

Defence Forces (2021). *DF CIS Corps Training Syllabus 28 – CIS Trainee Technician Scheme (TTS) – Amendment No. 4: 12 Nov 2021*. Available on DF Intranet. (Accessed 12 December 2022).

Defence Forces (2019a). *DF Infantry Training Syllabus 056/2019 – Land Command and Staff Course*. Available on DF Intranet. (Accessed 06 April 2023).

Defence Forces (2019b). *DF Infantry Training Syllabus 051/2019 – The Standard Cadet Course*. Available on DF Intranet. (Accessed 06 April 2023).

Defence Forces (2022). *DF Infantry Training Syllabus 016/2022 – Joint Command and Staff Course.* Available on DF Intranet. (Accessed 12 April 2023).

Farmer, A., Stevens, R., Jost, T., and O'Connell, R. (2014). Enabling cyber mission teams: Training, exercising, and innovating. *Military Intelligence Professional Bulletin*, 40(4), 19-20. (Accessed: 07 April 2023).

Fast Track into IT (2022). *What we do*. Available at: https://fit.ie/what-we-do/. (Accessed: 07 February 2023).

Fernandes, J., Starck, N., Shmel, R., Suslowicz, C., Kallberg, J., Arnold, T. (2022). Assessing the Army's Cyber Force Structure. *The US Army War College Quarterly*: Parameters 52. https://doi.org/10.55540/0031-1723.3170.

Glaser, B. and Strauss, A. (1967). Grounded theory: The discovery of grounded theory. *Sociology the journal of the British sociological association,* 12(1), pp.27-49.

Graham, E. (2022). *The Government Accountability Office found that the lack of required service time commitments within some of the military branches is making it difficult to retain personnel who have completed expensive and advanced cyber courses*. Nextgov.com. Available at: https://www.nextgov.com/cybersecurity/2022/12/military-branches-losing-expensive-cyber-talent-private-sector-watchdog-says/381261/. (Accessed 02 February 2023).

Government of Canada (2017). *Strong Secure Engaged – Canada's Defence Policy*. Available at: https://www.canada.ca/content/dam/dndmdn/documents/reports/2018/str-ong-secure-engaged/canada-defence-policy-report.pdf. (Accessed 30 January 2023).

Government of Canada (2020). *March 2020 - Canadian Armed Forces 101*. Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/caf-101.html. (Accessed: 08 February 2023).

Government of Canada (2021a). *Evaluation of the Cyber Forces*. Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/eval-cyber-forces.html. (Accessed: 31 January 2023).

Government of Canada (2021b). *Congratulations to the First Cyber Operator Graduates from the CFSCE*. Available at: https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/09/congratulations-first-cyber-operator-graduates-cfscr.html. (Accessed 31 January 2023).

Government of Ireland (2015). *White Paper on Defence*. Dublin: Defence Forces Printing Press.

Government of Ireland (2019a). *National Cyber Security Strategy 2019-2024*, p. 9. Available at: https://www.gov.ie/en/publication/8994a-national-cyber-security-strategy/ (Accessed 10 August 2022).

Government of Ireland (2019b). Defence | Policy. Available at: https://www.gov.ie/en/policy/f2c04b-defence/. (Accessed 02 May 2023).

Government of Ireland (2022). *Building for the Future – Change from Within: High Level Action Plan for the Report of the Commission on the Defence Forces*. Available at: https://www.gov.ie/en/publication/519f7-hlap-commission-on-the-defence-forces/. (Accessed 10 January 2023).

Hall, A. and Sobiesk, E. (2017). Integration of the Cyber Domain at the United States Military Academy. *Proceedings of the International Workshops Realigning Cybersecurity Education*, Melbourne, 24 November 2017, Vol. 10, Article No. 3293881.3295778.

Hall, Andrew and Schultz, Brian (2017). Direct Commission for Cyberspace Specialties. *Cyber Defense Review*, 2, no. 2: 111–23.

Hallett, J., Larson, R. and Rashid, A. (2018). Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. *Workshop on Advances in Security Education*, 18.

Hardison, C.M., Payne, L.A., Hamm, J.A., Clague, A., Torres, J., Schulker, D. and Crown, J.S. (2019). *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings*. Santa Monica, CA: RAND Corporation. Availableat: https://www.rand.org/pubs/research_reports/RR2618.html. Also available in print form.

Heatherly, J. C. and Melendez, I. (2019). Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army. *Cyber Defense Review*, 4, no. 1: 63–73.

HSE (2021). *Conti cyber attack on the HSE. Independent Post Incident Review*. Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf. (Accessed 03 February 2023).

IBM (2018). Cyber Aptitude Assessments component of IBM Kenexa Behavioral Assessments for Hourly Roles on Cloud helps organizations meet the challenge of hiring cybersecurity talent. Available at: https://www.ibm.com/common/ssi/Show-Doc.wss?docURL=/common/ssi/rep_ca/8/897/ENUS218098/index.html&request_locale=en. (Accessed: 07 February 2023).

Information and Communication Technologies Defense Division (n.d.). *Fort Gordon Online Course Login (Cyber Awareness and Cyber Security Fundamentals)*. Available at: https://cs.signal.army.mil/login.asp. (Accessed 10 April 2023).

Irish Defence Forces (2020). *Trainee Technician Scheme 2020*. Information Booklet. Available at: https://www.military.ie/en/members-area/members-area-files/final-df-tts-2020-booklet.pdf.

Irish Defence Forces (2022). *Current Competitions*. Available at: https://www.military.ie/en/careers/current-competitions/current-compeitions.html (Accessed: 26 September 2022).

(ISC)^2 (2023). Cybersecurity and IT Security Certifications and Training | (ISC)^2. Available at: https://www.isc2.org/. (Accessed: 05 March 2023).

Joint Chiefs of Staff (2020). Chairman of the Joint Chiefs of Staff Instruction | CJCSI 1800.01F. Available at: https://www.jcs.mil/Portals/36/Documents/-Doctrine/education/cjcsi_1800_01f.pdf?ver=2020-05-15-102430-580. (Accessed: 02 April 2023).

Jenkins, C. (2022). *Cyber Insider: Joint Cyber Reserve Force*. Blog – Strategic Command. Available at: https://stratcommand.blog.gov.uk/2022/11/22/cyber-insiders-joint-cyber-reserve-force/. (Accessed: 06 February 2023).

King's College London (2021). *The National Cyber Force that Britain Needs?* Available at: https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf. (Accessed: 02 February 2023).

Knox, B.J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R.G., Sütterlin, S., (2018). Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. *Military Psychology 30*, 350–359. https://doi.org/10.1080/08995605.2018.1478546.

Lamb, R.W. (2010). *Only hi tech forces can win wars of the future*. The Times. Available at: https://www.thetimes.co.uk/article/only-hi-tech-forces-can-win-wars-of-the-future-wzzr9kr7kcp. (Accessed: 20 September 2022).

Lee, S. and Kim, S. (2021). Blockchain as a cyber defense: opportunities, applications, and challenges. *IEEE Access*, 10, pp.2602-2618.

Leitzel, B. and Hillebrand, G. (2022). United States Army War College | Strategic Cyberspace Operations Guide. Available at: https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf. (Accessed: 04 April 2023).

Liles, S., Dietz, J.E., Rogers, M., Larson, D. (2012). Applying traditional military principles to cyber warfare, in: 2012. *4th International Conference on Cyber Conflict (CYCON 2012)*, pp. 1–12.

Line of Defence (2017). *The fog of smokeless war: A cyber security capability for the NZDF*. Available at: http://www.defsecmedia.co.nz/defence/march-2017-cyberwarfare/ (Accessed : 28 September 2022).

Lunn, L. (2021). *Cyber Operator: Are you sure you want to do that? Royal Military College Saint-Jean*. Available at: https://www.cmrsj-rmcsj.forces.gc.ca/cb-bk/art-art/2021/art-art-2021-7-eng.asp. (Accessed 30 January 2023).

Lynch, J. (2018). *Why recruiting cyberwarriors in the military is harder than retaining forces*. C4ISRNET. Available at: https://www.c4isrnet.com/dod/2018/11/01/why-recruiting-cyber-warriors-in-the-military-is-harder-than-retaining-forces/. (Accessed: 02 February 2023).

Mack, N.A., et al (2019). From Midshipmen to Cyber Pros: Training Minority Naval Reserve Officer Training Corp Students for Cybersecurity. *In Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (pp. 726-730).

Mead, N.R. and Tenbergen, B. (2021). *CyBOK Report on Classroom Usage of Case Studies*. Available at: https://www.cybok.org/media/downloads/CyBOK_Case_Studies-_Classroom_Usage_report.pdf. (Accessed: 09 March 2023).

Military Fitness (2022). *British Army Cyber Aptitude Assessment For 2022*. Available at: https://www.youtube.com/watch?v=CZdlzcKSZHg&ab_channel=MilitaryFitness. (Accessed: 01 February 2023).

Ministry of Defence (2020). *Allied Joint Doctrine for Cyberspace Operations*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. (Accessed: 01 January 2023).

Ministry of Defence (2021a). *Digital Strategy for Defence – Delivering the Digital Backbone and unleashing the power of Defence's data*. Available at: https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data. (Accessed 31 January 2023).

Ministry of Defence (2021b). *Joint Service Signals Unit (Volunteers)*. Available at: https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-corps-of-signals/joint-service-signals-unit-volunteers/. (Accessed: 20 August 2022).

Ministry of Defence (2021c). *Defence in a Competitive Age*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf. (Accessed 04 January 2023).

Ministry of Defence (2021d). *Reserve Forces Review 2030 – Unlocking the reserves' potential to strengthen a resilient and global Britain*. Available at: https://www.gov.uk/government/publications/reserve-forces-review-2030. (Accessed: 06 February 2023).

Ministry of Defence (2022a). *Cyber Primer*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1115061/Cyber_Primer_Edition_3.pdf. (Accessed: 21 December 2022).

Ministry of Defence (2022b). *Cyber Resilience Strategy for Defence*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1073315/20220425-Cyber_Resilience_Strategy_for_Defence.pdf. (Accessed: 02 January 2023).

Ministry of Defence (2022c). *DE&S Apprenticeship & Graduate Schemes*. Available at: https://des.mod.uk/careers/graduate-schemes-and-apprenticeships/. (Accessed: 02 February 2023).

National Cyber Security Centre (2019). *NCSC Certified Training*. Available at: https://www.ncsc.gov.uk/information/certified-training. (Accessed: 21 February 2023).

National Defense University (n.d.). *Graduate Certificates.* College of Information and Cyberspace. Available at: https://cic.ndu.edu/Academics/Graduate-Certificates/. (Accessed: 02 April 2023).

National Cyber Security Centre (2023). UK's schoolgirl cyber security champions joined by undeclared war star at prestigious awards night. Available at https://www.ncsc.gov.uk/news/cyber-security-champions-joined-by-undeclared-war-star-at-prestigious-awards-nights. (Accessed: 24 April 2023).

Nawrat, A. (2021). *How the UK military is using bespoke HR tech to tap private sector talent*. Unleash. Available at: https://www.unleash.ai/talent-management/how-the-uk-military-uses-recruitment-technology/. (Accessed: 02 February 2023).

New Zealand Army (2021). *Army | Defence Careers. Defence Careers*. Available at: https://www.defencecareers.mil.nz/army/ (Accessed: 05 August 2022).

New Zealand Air Force (2021). *CIS Officer | Intelligence IT & Communications | Defence Careers*. Available at: https://www.defencecareers.mil.nz/air-force/careers/browse-roles/cis-officer/. (Accessed: 12 August 2022).

New Zealand, Ministry of Defence (2016). *Defence White Paper 2016,* p.76. Available at: https://www.defence.govt.nz/assets/Uploads/daac08133a/defence-white-paper-2016.pdf. (Accessed: 07 August 2022).

New Zealand Ministry of Defence (2022). *Cyber Security and Support Capability | Ministry of Defence Website*. Available at: https://www.defence.govt.nz/what-we-do/delivering-defence-capability/defence-capability-projects/cyber-security-and-support-capability/. (Accessed: 13 August 2022).

Office of the Army Chief Information Officer (2021). Army Digital Transformation Strategy. Available at: https://api.army.mil/e2/c/downloads/2021/10/20/3b64248b/army-digital-transformation-strategy.pdf. (Accessed: 28 March 2023).

Orye, E. and Faith-Ell, G. (2020). *Cyber workforce recruitment and retention: an awareness assessment*. NATO CCDCOE Report. Available at: https://ccdcoe.org/library/publications/cyber-workforce-recruitment-and-retention-an-awareness-assessment/. (Accessed: 07 February 2023).

PricewaterhouseCoopers (2021). *Conti cyber attack on the HSE – Independent Post Incident Review*. Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf. (Accessed: 01 Jan 2023).

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M. and Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, 16(3), pp.96-102.

Porche III, I.R., O'Connell, C., Davis II, J.S., Wilson, B., Serena, C.C., McCausland, T.C., Johnson, E.E., Wisniewski, B.D., Vasseur, M. (2017). *Cyber Power Potential of the Army's Reserve Component*. Santa Monica, CA: RAND Corporation, 2017. Available at: https://www.rand.org/pubs/research_reports/RR1490.html.

QA (n.d.). *Network Engineer Level 4 Apprenticeship*. Available at: https://www.qa.com/apprenticeships/it/network-engineer-level-4/. (Accessed: 03 March 2023)

Rodriguez, A. (2022). *We Need Senior Cyber Leaders. Service War Colleges Can Train Them*. War on the Rocks. Available at: https://warontherocks.com/2022/03/we-need-senior-cyber-leaders-service-war-colleges-can-train-them/. (Accessed: 02 April 2023).

Royal Air Force (2022). *Joint Cyber Unit*. Available at: https://recruitment.raf.mod.uk/roles/roles-finder/cyberspace/joint-cyber-unit. (Accessed: 06 February 2023).

Scanlon, E. (2004). 'The Issue of Separation – Towards Developing Good Practices'. MA (LMDS) thesis. National University of Ireland, Maynooth.

Schatz, D., Bashroush, R., Wall, J., 2017. Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, 12. https://doi.org/10.15394/jdfsl.2017.1476.

Seanad Éireann (2023). Report of the Independent Review Group on Dignity and Equality Issues in the Defence Forces: Statements. Available at: https://www.oireachtas.ie/en/debates/debate/seanad/2023-04-25/12/. (Accessed: 26 April 2023).

Slapakova, L., Caves, B., Posard, M.N., Muravska, J., Dascalu, D., Myers, D.Y., Kuo, R. and Thue, K. (2022). *Leveraging diversity for military effectiveness: Diversity, inclusion and belonging in the UK and US Armed Forces*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1026-1.html.

Sipper, J. (2021). It's Not Just About Cyber Anymore: Multidisciplinary Cyber Education and Training Under the New Information Warfare Paradigm. *Joint Forces Quarterly, Joint Forces Quarterly* 100 (1), 49-56.

Smeets, M. (2022). What it Takes to Develop a Military Cyber-Force. *Policy Perspectives*, 10, 4. Available at: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-7_2022-EN.pdf.

Spidalieri, F. and McArdle, J. (2016). Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*, 1, 141–164.

Tabansky, L. (2020). Israel Defense Forces and National Cyber Defense. *Connections* 19, 45–62.

The Irish Times (2023). *The Irish Times view on job losses in tech: a warning signal*. Editorial. Available at: https://www.irishtimes.com/opinion/editorials/2023/01/23/the-irish-times-view-on-job-losses-in-tech-a-warning-signal/. (Accessed: 08 February 2023).

Tikk-Ringas, E., Kerttunen, M., Spirito, C. (2014). Cyber Security as a Field of Military Education and Study. *Joint Force Quarterly,* no. 75 (2014): 44.

Tranfield, D., Denyer, D. and Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), pp.207-222.

Trippe, D., Matthew. (2014). Development of a Cyber/Information Technology Knowledge Test for Military Enlisted Technical Training Qualification. *Military Psychology*, 26:3 (2014): 182–98. https://doi.org/10.1037/mil0000042.

UCD (2020). CCI joins NATO Cyber Coalition 2020 exercise. Available at: https://www.ucd.ie/cci/news/ccijoinsnatocybercoalition2020exercise/. (Accessed: 06 February 2023).

UCD (2022). *MSc Forensic Computing and Cybercrime Investigation*. Available at: https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=PROG&MAJR=T146. (Accessed: 02 February 2023).

UK Government (2016a). *National Cyber Security Strategy 2016-2021*. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. (Accessed: 01 February 2023).

UK Government (2016b). *Defence cyber test launched*. Available at: https://www.gov.uk/government/news/defence-cyber-test-launched#:~:text=The%20Ministry%20of%20Defence%20has,an%20aptitude%20for%20cyber%20work.&text=The%20Defence%20Cyber%20Aptitude%20Test,particular%20skill%20for%20cyber%20work. (Accessed: 01 February 2023).

UK Government (2020). *DESG Graduate Scheme – Fact Sheet*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/28401/grad_fact_sheet.pdf. (Accessed: 02 February 2023).

UK Government (2021a). *UK Strategic Commander DSEI 2021 Speech*, GOV.UK. Available at: https://www.gov.uk/government/speeches/uk-strategic-commander-dsei-2021-speech (Accessed: 01 February 2023).

UK Government (2021b). *Ministry of Defence launches Unified Career Management*. Available at: https://www.gov.uk/government/news/ministry-of-defence-launches-unified-career-management. (Accessed: 01 February 2023).

UK Government (2022a). *National Cyber Strategy 2022*. Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022. (Accessed: 10 August 2022).

UK Government (2022b). *Ministry of Defence Annual Report and Accounts 2021 to 2022*. Available at: https://www.gov.uk/government/publications/ministry-of-defence-annual-report-and-accounts-2021-to-2022. (Accessed: 01 February 2023).

UK Government (2020). *About us - The National Cyber Force (NCF) is a partnership between defence and intelligence*. Available at: https://www.gov.uk-/government/organisations/national-cyber-force/about. (Accessed: 01 February 2023).

US Army (2017). *Army Regulation 350-1 | Army Training and Leader Development*. Available at: https://usacac.army.mil/sites/default/files/documents/cace/LREC/AR350-1_Web_FINAL.PDF. (Accessed: 29 March 2023).

U.S. Army Command and General Staff College (2020). U.S. Army Command and General Staff College Catalog | CGSC Circular 350-1. Available at: https://usacac.army.mil/sites/default/files/documents/cace/CGSC/CGSC_Circular_350-1_College_Catalog_%282020-2021%29.pdf. (Accessed: 05 April 2023).

US Army Cyber Command (2021). *Army Cyber Fact Sheet: Army Cyber Direct Commissioning Program*. Available at: https://bit.ly/3CsSDek. (Accessed: 15 August 2022).

US Department of Defense (2011). *Department of Defense Strategy for Operating in Cyberspace 19*. Available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/-

documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. (Accessed: 21 September 2022).

US Department of Defense (2021). Career Pathway Executive Cyber Leadership (901). Available at: https://dl.dod.cyber.mil/wp-content/uploads/ccp/pdf/901_Executive-_Cyber_Leadership-Career_Pathway.pdf. (Accessed: 02 April 2023).

US Department of Health and Human Services (2022). *Lessons Learned from the HSE Cyber Attack*. Available at: https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf. (Accessed 13 January 2023).

US Marine Corps (2016). FY-16 Annual Cyber Security Awareness Training. Available at: https://www.marines.mil/News/Messages/Messages-Display/Article/898038/fy-16-annual-cyber-security-awareness-training/#.ZDcj5yKo-WY.link. (Accessed 12 April 2023).

US Military Academy (n.d. a). *Academic Majors and Minors*. Available at: https://www.westpoint.edu/academics/majors-and-minors. (Accessed 13 April 2023).

US Military Academy (n.d. b). *Cadet Summer Training*. Available at: https://www.westpoint.edu/military/department-of-military-instruction/cadet-summer-training. (Accessed 13 April 2023).

Waddell, W., Smith, D., Shufelt, J. and Caton, J. (2011). *Cyberspace Operations | What Senior Leaders Need to Know About Cyberspace*. U.S. Army War College, Center for Strategic Leadership. Available at: https://apps.dtic.mil/sti/pdfs/ADA540637.pdf. (Accessed: 03 April 2023).

Warrell, H. (2021). *UK Military Relaxes Recruiting Rules to Attract Cyber Specialists*. Financial Times. Available at: https://www.ft.com/content/92a63e8b-36a3-477d-9bb4-3bcfb60cc7fa. (Accessed: 01 February 2023).

WhatDoTheyKnow (2022). *Golden Hello awarded to Royal Signals Info Services Engineers 2017-2020*. WhatDoTheyKnow. Available at: https://www.whatdo-theyknow.com/request/golden_hello_awarded_to_royal_si. (Accessed 02 February 2023).

Williams, B. (2020). Cyber Warriors: Army Reserve units take up mission task of cyber operators. Canadian Army Today. Available at: https://canadianarmytoday.com/cyberwarriors-army-reserve-units-take-up-mission-task-of-cyber-operators/. (Accessed: 07 February 2023).

Willis College (2023). CyberSecurity Operator – Become a CyberSecurity Operator. Available at: https://williscollege.com/programs/technology/cybersecurity-operator/. (Accessed: 03 March 2023).

Appendix 1 – CyBOK Knowledge Areas and Acronyms

Acronym	Knowledge Area	Broad Category
AAA	Authentication, Authorisation & Accountability	Systems Security
AC	Applied Cryptography	Infrastructure Security
AB	Adversarial Behaviours	Attacks and Defences
C	Cryptography	Systems Security
CI	CyBOK Introduction	(Not used)
CPS	Cyber-Physical Systems Security	Infrastructure Security
DSS	Distributed Systems Security	Systems Security
F	Forensics	Attacks and Defences
FMS	Formal Methods for Security	Systems Security
HF	Human Factors	Human, Organisational and Regulatory Aspects
HS	Hardware Security	Infrastructure Security
LR	Law & Regulation	Human, Organisational and Regulatory Aspects
MAT	Malware & Attack Technologies	Attacks and Defences
NS	Network Security	Infrastructure Security
OSV	Operating Systems & Virtualisation	Systems Security
PLT	Physical Layer & Telecommunications Security	Infrastructure Security
POR	Privacy & Online Rights	Human, Organisational and Regulatory Aspects
RMG	Risk Management & Governance	Human, Organisational and Regulatory Aspects
SOIM	Security Operations & Incident Management	Attacks and Defences
SS	Software Security	Software and Platform Security
SSL	Secure Software Lifecycle	Software and Platform Security
WAM	Web & Mobile Security	Software and Platform Security

Appendix 2 – CyBOK KA Mapping of UCD MSc FCCI

Module Name	Learning Outcome	CyBOK KA	CyBOK Broad Category
Computer Forensics	Information representation in computing	F	Attacks and Defences
	Convert between number systems	PLT	Infrastructure Security
	Interpret raw hexadecimal information	F	Attacks and Defences
	Acquire and verify a disk image	F	Attacks and Defences
	Explain logical and physical hard disk structure	F	Attacks and Defences
	Interpret common file system structures	F	Attacks and Defences
Network Investigations	Describe basic networking concepts and hardware	NS	Infrastructure Security
	Identify networking hardware components	NS	Infrastructure Security
	Design subnetworks	NS	Infrastructure Security
	Describe common Internet protocols	CPS, NS	Infrastructure Security x 2
	Perform lawful interception and analysis of network traffic	NS, FMS, MAT, SOIM	Infrastructure Security, Systems Security, Attacks and Defences x 2
	Analyse common networking artifacts such as: Web browsers; email clients; IRC;etc.	FMS, F	Attacks and Defences, Systems Security
Programming for Investigators	Write scripts in Bash	SS	Software and Platform Security
	Build custom tools for extracting necessary information from evidential data and for post-processing of output of third-party digital forensic tools.	F	Attacks and Defences
	Describe the differences between compiled and interpreted programming languages	SS	Software and Platform Security
	Write scripts and programs using simple constructs such as assignment, selection, iteration, etc.	SS, SSL	Software and Platform Security x 2
	Write scripts and programs using regular expressions	SS	Software and Platform Security
Case Studies	Apply forensic techniques to running investigations	F	Attacks and Defences
	Report on the results of these investigations	F, SOIM	Attacks and Defences x 2
	Evaluate the performance of these techniques	F, SOIM	Attacks and Defences x 2
Linux for Investigators	Install the Linux Operating System	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Navigate the Linux File System	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2

	Utilise standard Linux tools for digital forensics	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Acquire images of electronic storage devices in a forensically sound manner	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Analyse file systems using Linux tools	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Perform data carving using Linux tools	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Gather information on running Linux systems	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
VoIP and Wireless Investigations	Describe the technologies used in creating and using a wireless network	PLT, AC, CPS, NS	Infrastructure Security x 4
	Explain the operation of various wireless security protocols	NS, SSL	Infrastructure Security, Software and Platform Security
	Compare and contrast the relative strengths of said security protocols	C, PLT, WAM	Infrastructure Security x 2, Systems Security, Software and Platform Security
	Gather information on wireless networks using both passive and active means	AB, MAT, HF	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	Explain the technology on which Voice over IP is reliant	WAM, NS, PLT	Infrastructure Security x 2, Software and Platform Security
	Describe the potential sources of evidence available in VoIP clients and interceptions.	F	Attacks and Defences
	Analyse artifacts associated with common VoIP clients.	F	Attacks and Defences
Advanced Computer Forensics	Locate and describe various Windows system and application artifacts	F	Attacks and Defences
	Analyse various Windows system and application artifacts	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Locate, describe, and analyse Linux Forensic Artifacts	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Describe the principles of applied forensic research	F	Attacks and Defences
	Evaluate the performance of forensic tools	F	Attacks and Defences
	Conduct applied research into new artifacts	F, LR	Attacks and Defences, Human, Organisational and Regulatory Aspects
Malware Investigations	List and explain hacking offences as defined by the Council of Europe's Convention of Cybercrime	LR	Human, Organisational and Regulatory Aspects
	Explain the purpose of malware	MAT	Attacks and Defences
	Describe common methods of malware dispersal and transmission	MAT, AB	Attacks and Defences x 2
	Explain the “Business Models” of Malware	AB, MAT	Attacks and Defences x 2
	Describe the process of Malware Analysis	AB, MAT	Attacks and Defences x 2

	Determine the purpose of unknown executable files in a safe manner	OSV, F	Attacks and Defences, Systems Security
	Detect the signs of malware intrusion on computer systems	MAT, SOIM, NS	Infrastructure Security, Attacks and Defences x 2
Live Data Forensics	Describe the live data forensic process	F, MAT	Attacks and Defences x 2
	Prepare teams for site searches	LR	Human, Organisational and Regulatory Aspects
	Knowing the legal aspects of live data forensics	LR	Human, Organisational and Regulatory Aspects
	Acquire and analyse the contents of RAM	F, OSV	Attacks and Defences, Systems Security
	Gather information on running systems	SOIM, F	Attacks and Defences x 2
	Detect encrypted volumes	HS, C, OSV, AC	Infrastructure Security x 2, Systems Security x 2
	Preserve information found on running systems in a forensically sound manner	AAA, F	Attacks and Defences, Systems Security
	Analyse gathered artefacts and report their findings	F, OSV, MAT, AAA, SOIM	Attacks and Defences x 3, Systems Security x 2
	Research new devices or techniques in the field of live data forensics	CPS, F	Attacks and Defences, Infrastructure Security
Data & Database Forensics	Define database terminology, design and build simple database solutions for investigations	OSV, AAA, SOIM	Systems Security x 2, Attacks and Defences
	Describe a general technique for analysing	SOIM	Attacks and Defences
	Analyse SQLite3 artefacts from common applications	F	Attacks and Defences
	Extract information from unstructured data	F	Attacks and Defences
	Analyse text files, email, log files, social media feeds, news feeds, blogs and chats	SOIM, F	Attacks and Defences x 2
Advanced Malware Analysis	Assess the Windows Operating System as an attack platform for malicious code	OSV, F, MAT	Attacks and Defences x 2, Systems Security
	Analyse malware through reverse engineering and debugging	MAT, FMS, CI, AC, SSL, F, LR, HS	Attacks and Defences x 2, Infrastructure Security, Systems Security, Human, Organisational and Regulatory Aspects, Software and Platform Security
	Analyse some of the most common non-Windows executable malware, such as PDF or Android.	SOIM, WAM, F, SSL, HF	Attacks and Defences, Human, Organisational and Regulatory Aspects, Software and Platform Security x 2
Online Fraud Investigations for Irish Law Enforcement (5 ECTS Credits)	Understand how fraud is conducted via the Internet and the models that support it	LR, MAT, PLT, WAM, AB	Infrastructure Security, Attacks and Defences x 2, Human, Organisational and Regulatory Aspects, Software and Platform Security
	Understand the Darknet and how Virtual Private Networking can be used by investigators and criminals	NS, POR, F, LR	Attacks and Defences, Infrastructure Security,

			Human, Organisational and Regulatory Aspects x 2
	Seize devices at a crime scene in an appropriate manner, with respect to the preservation of evidence while maintaining chain of custody	F, SOIM, LR	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	Request subscriber information from Internet service providers through the SPOC (Garda Single Point of Contact)	PLT, HS, LR	Infrastructure Security x 2, Human, Organisational and Regulatory Aspects
	Perform basic open source intelligence gathering tasks while maintaining anonymity on the Internet	SOIM, HS, SSL, F, AC, LR, OSV	Attacks and Defences x 2, Infrastructure Security x 2, Human, Organisational and Regulatory Aspects, Systems Security, Software and Platform Security
	Understand and utilise their relationship with the Garda Bureau of Fraud Investigation, CCIU	LR	Human, Organisational and Regulatory Aspects
Mobile Devices Investigation	Identify common data types stored on mobile devices	F, SSL, WAM	Attacks and Defences, Software and Platform Security, Software and Platform Security
	Understand the different methods of data acquisition	F	Attacks and Defences
	Acquire knowledge of how data is stored on different mobile operating systems	PLT, F, WAM	Attacks and Defences, Infrastructure Security, Software and Platform Security
	Develop an awareness of different methods of communication used by mobile devices	WAM, PLT	Infrastructure Security, Software and Platform Security
	Have a knowledge of flash memory used in mobile devices	F	Attacks and Defences
Legislation regarding Fraud & Economic Crime (5 ECTS Credits)	Investigate payment card & currency fraud	AB, AC, LR	Infrastructure Security, Attacks and Defences, Human, Organisational and Regulatory Aspects
	Working knowledge of the main fraud offences	AB, AC, LR	Infrastructure Security, Attacks and Defences, Human, Organisational and Regulatory Aspects
	Working knowledge of the relevant legislative Acts	AB, AC, LR	Infrastructure Security, Attacks and Defences, Human, Organisational and Regulatory Aspects
	How to apply for information from Revenue for investigations	LR	Human, Organisational and Regulatory Aspects
	How to obtain suitable warrants and court orders	LR	Human, Organisational and Regulatory Aspects
	Have a broad knowledge of other relevant legislation	LR	Human, Organisational and Regulatory Aspects
Financial Fraud Investigation	Conduct a fraud investigation including preparing and managing a complex fraud investigation file	LR, AB, FMS	Attacks and Defences, Systems Security, Human, Organisational and Regulatory Aspects
	Identify criminality in a complaint and identify proofs necessary.	LR, AB, FMS	Attacks and Defences, Systems Security,

			Human, Organisational and Regulatory Aspects
	Prepare for the taking of witness statements and suspect statements.	LR, FMS	Systems Security, Human, Organisational and Regulatory Aspects
	Carry out investigation plan, including uplifting evidence correctly and to be cognisant of disclosure obligations.	FMS, F, LR	Attacks and Defences, Systems Security, Human, Organisational and Regulatory Aspects
	Be able to apply learned skills in investigations of specific types of criminality (Complex commercial fraud cases e.g. pyramid schemes, mortgage fraud, bribery & corruption fraud, company fraud, money laundering and terrorist financing, payment card fraud, and proceeds of crime etc.)	LR, AB, F	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
Financial Investigation Techniques - Following the Money	Explain basic principles of financial	LR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Apply basic accounting techniques to money laundering	LR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Be aware of, and familiar with, the main methods used by criminals to hide the proceeds of crime	LR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Safely use the many OSINT methods that are available to investigate financial crimes	LR, AB, SOIM	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	Understand how criminals use the Darknet and hidden internet.	NS, POR, F, LR, AB	Attacks and Defences x 2, Infrastructure Security, Human, Organisational and Regulatory Aspects x 2
	Recognise and be capable of investigating money laundering and the financing of terrorism	AC, AAA, AB	Systems Security, Infrastructure Security, Attacks and Defences
	Understand and be able to counter the most common excuses offered by criminals for unexplained wealth.	AC, AAA, AB	Systems Security, Infrastructure Security, Attacks and Defences
	Understand the financing of terrorism	AC, CPS, PLT, LR, CI	Infrastructure Security x 3, Human, Organisational and Regulatory Aspects
OSINT Collection & Analysis	Describe open source intelligence gathering methodologies	SOIM, HS, SSL, F, AC, LR, OSV, AB	Attacks and Defences x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects, Software and Platform Security
	Search open sources, social media sites, DarkWeb/DeepWeb for intelligence in a forensic sound manner	SOIM, LR, AB	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	Develop and use automated social network analyses	SOIM, LR, AB	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects

	Describe the hidden use of the internet and search in an anonymous way, so that traces are kept to the minimum	AB, F	Attacks and Defences x 2
	Describe the reliability of search results	F	Attacks and Defences
	How to use social media sites without endangering yourself or others in Law Enforcement	AB, WAM	Attacks and Defences, Software and Platform Security
	List and use online databases and information gathering tools	SOIM, LR, AB	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	Analyse and report search results	AB	Attacks and Defences
Online Child Abuse Invest.	Understand how criminals use ICT to offend against children as well as sex offenders from an investigators perspective both online and offline	HF, AB, AC, LR, POR	Infrastructure Security, Attacks and Defences, Human, Organisational and Regulatory Aspects x 3
	Understand technologies and platforms used by offenders to access CSAM including anonymization, obfuscation and encryption.	C, AC, NS, SOIM, MAT, AC	Infrastructure Security x 2, Systems Security, Attacks and Defences x 2
	Understand the digital forensic aspects of online offenders and explore digital media formats preferred by offenders	F, C, SOIM, AB	Attacks and Defences x 3, Systems Security
	Grasp the importance of social media to both offenders and victims	AB, POR, LR, WAM	Attacks and Defences, Human, Organisational and Regulatory Aspects x , Software and Platform Security
	Fully understand risk taking activity of children online	LR, POR, AB, F	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects x 2
	Victimology in an online environment	LR, POR, AB, F	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects x 2
	Recognise the role of law enforcement in online prevention of offending	LR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Understand the importance of CSAM Victim Identification and master CSAM victim identification techniques and tools	F	Attacks and Defences

Knowledge Area Emphasis	
Human, Organisational & Regulatory Aspects	
Risk Management and Governance	0
Law and Regulation	37
Human Factors	3
Privacy and Online Rights	6
Total:	**46**
Attacks & Defences	
Malware and Attack Technology	22
Adversarial Behaviours	31
Security Operations and Incident Management	28
Forensics	54
Total:	**135**
Systems Security	
Cryptography	4
Operating Systems and Virtualisation Security	17
Distributed System Security	0
Formal Methods for Security	7
Authentication, Authorisation and Accountability	14
Total:	**42**
Software and Platform Security	
Software Security	4
Web and Mobile Security	9
Secure Software Lifecycle	7
Total:	**20**
Infrastructure Security	
Applied Cryptography	13
Network Security	12
Hardware Security	5
Cyber Physical Systems	4
Physical Layer and Telecommunications Security	9
Total:	**43**

Appendix 3 – UCD MSc Cybersecurity

Module Name	Learning Outcome	CyBOK KA	CyBOK Broad Category
Leadership in Security (5 ECTS Credits)	Measuring security and identifying critical gaps	SOIM, RMG	Human, Organisational and Regulatory Aspects, Attacks and Defences
	Assessing risk and weighing priorities	SOIM, RMG	Human, Organisational and Regulatory Aspects, Attacks and Defences
	Tracking strategic threats and maintaining situational awareness	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Information security governance frameworks	RMG	Human, Organisational and Regulatory Aspects
	Influencing leadership and organisational culture	LR, HF	Human, Organisational and Regulatory Aspects x 2
	Communicating security to executives	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Gaining and increasing security investment	RMG	Human, Organisational and Regulatory Aspects
	Security versus compliance (and other key alliances)	RMG	Human, Organisational and Regulatory Aspects
	Attracting and assessing security talent	-	
	Maximising retention in security roles	-	
	Leading security professionals	-	
	Executing on a Security Programme	-	
	Managing yourself and achieving a sustainable career	-	
	Benefiting from external perspectives	-	
	Working with security vendors	RMG, HF	Human, Organisational and Regulatory Aspects x 2
Incident Response (5 ECTS Credits)	Understand the process of Incident Response	RMG, SOIM	Human, Organisational and Regulatory Aspects, Attacks and Defences
	Understand how various malware tool sets work	MAT	Attacks and Defences
	Understand and learn from major incidents of the recent past, including both 'for profit' criminal attacks, espionage, and military attacks	AB, SOIM	Attacks and Defences x 2
	Understand the legal, human resource, and corporate ramifications arising from acting in response to incidents	HF, SOIM, LR	Human, Organisational and Regulatory Aspects x 2, Attacks and Defences
	Discuss current trends and likely future directions in cyber threat	RMG, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Understand, and be able to, rapidly assess an individual threat, using high quality, trusted sources on the internet	SOIM	Attacks and Defences
Network Security	Obtain an extensive knowledge of both the principles and the practice of	NS, AAA	Systems Security, Infrastructure Security

	modern network and communication security.		
	Understand the in-depth understanding of computer and wireless network concepts	NS, CPS	Infrastructure Security x 2
	Understand the issues to be addressed by network security related to both computer and wireless networks	NS, CPS	Infrastructure Security x 2
	Understand current issues with network security and the state-of-the-art attack detection and prevention mechanisms	NS, CPS, SOIM	Infrastructure Security x 2, Attacks and Defences
	Learn about the network security of practical applications (i.e., telecom networks, cloud computing, IoT) and secure network communications techniques used for these applications around the globe.	PLT, AAA, NS, CPS	Systems Security, Infrastructure Security x 2
	Learn about emerging network and communication security techniques (i.e., network softwarization, quantum computing, cloud-native technologies, AI, and Blockchain)	RMG, SOIM	Human, Organisational and Regulatory Aspects, Attacks and Defences
Applied Cryptography (5 ECTS Credits)	Understand the fundamentals of the major algorithms used in modern cryptography	AC, C	Infrastructure Security, Systems Security
	Understand the practical deployment of such algorithms	AC	Infrastructure Security
	Use cryptographic tools and techniques to encrypt, decrypt and sign messages	AC, C	Infrastructure Security, Systems Security
	Identify attacks and vulnerabilities in cryptographic systems, and their countermeasures	AC, C	Infrastructure Security, Systems Security
	Explain multi-step security protocols	NS, PLT, AAA, WAM	Systems Security, Infrastructure Security x 2
Risk Assessment and Standards (5 ECTS Credits)	Understand the concepts of risk, risk response and mitigation	RMG	Human, Organisational and Regulatory Aspects
	Identify and protecting an organization from unacceptable losses	RMG	Human, Organisational and Regulatory Aspects
	Apply the NIST/ISO risk management processes	RMG	Human, Organisational and Regulatory Aspects
	Outlining the system security boundary	RMG	Human, Organisational and Regulatory Aspects
	Identify security risk components	RMG	Human, Organisational and Regulatory Aspects
	Estimate the impact of compromises to confidentiality, integrity and availability	RMG, MAT, AAA	Systems Security, Human, Organisational and Regulatory Aspects, Attacks and Defences
	Adopt the appropriate model for categorizing system risk	RMG	Human, Organisational and Regulatory Aspects
	Setting the stage for successful risk management	RMG, HF	Human, Organisational and Regulatory Aspects x 2

	Documenting risk assessment and management decisions	RMG	Human, Organisational and Regulatory Aspects
Secure Software Engineering	Identify key security concepts (assets, requirements, vulnerabilities), threats and attacks to software systems	SSL, MAT	Attacks and Defences, Software and Platform Security
	Distinguish the most common classes of vulnerabilities, including architectural flaws and security bugs, in software projects	SSL	Software and Platform Security
	Select countermeasures that could be applied to mitigate vulnerabilities	SSL, MAT	Attacks and Defences, Software and Platform Security
	Identify and exploit security vulnerabilities in software projects using security testing	RMG, SSL	Human, Organisational and Regulatory Aspects, Software and Platform Security
	Design secure software and develop patches to remove vulnerabilities from existing software projects	SSL	Software and Platform Security
	Specific security and privacy requirements, including compliance with necessary standards and regulations	SSL, SOIM	Attacks and Defences, Software and Platform Security
	Work in teams, share work fairly and meet the obligations set by the group	-	
	Be curious about latest security vulnerabilities and patches	-	
	Actively promote security practices	-	
Information Security	Understand Information Security	RMG	Human, Organisational and Regulatory Aspects
	Identify Security concerns in the design and implementation of secure systems	RMG, FMS	Systems Security, Human, Organisational and Regulatory Aspects
	Understand and apply Security models and design principles	SSL, FMS	Systems Security, Software and Platform Security
	Understand the role of cryptography and security protocols	AC, SSL, FMS	Infrastructure Security, Systems Security, Software and Platform Security
	Understand privilege management access control	AAA, OSV	Systems Security x 2
	Understand common software and network vulnerabilities	SSL, NS	Infrastructure Security, Software and Platform Security
	Understand usable security and the human factor	AC, HF	Infrastructure Security, Human, Organisational and Regulatory Aspects
	Discuss the concepts of Privacy VS Surveillance	AC, LR, POR	Infrastructure Security, Human, Organisational and Regulatory Aspects x 2
	Undertake real world case studies in information security	POR, RMG, LR	Human, Organisational and Regulatory Aspects x 3
Cybersecurity Law and Regulation	Describe the international and domestic legal framework relevant to cybersecurity	LR	Human, Organisational and Regulatory Aspects
	Describe and critically assess key legal issues presented by cybercrime	LR	Human, Organisational and Regulatory Aspects
	Data protection compliance	LR	Human, Organisational and Regulatory Aspects
	Outline and discuss the legal issues which may arise at each step of responding to a cybersecurity	LR	Human, Organisational and Regulatory Aspects

	incident (cybersecurity incident response)		
	Consider a hypothetical cybersecurity incident, identify the key legal issues which arise from it, and describe what steps need to be taken on foot of these issues	LR, SOIM	Human, Organisational and Regulatory Aspects, Attacks and Defences
Malware Analysis (5 ECTS Credits)	Learn key concepts and techniques of static reverse engineering	FMS, MAT, AC, SSL, F, LR, HS	Infrastructure Security x 2, Attacks and Defences x 2, Systems Security, Human, Organisational and Regulatory Aspects
	x86 assembly programing	OSV, FMS	Systems Security x 2
	Common code structures introduced by compilers	OSV, HS, AC, WAM, FMS, SS, SSL	Infrastructure Security x 2, Systems Security x 2, Software and Platform Security x 3
	Windows PE format	OSV	Systems Security
	Common approaches to reverse engineering using interactive disassembly and interactive debugging	FMS, MAT, AC, SSL, F, LR, HS	Infrastructure Security x 2, Attacks and Defences x 2, Systems Security, Human, Organisational and Regulatory Aspects
	Determining behavioural characteristics of a malware executable using dynamic analysis	MAT, OSV, F	Attacks and Defences x 2, Systems Security
	Practical skills with IDA Pro interactive disassembler, OllyDbg interactive debugger, Cuckoo Sandbox	MAT, F	Attacks and Defences x 2
Cybersecurity Case Study (15 ECTS Credits)	Apply cybersecurity techniques to practical security problems	RMG, NS, MAT, F, SOIM, LR	Attacks and Defences x 3, Human, Organisational and Regulatory Aspects x 2, Infrastructure Security
	Report on the results obtained	RMG, NS, MAT, F, SOIM, LR	Attacks and Defences x 3, Human, Organisational and Regulatory Aspects x 2, Infrastructure Security
	Evaluate the performance of these techniques	RMG, NS, MAT, F, SOIM, LR	Attacks and Defences x 3, Human, Organisational and Regulatory Aspects x 2, Infrastructure Security
Trends in Cybersecurity (5 ECTS Credits)	Fundamentals of Blockchain Technologies	C, AAA, POR, AC, DSS	Systems Security x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects
	Blockchain Stack, and its Core Components	C, AAA, POR, AC, DSS	Systems Security x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects
	Existing as well as emerging blockchain security use cases	C, AAA, POR, AC, DSS	Systems Security x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects
	Blockchain security and digital identity	C, AAA, POR, AC, DSS	Systems Security x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects

	Zero trust security model and applications	C, AC	Infrastructure Security, Systems Security
	Ransomware families and characteristics	SOIM, AB, LR, MAT, CPS, RMG	Attacks and Defences x 3, Infrastructure Security, Human, Organisational and Regulatory Aspects x 2
	Modern approaches to ransomware detection and analysis	MAT	Attacks and Defences
	Secure software development lifecycle and security DevOps	SSL, SOIM	Attacks and Defences, Software and Platform Security
	Review of modern security as a service technologies	FMS, AC	Infrastructure Security, Systems Security
	Review of the current research approaches on defensive AI and machine learning for cybersecurity	AC, HS, PLT, NS, POR, MAT, CPS, SS, AAA, SOIM, F	Systems Security, Infrastructure Security x 5, Attacks and Defences x 3, Human, Organisational and Regulatory Aspects, Software and Platform Security
Ethical Hacking (5 ECTS Credits)	Introduction to Ethical Hacking	SSL	Software and Platform Security
	Industry Threats	SSL, CPS, SOIM	Infrastructure Security, Attacks and Defences, Software and Platform Security
	Measuring Risk (Common Vulnerability Scoring System)	RMG	Human, Organisational and Regulatory Aspects
	SQL Injection	WAM, FMS, CPS, PLT, SSL	Infrastructure Security x 2, Systems Security, Software and Platform Security x 2
	Cross Site Scripting (XSS)	SS	Software and Platform Security
	Cross Site Request Forgery (CSRF)	WAM	Software and Platform Security
	Broken Authentication	WAM	Software and Platform Security
	Broken Authorisation	WAM	Software and Platform Security
	Bad Cryptography	C, AC	Infrastructure Security, Systems Security
	Current Trends	SSL, SOIM, RMG	Human, Organisational and Regulatory Aspects, Attacks and Defences, Software and Platform Security

Knowledge Area Emphasis	
Human, Organisational & Regulatory Aspects	
Risk Management and Governance	30
Law and Regulation	15
Human Factors	7
Privacy and Online Rights	7
Total:	**59**
Attacks & Defences	
Malware and Attack Technology	13
Adversarial Behaviours	3
Security Operations and Incident Management	18
Forensics	8
Total:	**42**
Systems Security	
Cryptography	9
Operating Systems and Virtualisation Security	5
Distributed System Security	4
Formal Methods for Security	9
Authentication, Authorisation and Accountability	10
Total:	**37**
Software and Platform Security	
Software Security	3
Web and Mobile Security	6
Secure Software Lifecycle	17
Total:	**26**
Infrastructure Security	
Applied Cryptography	18
Network Security	11
Hardware Security	4
Cyber Physical Systems	8
Physical Layer and Telecommunications Security	4
Total:	**45**

Appendix 4 – Cranfield University Cyber Defence and Information Assurance MSc (Defence)

Module Name	Learning Outcome	CyBOK KA	CyBOK Broad Category
Foundations of Cyber	Understanding business strategy, goals and objectives	RMG	Human, Organisational and Regulatory Aspects
	Understand the relationship between governance and management concepts within organisations	RMG	Human, Organisational and Regulatory Aspects
	Explain the management system concept.	RMG	Human, Organisational and Regulatory Aspects
	Develop cyber strategy to meet strategic information assurance requirements	RMG	Human, Organisational and Regulatory Aspects
	Introduction to enterprise and process architecture; definition and role in the organisation	RMG	Human, Organisational and Regulatory Aspects
	Trust and assurance	RMG, SSL	Human, Organisational and Regulatory Aspects, Software and Platform Security
	Range of requirements (people, process, IT systems, IT products)	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Legal requirements	LR	Human, Organisational and Regulatory Aspects
	Measuring IS and IA performance (metrics, KPIs).	RMG	Human, Organisational and Regulatory Aspects
	Developing policies and procedures	RMG	Human, Organisational and Regulatory Aspects
	Implementing policies and procedures	RMG	Human, Organisational and Regulatory Aspects
	Security standards including, for example, the ISO 27000 series	RMG, NS	Human, Organisational and Regulatory Aspects, Infrastructure Security
Cyber Deception	Distinguish the technical structures of information systems that facilitate successful cyber deception	AB	Attacks and Defences
	Determine the human factors associated with attacking and defending computer systems exploiting principles of cyber deception.	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Formulate the technical basis for a successful cyber deception,	AB	Attacks and Defences
	Evaluate the threats and opportunities necessary to conduct a risk assessment for the use of cyber deception	RMG, MAT, AB, LR	Human, Organisational and Regulatory Aspects x 2, Attacks and Defences x 2
	Critically appraise the use of cyber deception in relation to concepts of Effects Based Operations and deterrence.	AB, LR, AAA	Attacks and Defences, Human, Organisational and Regulatory Aspects
Critical Networks and Cyber-	Critically evaluate theories of criticality and interdependence in the context of security planning	CPS, RMG	Human, Organisational and Regulatory Aspects, Infrastructure Security

Physical Systems			
	Appraise the current state of best practice in network and security operations management in the security context	CPS, RMG	Human, Organisational and Regulatory Aspects, Infrastructure Security
	Assess the factors that facilitate or prevent effective risk management of interdependent systems in the context of critical national [sic]	CPS, RMG	Human, Organisational and Regulatory Aspects, Infrastructure Security
	Summarise the cyber risks associated with Internet of Things (IoT) devices and wider IoT ecosystems.	CPS, RMG, SSL	Human, Organisational and Regulatory Aspects, Infrastructure Security, Software and Platform Security
	Critical national infrastructure - Definitions and approaches to classifying national infrastructure and critical national infrastructure	CPS, NS, LR, RMG	Human, Organisational and Regulatory Aspects x 2, Infrastructure Security x 2
	Critical national infrastructure - The global, national and organisational view of national infrastructure	CPS, NS, LR, RMG	Human, Organisational and Regulatory Aspects x 2, Infrastructure Security x 2
	Critical national infrastructure - Frameworks for identifying and managing cyber risk in critical national infrastructure	CPS, NS, LR, RMG, AB	Human, Organisational and Regulatory Aspect x 2s, Attacks and Defences, Infrastructure Security x 2
	Cyber Physical Systems - Characteristics of cyber-physical systems and the inherent security and privacy concerns	CPS, NS, LR, RMG, POR	Human, Organisational and Regulatory Aspects x 3, Infrastructure Security
	SCADA and OT - The differences between OT and IT	CPS	Infrastructure Security
	SCADA and OT - The technical and socio-technical elements to managing the cyber risk of Supervisory Control and Data Acquisition (SCADA) systems	CPS, HF, RMG	Human, Organisational and Regulatory Aspects x 2, Infrastructure Security
	IoT and smart technologies - IoT devices and wider supporting ecosystems	CPS, NS	Infrastructure Security x 2
	IoT and smart technologies - Frameworks to support the identification and management of cyber risk associated with the Internet of Things deployed in smart homes, smart cities and smart grids.	RMG, CPS, NS, SSL	Human, Organisational and Regulatory Aspects, Infrastructure Security x 2, Software and Platform Security
	Strategic effects - How critical networks are targeted to deliver strategic outcomes by malicious actors	CPS, AB	Attacks and Defences, Infrastructure Security
	Strategic effects - Links to the strategic context.	-	
Cyber Attacks – Threats and Opportunities	Understanding cyber crime, cyber attack and cyber war	AB, LR, F	Attacks and Defences x 2, Human, Organisational and Regulatory Aspects
	The different categories of threat actors and their motivations	AB	Attacks and Defences
	How cyber fits within an organization.	RMG, LR, SOIM	Human, Organisational and Regulatory Aspects x 2, Attacks and Defences

	An overview of common cyber attacks, for example, SQL injection, XSS, and enumeration	F, AB, MAT	Attacks and Defences x 3
	Explanation of how these attacks can be mitigated, including the use of penetration testing	F, AB, MAT, SSL, NS, SOIM	Attacks and Defences x 4, Infrastructure Security, Software and Platform Security
	Understanding the human aspects of vulnerabilities, for example, insider threat and social engineering.	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Understanding the different tools available, and their application. For example, IDS systems, authentication methods, and encryption	CPS, NS	Infrastructure Security x 2
Cyber Law	The range of different legal regimes that need to be considered when planning or conducting offensive cyber operations	LR	Human, Organisational and Regulatory Aspects
	The applicable legal framework for intelligence operations, military operations, information operations and propaganda	LR	Human, Organisational and Regulatory Aspects
	The obligations provided through customary international law, international humanitarian law and domestic legislation that need addressing when considering a cyber operation.	LR	Human, Organisational and Regulatory Aspects
	The implication of conducting cyber operations in a range of different contexts, considering cyber as part of a military campaign, prior to the declaration of war and against non-state actors. The applicability of the Laws of Armed Conflict will be explored when considering cyber operations.	LR	Human, Organisational and Regulatory Aspects
	Concepts including: sovereignty, right to self-defence, espionage, sabotage, subversion, intelligence, ius ad bellum, ius in bello, armed attack, threat or use of force, necessity, proportionality, distinction, targeting, perfidy, ruse and state responsibility.	LR	Human, Organisational and Regulatory Aspects
	The various proposed legal frameworks for cyber operations and assess their suitability to support operational planners	LR	Human, Organisational and Regulatory Aspects
Data Led Decision Support and Artificial Intelligence	Machine Learning and Artificial Intelligence	AC, HS, PLT, NS, POR, MAT, CPS, SS, AAA, SOIM, F	Infrastructure Security x 4, Attacks and Defences x 3, Human, Organisational and Regulatory Aspects, Software and Platform Security
	Data mining pipeline	POR	Human, Organisational and Regulatory Aspects
	Big Data models for exploring data	LR, POR, SOIM, DSS	Systems Security, Human, Organisational and Regulatory Aspects x 2, Attacks and Defences
	Data Science	F	Attacks and Defences

Emerging Technology Monitoring	Horizon scanning	RMG	Human, Organisational and Regulatory Aspects
	Predictive methods	CPS	Infrastructure Security
	Strategic assessment of new technologies	RMG	Human, Organisational and Regulatory Aspects
	Evaluation	-	
	Maintaining personal awareness.	HF	Human, Organisational and Regulatory Aspects
	A selection of currently relevant technologies will be studied.	-	
Systems Thinking for Organisational Viability	Adapting to change in complex environments	-	
	Representing and navigating complexity	-	
	Systems methods including Soft Systems Methodology, the Viable Systems Model and Critical Systems Heuristics	-	
	Organisational dynamics and change	-	
	Monitoring and adapting	HF, RMG	Human, Organisational and Regulatory Aspects x 2
	Anticipating future requirements	-	
	Dealing with disruptive and novel technologies, events and emergent changes	RMG, HF	Human, Organisational and Regulatory Aspects x 2
Information Operations	Elaborate the main elements and key management issues in the conduct of Information Operations	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Evaluate theories of behavioural and social change relevant to Information Operations.	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Formulate the behaviour change effects sought through Information Operations	HF	Human, Organisational and Regulatory Aspects
	Recommend alternate courses of action based on self evaluation, evaluation of the target audience, and the needs of the primary decision makers in the planning process	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Critically examine behavioural change techniques used in military and other domains, with respect to their implicit treatment of causation. Where ‘other domains may include; health education, marketing, offender rehabilitation, mine awareness campaigns, weapons amnesties, mass civilian evacuations, and crime prevention.	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
Incident Management	Incident identification - the role of the security operations centre	SOIM	Attacks and Defences
	Incident identification - intrusion detection methods and tools.	NS, SOIM	Infrastructure Security, Attacks and Defences
	Incident containment - intrusion management	SOIM	Attacks and Defences

	Incident containment - intrusion analysis, monitoring and logging	SOIM	Attacks and Defences
	Incident containment - evidence preservation	F	Attacks and Defences
	Incident management - backup management	SOIM	Attacks and Defences
	Incident management - disaster recovery techniques	RMG, SOIM	Human, Organisational and Regulatory Aspects, Attacks and Defences
	Incident management - business continuity management	SOIM	Attacks and Defences
	Incident management - stakeholder management	FMS, HF, RMG	Human, Organisational and Regulatory Aspects x 2, Systems Security
Social Technologies	What are social technologies and media?	AB, WAM	Attacks and Defences, Software and Platform Security
	Development and horizon scanning	RMG	Human, Organisational and Regulatory Aspects
	Asocial interaction		
	E-inclusion and the citizenship agenda	-	
	Other uses of social media – education, scenario planning, simulation and design social technologies and security	AB, WAM	Attacks and Defences, Software and Platform Security
	Impact on productivity and working practices	-	
	Understanding generational differences	HF	Human, Organisational and Regulatory Aspects
	Mobility and pervasiveness	POR, F	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Security awareness and policies	RMG, HF	Human, Organisational and Regulatory Aspects x 2
	Social networks and information exploitation	AB	Attacks and Defences
	Personas, identity, privacy and anonymity	POR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Information leakage	POR	Human, Organisational and Regulatory Aspects
	Social marketing	AB, WAM, HF	Attacks and Defences, Human, Organisational and Regulatory Aspects, Software and Platform Security
	Persuasive technologies	-	
	Terrorism and social media	AB, HF, LR	Attacks and Defences, Human, Organisational and Regulatory Aspects x 2
	Social mobilization	AB, HF	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Two-way communication and dialogue	-	
	Second life and alternative worlds	-	
	Social technologies and intelligence	AB, MAT	Attacks and Defences x 2
	Open source exploitation	AB, MAT	Attacks and Defences x 2
	Data analytics & big data driving behavioural profiling	HF, DSS	Systems Security,

			Human, Organisational and Regulatory Aspects
	Automated tools and techniques	MAT	Attacks and Defences
	Challenges for situational awareness	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
The Human Dimension	End user behaviour	LR, HF	Human, Organisational and Regulatory Aspects x 2
	Human error (at an individual level).	HF	Human, Organisational and Regulatory Aspects
	The importance of context	-	
	Human error (at an organisational/systems level)	HF, RMG	Human, Organisational and Regulatory Aspects x 2
	Circumventing security	LR, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	The role of the security specialist.	FMS	
	Behaviour change	HF, AB	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Awareness and training for cyber security	HF	Human, Organisational and Regulatory Aspects
	Designing security mechanisms for and with the end user.	HF, SSL	Human, Organisational and Regulatory Aspects, Software and Platform Security
Understanding Risk	History of hacking	HF	Human, Organisational and Regulatory Aspects
	Threat landscape	F, LR	Attacks and Defences, Human, Organisational and Regulatory Aspects
	Cyber Security Risk Management in Practice - basic principles	RMG	Human, Organisational and Regulatory Aspects
	Legislation and standards	LR	Human, Organisational and Regulatory Aspects
	Risk management approaches	RMG	Human, Organisational and Regulatory Aspects
	Strategies for managing risk.	RMG	Human, Organisational and Regulatory Aspects
	Quantifying risk in a complex environment	RMG, LR	Human, Organisational and Regulatory Aspects x 2
	Risk economics	RMG	Human, Organisational and Regulatory Aspects
	Social dimension of risk	HF, RMG	Human, Organisational and Regulatory Aspects x 2
	Risk communication	HF, RMG	Human, Organisational and Regulatory Aspects x 2

Knowledge Area Emphasis	
Human, Organisational & Regulatory Aspects	
Risk Management and Governance	41
Law and Regulation	22
Human Factors	28
Privacy and Online Rights	7
Total:	**98**
Attacks & Defences	
Malware and Attack Technology	7
Adversarial Behaviours	26
Security Operations and Incident Management	11
Forensics	8
Total:	**52**
Systems Security	
Cryptography	0
Operating Systems and Virtualisation Security	0
Distributed System Security	2
Formal Methods for Security	2
Authentication, Authorisation and Accountability	2
Total:	**6**
Software and Platform Security	
Software Security	1
Web and Mobile Security	3
Secure Software Lifecycle	5
Total:	**9**
Infrastructure Security	
Applied Cryptography	1
Network Security	11
Hardware Security	1
Cyber Physical Systems	16
Physical Layer and Telecommunications Security	1
Total:	**30**

Appendix 4 – CIS Corps Cyber SME Questionnaire and Responses

1. Please enter a brief description of your education, certification and/or role(s) in a cyber/IT-related field.					
The following Knowledge Areas (KAs) are within the field of ***Human, Organisational & Regulatory Aspects*** *of cybersecurity. For each KA, please rate 5 as very important and 1 as not important* ***for a cyber CIST****. Remember not to confuse this with the role of a CIS Officer.* More detail here if required.					
2. Risk Management and Governance	1 (not important)	2	3	4	5 (very important)
3. Law & Regulation	1 (not important)	2	3	4	5 (very important)
4. Human Factors (Cybersecurity awareness, Minimising human error, Positive attitude, Stakeholder engagement, etc.)	1 (not important)	2	3	4	5 (very important)
5. Privacy & Online Rights (engineering and protecting systems that inherently protect users' privacy)	1 (not important)	2	3	4	5 (very important)
The following Knowledge Areas (KAs) are within the field of ***Attacks and Defences****. For each KA, please rate 5 as very important and 1 as not important* ***for a cyber CIST****. Remember not to confuse this with the role of a CIS Officer.* More detail here if required.					
6. Malware and Attack Technologies	1 (not important)	2	3	4	5 (very important)
7. Adversarial Behaviours (malicious operations happening on the Internet today)	1 (not important)	2	3	4	5 (very important)
8. Security Operations and Incident Management	1 (not important)	2	3	4	5 (very important)
9. Forensics	1 (not important)	2	3	4	5 (very important)
The following Knowledge Areas (KAs) are within the field of ***Systems Security****. For each KA, please rate 5 as very important and 1 as not important* ***for a cyber CIST****. Remember not to confuse this with the role of a CIS Officer.* More detail here if required.					
10. Cryptography (formal mathematics, not focusing on applications)	1 (not important)	2	3	4	5 (very important)
11. Operating Systems and Virtualisation Security	1 (not important)	2	3	4	5 (very important)
12. Distributed Systems Security (geo-dispersed computing and communications including blockchain, peer-to-peer and cloud)	1 (not important)	2	3	4	5 (very important)
13. Formal Methods for Security (foundations, methods and tools,	1 (not important)	2	3	4	5 (very important)

based on mathematics and logic, for rigorously developing and reasoning about computer systems, whether they be software, hardware, or a combination of the two)	
14. Authentication, Authorisation and Accountability (access control, audit logs, web authentication protocols, etc.)	1 (not important) 2 3 4 5 (very important)
The following Knowledge Areas (KAs) are within the field of ***Software and Platform Security***. *For each KA, please rate 5 as very important and 1 as not important* ***for a cyber CIST***. *Remember not to confuse this with the role of a CIS Officer*. More detail here if required.	
15. Software Security	1 (not important) 2 3 4 5 (very important)
16. Web & Mobile Security	1 (not important) 2 3 4 5 (very important)
17. Secure Software Lifecycle	1 (not important) 2 3 4 5 (very important)
The following Knowledge Areas (KAs) are within the field of ***Infrastructure Security***. *For each KA, please rate 5 as very important and 1 as not important* ***for a cyber CIST***. *Remember not to confuse this with the role of a CIS Officer*. More detail here if required.	
18. Applied Cryptography (broad introduction to the field of cryptography, focusing on applied aspects of the subject)	1 (not important) 2 3 4 5 (very important)
19. Network Security	1 (not important) 2 3 4 5 (very important)
20. Hardware Security	1 (not important) 2 3 4 5 (very important)
21. Cyber Physical Systems (engineered systems that are built from, and depend upon, the seamless integration of computation, and physical components - including cybersecurity of critical infrastructure etc.)	1 (not important) 2 3 4 5 (very important)
22. Physical Layer and Telecommunications Security	1 (not important) 2 3 4 5 (very important)

CIS Corps Cyber SME Questionnaire Responses

		SME 1	SME 2	SME 3	SME 4	SME 5	SME 6
Human, Organisation & Regulatory Aspects	RMG	5	2	5	5	3	2
	LR	2	1	5	3	3	3
	HF	4	4	5	5	4	2
	POR	2	4	4	2	3	4
Attacks & Defences	MAT	4	5	5	5	4	4
	AB	4	5	4	4	5	4
	SOIM	5	5	5	3	5	5
	F	2	4	4	5	5	4
Systems Security	C	1	3	3	2	2	2
	OSV	4	5	4	5	4	3
	DSS	3	3	3	5	3	3
	FMS	3	3	5	3	4	4
	AAA	5	4	5	4	4	5
Software & Platform Security	SS	3	4	2	4	3	3
	WMS	4	4	4	5	4	3
	SSL	2	3	2	2	2	3
Infrastructure Security	AC	2	2	4	3	4	1
	NS	5	4	5	5	5	4
	HS	5	3	5	5	5	4
	CPS	5	2	4	4	5	3
	PLT	5	4	3	5	5	3

Standardised Broad Category Emphasis

	SME 1	SME 2	SME 3	SME 4	SME 5	SME 6
Human, Organisation & Regulatory Aspects	2.95	3.16	4.52	3.41	2.71	3.24
Attacks & Defences	4.09	5	4.29	3.86	3.96	5
Systems Security	3.64	4.74	4.76	4.32	3.54	5
Software & Platform Security	2.05	2.9	1.9	2.5	1.88	2.65
Infrastructure Security	5	3.95	5	5	5	4.41