School of Science, Engineering and Environment

DEVELOPING A DIGITAL COMPETENCE FRAMEWORK FOR UAE LAW ENFORCEMENT AGENCIES TO ENHANCE CYBER SECURITY OF CRITICAL PHYSICAL INFRASTRUCTURE (CPI)

By

Mohamed Alhajeri

Supervisor

Prof. Zeeshan Aziz

Abstract

Critical Physical Infrastructures (CPI) are assets and systems that are vital to the health, safety, security, and economic or social well-being of people, and have become increasingly vulnerable to cyberattacks that have the potential to cause severe debilitating and destructive impact on a nation’s economic security or public health and safety. The United Arab Emirates (UAE) has experienced a high level of cyberattacks targeted at its critical physical infrastructure which has also undergone rapid modernisation, digitisation and interconnection of systems that could expose it to potential vulnerabilities in cyberspace. This thesis addresses a major challenge in the capacity of law enforcement to address cyberattacks in respect of the digital capabilities that are necessary to maintain pace with technologies and respond effectively in a digital environment. The purpose of this study is to develop a digital competences framework for UAE law enforcement agencies to combat cyber security threats facing CPI. This identifies the key functions and role of law enforcement and prioritises primary domains and elements of digital competency for cyber security that are critical for law enforcement to perform its role in protecting CPI. A holistic case study design using multiple methods to generate qualitative and quantitative data is adopted. A Delphi method is applied over multiple stages aimed at achieving consensus among experts and professionals using open and semi-structured interviews, analytical hierarchy process (AHP), quantitative survey and group building methods. The sample consists of 25 experts from different law enforcement organisations and from different roles and different levels of the organisation. The findings present a digital competency framework for cybersecurity of CPI which models a holistic socio-technical approach and evaluation of digital competency requirements in line with the different functions and roles of law enforcement. Digital competency is conceptualised as an interplay of multiple interconnected dimensions including balance, type and relevance of training and future proofing. The highest ranked digital competencies for law enforcement to protect CPI are identified as Investigate, Analyse, Collect and Operate and Protect and Defend. The three highest ranked specialty areas are Cyber Investigation, Digital Forensics and All-Source Analysis. Cybercrime Investigator, Law Enforcement/Counterintelligence Forensics Analyst, and All-Source Analyst are the highest ranked work roles. The framework identifies knowledge skills and ability competencies for each of these domains. This study makes a novel contribution to theory of digital competency in identifying and prioritising key factors and processes for the design and implementation of digital competency development. The study prioritises the competences and speciality areas of digital competency and the associated knowledge, skills and abilities (KSAs) in the area of law enforcement for enhancing security of CPI.

Acknowledgements

Thank you to my supervisor for providing guidance and feedback throughout this project. I am grateful for the support of my family during the course of my research and for believing and encouraging me.

Table of Contents

Glossary of terms

ADNOC	Abu-Dhabi National Oil Company
ACPO	Association of Chief Police Officers
CIP	Critical Infrastructure Protection
CPI	Critical Physical Infrastructure
CIIPP	Critical Information Infrastructure Protection Policy
CICPA	Critical Infrastructure & Coastal Protection Authority
GCI	Global Cyber security Index
GMB	Group Model Building
Iaas	Infrastructure as a Service
IAS	Information Assurance Standards
IA	Information Assurance
ICS-CERT	Industrial Control Systems Emergency Response Team
LEA	Law Enforcement Agencies
NIAF	National Information Assurance Framework
NICE	National Initiative for Cybersecurity Education
NCSS	National Cyber security Strategy
NCCIC	National Cyber Security & Communications Integration Centre
PCeu	Police Central e-Crime Unit
Paas	Platform as a Service
Saas	Software as a Service
TCA	Thematic Content Analysis
TRA	Telecommunications Regulations Authority
UAE	United Arab Emirates

List of Tables

List of Figures

Chapter 1 Introduction

1.1 Research Background

Critical national infrastructure such as power, water, or waste installations, airports and ports, oil storage and refineries, hospitals and key government installations is the backbone of any country's security and economy. Rapid technological development and the pervasive role of the Internet cyberspace touches on every facet of modern life (Willits and Nowacki, 2016). The growth in the use of the Internet and increasingly interconnected networks coincides with increasing threat and risk of cybercrimes on individuals, organisations and national and critical infrastructures (Johnson, 2014). Over decades critical infrastructures (CI) consisting of organisational and physical structures and facilities that are vital to nations' social and economic functioning have been subject to technological change.

Increasing digitalisation means that cyber security is emerging as a major issue for critical infrastructures (Gjesvik, 2019). Inter-connected computers and industrial control systems are at the heart of operating critical physical infrastructure (CPI), allowing for centralised monitoring and remote operations and maintenance. Cyberspace is the sphere in which operations across all different fields of personal and public life are conducted and interconnect (Galik and Tolnaiova, 2020).

1.1.1 Cyber Security Threat to Critical Infrastructure

Cyberattacks on CPI are able to inflict major impacts and incapacitate physical and economic security and health and safety at national levels. All different CPI systems for power, water, health, defence, manufacturing, and transportation have become increasingly interconnected and vulnerable to cyberattacks. CPIs have been subject to increasingly frequent and intense disruptions and hazards originating with cyber-physical systems and systems-of-systems, that includes the Internet of Things (IoT) (Bogdanoski et al., 2019).

The protection of CPIs is a matter of national security and an issue attracting increased attention from governments and law enforcement and security agencies (Enisa, 2019; Bate, 2017). This is because CPIs around the world are victims of a rising incidence of cyberattacks ranking as the fifth highest economic risk in 2020 (WEF, 2020). CPIs are under threat of attack through different areas and levels of technologies: device/IoT, network level, system, applications, data or user level (Kohnke et al., 2019). Attacks can be boundaryless and a single cyberattack can result in paralysis of CPI or data breaches and impact victims in multiple jurisdictions.

The potential impact of cyberattacks on a nation's CPI can be even more significant than conventional terrorist attacks (Lin, 2016). Cyberattacks can cause significant economic damage and threaten public safety and security. In recent years CPI across all sectors and around the world has faced disruption and damage as cyberattacks caused partial or full shutdown or disabling of systems affecting health, power, water and causing serious threat to life. Cyberattacks have halted air traffic (Haugli et al., 2019), disrupted the functioning of health systems and the daily delivery of health care and surgeries (Wiedeman, 2019), impeded commerce and business at global level (Greenberg, 2018) and have provoked temporary power outages (Gjesvik, 2019; FireEye, 2018).

Examples show the extent to which cyberattacks can threaten critical physical infrastructure. In 2021 the Irish health system suffered a ransomware attack that severely disabled key Health Service Executive systems and necessitated the shutdown of the majority of its other systems. In 2017 the 'WannaCry' ransomware attack on the UK NHS disrupted a third of English NHS trusts resulting in cancelled appointments and medical operations (Rees, 2021). In 2020 cyberattacks on European energy infrastructure caused temporary shutdowns of power systems and produced major economic disruption and life-threatening impacts to medical systems (Owaida, 2020). Moreover spear phishing attacks on power distribution companies in one European country resulted in disruption of the power grid that affected more than 200,000 people, left 8 provinces without power and physically degraded operational systems (ECSO, 2018).

1.1.2 Critical Infrastructure in the UAE

Cyberattacks on critical physical infrastructure are increasingly a threat to the security of the Middle East. In this region the oil and gas sector and CPIs are a major target accounting for half of all cyberattacks. In 2019 an oil company in the United Arab Emirates (UAE) was the focus of Shamoon 3, a malware attack that deleted and overwrote files and systems (Murphy, 2020). In January 2021 UAE telecom companies and internet service providers were hacked and data was stolen by a cyberespionage group linked to Hezbollah (CSIS, 2021).

For the UAE the protection and safeguarding of its growing and evolving CPIs has become an issue of paramount importance for national security and safety. The country has increasingly emerged as a popular and attractive target for cybercriminals as a result of its strong economic growth and activity, widespread adoption of technology, high levels of tourism and the development of the oil and gas sector (Rajan et al., 2017). The UAE has increasingly become a gateway hub for trade and travel both in the Middle East and worldwide. Due to these factors the country is the second-most targeted nation globally for cybercrime with an increasing level of attacks against infrastructure (digital14, 2021). Industry reports show for example that a 4% increase in cyberattacks on the UAE's Industrial Control Systems (ICS) in 2021 is considerably greater than the 1.2% increase experienced by the rest of the world (Zawya, 2021).

All the seven emirates of the UAE have undergone rapid economic development and urbanisation. Major private, commercial and infrastructure construction projects and mega projects in all sectors have implications for the built environment and the expansion of critical infrastructures (Al-Shihri, 2016; Jamil et al., 2016). The UAE context in respect of CPI is evolving rapidly due both to urbanisation and a modernisation programme that has resulted in a process of rapid and comprehensive adoption of technology in which infrastructures and government services are substantially digitised, smart cities are highly interconnected and internet and smartphone penetration rates are among the world's highest (UAE Gov, 2021; eMarketer, 2019). This has included the expansion and digitisation of critical physical infrastructures and systems. There has been significant development in health, water and electricity, financial, chemical, transport, nuclear, and oil and gas infrastructures accompanied by new installations and systems that have yet to be fully tested and secured. This underlines that despite rapid modernisation the country remains under-developed in certain areas and compared to more developed nations such as the US and Europe cybersecurity and protection remains in its infancy. The Middle East and UAE are still vulnerable and evolving and there is an imperative to develop the competencies of law enforcement for the protection of CPI.

The UAE further inhabits a volatile and fragile geo-political context geopolitical context that has implications for cybersecurity and law enforcement protection of CPI. The importance of the UAE regionally and globally suggests that critical damage to its infrastructure would have significant implications for the rest of the world. Evidence shows that the UAE is experiencing significant pressures from cyberattacks driven by nation states for economic and political purposes (digital14, 2021) and on CPI leading to espionage and disruption to public life and which pose a potent threat to national security. Development of these CPIs has relied on foreign involvement and an immigrant workforce, potentially increasing vulnerabilities. Moreover general issues exist of aging and decaying infrastructure and the adaptation required to meet modern standards. To mitigate the threats and risks of cyberattacks in the future, there is a need in the UAE for a framework which could enhance the development of digitally competent professionals capable of managing and securing reliable digital infrastructures effectively (Al Neaimi et al., 2015).

1.1.3 Law Enforcement and Cyber Security of CPI

The threat to CPI underscores the capacity of law enforcement to respond effectively. The role of law enforcement and the development of competencies in cyber security skills is viewed as a critical dimension to protection of CPIs (Robertson, 2019; Nowacki and Willits, 2019). Cybercrime is increasing in size and scope across the globe and rapidly creating new and changing forms of crime. Cyberspace represents a major opportunity for criminals to launch attacks against a nation’s critical physical infrastructure (Cavelty et al., 2016; Brown et al., 2006). Law enforcements’ ability to protect CPI is dependent on maintaining pace with the evolving cybercrime and threat landscape. Improving the capabilities and understanding of skills required of law enforcement agencies in order to effectively combat physical and cyber threats facing national infrastructure is recognised as a major imperative.

The scope of awareness, skills and knowledge required for cyber security is vast, multidimensional, layered and complex (Cavelty et al., 2016; Deibert and Rohozinski, 2010). Tackling the problem of cybercrime in the UAE and around the world is linked to the imperative to develop a digital competence framework for UAE enforcement agencies especially in regards to critical physical infrastructure. Law enforcement needs to be responsive and competent so as to be able to counter threats against national and critical infrastructures and effectively investigate and prevent cybercrime (Robertson, 2019; Bossler and Holt, 2012).

1.2 Research Rationale

Cybercrime poses a range of problems for police organisations. A major issue is deepening understanding of the best way to develop key knowledge and skills in relation to cybercrime across the organisation to ensure the appropriate responses to cybercrime incidents from police officers. There is a strong rationale for the development of a digital competency (DC) framework. Current research and practice remain fragmented and unclear in defining digital competences and establishing key dimensions that are required for law enforcement to prevent and investigate cybercrime both in general and in relation to CPI.

In particular there exists no detailed framework or reference that enables practitioners to understand the type of skills needed to develop law enforcement. Much research has identified the relation between law enforcement and technology (Wall, 2015; Faith and Bekir, 2015; White and Escobar, 2008; Nuth, 2008). Other studies stress the link between advancements in technology and crime (Custers, 2012; Wexler, 2012; Savona and Mignone, 2004). Nuth (2008, p.443) argues that development of digital technology has driven police into a “crime technology race” where both criminals and police utilise technology to obstruct the other side.

Moreover in research and practice there remains limited understanding of the relationship between digital capabilities and law enforcement roles. There is growing acceptance among law enforcement globally that there are insufficient skills and knowledge, training and resources to identify, understand and respond to the increasing challenges posed by cybercrime and the additional implications of cybersecurity (Hunton, 2012, p. 225). Cyber security is a highly multifaceted and often subjective discipline, and the absence of universally accepted definitions and competencies underscore the need for a methodological approach to explore and validate digital competencies.

Cybercrime is an increasing global challenge for which police require training to enable an effective response, and identifies incidences in which a computer is employed in carrying out a crime or is the crime target itself. Without necessary digital competencies law enforcement will be less effective in addressing cybercrime. It is important to provide recognised behaviours and values and establish a consistent foundation for development and raise standards and capabilities for law enforcement. Although consensus exists in relation to the requirement to develop and strengthen law enforcement digital competencies, until now this has not been reflected in the priorities of governments for capacity building.

The driving force of technology and the digitisation of CPI underscores the importance of developing the digital capabilities of law enforcement. The problem context emphasises the need to develop attitudes, knowledge and skills for cyber security across law enforcement to engender necessary levels of expertise organisation-wide to address the challenges of cybercrime. There is a requirement for a law enforcement skilled in cyber security to address the unique cyber security needs of critical infrastructure. This recognises that given the evolution of technology and cyber threats police need to persist in the adaptation, design, implementation, maintenance and continuous improvement of cyber security practices (Newhouse et al., 2017). Digital competency represents an integral facet for maintaining pace with innovations in technology impacting cybercrime and the methods and operations of cybercriminals.

To comprehend the consequences and complex issues linked to the development of digital competence, a detailed mapping of available resources and skills training needs across different cyber technical disciplines is imperative (Hunton, 2012). The digital competences needed for future operational functioning are likely to be framed as multi-disciplinary, multi-skill, and multi-agency (Hunton, 2012). This provides the rationale for the multi-faceted approach applied in this research that links training and digital competences in the context of the UAE police force to propose a framework. Recent research has identified five key technical roles for police departments to consider: technical domain expert, technical enquirer, network investigator, digital forensic examiner and forensic technician (Hunton, 2012). Few studies have examined this topic in the context of UAE law enforcement which underscores the need to investigate further to understand the technical roles, competencies and knowledge required in this context (Hunton, 2012). There is a strong rationale for conducting this research in the UAE. Like many aspects of UAE society critical physical infrastructure has undergone rapid modernisation, digitisation and interconnection of systems that in turn represent potential vulnerabilities. This links further to the level of cybersecurity and protection in the country which remains under-developed in comparison with developed nations. Compounding this issue the UAE is one of the most highly targeted countries in the world for cyberattacks (digital14, 2021) with assaults on infrastructure and industrial control systems higher than global averages (Zawya, 2021). This situation is not helped by limited analysis or empirical evidence in the area of developing digital competence within the UAE context, and even less in terms of cybersecurity and the protection of CPI. This points to a critical need for additional research in safeguarding CPI within UAE against growing threats of cyberattacks.

Governments and law enforcement are experiencing major challenges in responding to cybercrime and safeguarding CPI. There is an imperative for the development of digital competencies that underpin capabilities for investigation and attribution and stimulate novel operating practises. It is necessary to address this issue through more education and training in cybercrime. However there is a need for greater transparency and consistency for required practitioners for digital competence development that can be addressed by a DC framework which can provide impetus and focus for the development of all-round skills of law enforcement personnel in their specific roles. To date cyber security curricula have been challenged to maintain pace, predominantly due to a lack of structure and systems to rapidly integrate new content in response to developing threats or needed skills (ENISA, 2019). A DC framework will support the law enforcement training curriculum and provide greater clarity and support in the design of programmes to provide more comprehensive and unified knowledge and skills that law enforcement should develop.

There is also significant rationale to provide policy and strategists with a comprehensive understanding of digital competencies for law enforcement to promote awareness and understanding that has been validated. A proposed framework in the UAE should take into consideration not only adoption but also training for technological engagement within the police workforce (Willits and Nowacki, 2016). It is necessary to acquire digital capabilities beyond specialised units to ensure that personnel across all divisions and levels are able to perform effectively in the digital environment. A competency framework can establish foundation for creating in law enforcement officers broad cybercrime knowledge and addressing deficiencies in the cyber workforce. Further, it is necessary to provide clarity on specific requirements for DC for law enforcement roles that is necessary to raise the level of digital competence among all law enforcement personnel and address skills shortages.

1.3 Research Problem

Despite the significance of developing digital competences of enforcement agencies, few attempts have been made to undertake rigorous analysis with empirical evidence in this area within the UAE context. Governments have trailed behind the evolution of cybercrime in their capacity to stop or prevent cyberattacks and the extent to which they are able to ascribe crime to cybercriminals and ensure they meet justice, generating a gap in cyber enforcement worldwide (Nowacki and Willits, 2019). Law enforcement faces a major challenge in ensuring cyber security competencies at organisational level to effectively combat cybercrime in general and in relation to the protection of critical physical infrastructure (CPI).

The problem context that underpins the motivation and goal of this study is characterised by a number of issues that underline the need for a digital competency framework that supports the capabilities of the police to effectively respond to cyber threats to CPI. To address these research questions this research aims to develop a digital competences framework for UAE law enforcement agencies to combat cyber security threats facing the UAE’s critical physical infrastructure

Cyber security skills globally and across all sectors are in crisis where demand for such skills significantly exceeds supply and a skills gap is evident in the CPI sector

(Enisa, 2019; UK Gov, 2018). It is evident that law enforcement faces challenges in recruiting the necessary skills. Of all the sectors in the labour market cyber security is one of the most constricted. The Cybersecurity Workforce Study (ISC2, 2021) shows that globally there are 4.19 million cyber security professionals however a further 2.72 million are needed with growth of 65% required in the cyber workforce to address the demands of the labour market. Results indicate that nearly 65% of organisations surveyed are deficient in the staff needed for cyber security tasks and a lack of experienced and skilled cyber security personnel is a major issue (ISC2, 2021).

This skills gap is more acute in law enforcement where competencies remain largely embedded in traditional law enforcement skills. This skills shortage places stress on organisational training and development to increase officers' levels of digital competencies and develop core specialists' competencies to address different types of cybercrime. Cybercrime is steadily increasing and existing technical models to address cybercrime appear to be ineffective in countering its growth. Cybercrime trends indicate a growing aggressiveness and willingness to confront targets. Rapid societal digitalisation, which has increased with the advent of the Covid-19 pandemic, generates new vulnerabilities able to be utilised by criminals conducting their activities online. Cyberattacks such as ransomware, the generation and dissemination of malware, theft of sensitive personal or industry data through hacking, and denial of service (DoS) attacks, have risen in recent years both in number and level of complexity (EU, 2021).

Further, the increasing complexity and interconnectedness of information and technology, incorporating operational technologies, represents a major challenge to plainly describe the work being conducted or desired to be achieved. The response of law enforcement agencies to cybercrimes has been made more difficult by issues of jurisdiction, budget and training, and interest among police management (Nowacki and Willits, 2019; Holt et al., 2015). Cybercrime is in a stage of infancy and its rapid and evolving nature is associated with minimal consensus of the definition and parameters of cybercrime that makes it difficult for organisations to identify and address the demand for skills (Schreuders et al., 2018; Vogel, 2016).

In the United Arab Emirates (UAE) while the government has brought in modifications to its sole law on cybercrime there exist concerns over its ability to provide adequate protections (Rajan et al., 2017). This concern is not unique to the UAE as there is consensus that law enforcement and the criminal justice system is ill prepared to address cybercrime globally (Joshi, 2015; Peachy, 2014). Enforcement agents often find themselves disadvantaged due to lack of clarity in regards to governance of interconnected threats, leading to the need to enhance understanding of the nature of interdependence and cooperativeness of governments and law enforcement agencies at regional and global levels (Cavelty et al., 2016; Deibert and Rohozinski, 2010).

Additionally, due to the nature of cyber networks as cross border/transnational organisms, the issue of security and governance of such networks requires supra national solutions (Cavelty et al., 2016; Deibert and Rohozinski, 2010). The above supra national/transnational solutions for cyber defences appear to still be ‘grey areas’ with need for further documented empirical studies, especially in Middle Eastern countries (Alneaimi, 2016). This research therefore is long overdue and as the Global Cybersecurity Index 2018 has identified, the issue of capacity building and in particular education and training programs for public sector agencies such as law enforcement have been under researched or given less priority.

The complexity of cybercrime, the evolving nature and the threat landscape creates a major challenge for law enforcement to maintain pace and achieve the necessary level of competency across all areas to sufficiently counter the threats to CPI. A key challenge lies in understanding and maintaining pace with developments (Nowacki, and Willits, 2019). As criminals adapt and capitalise on the opportunities provided by new technologies police forces are also under pressure to continually innovate and change and update to address different forms of criminal innovation. Responding effectively to criminal innovation and use of technology to commit crime is rapidly becoming a key priority, driving a need to keep pace with emerging technologies, new crimes and a dynamically changing threat landscape (Europol, 2018).

Thus a wide range of criminal innovation represents a major impetus for police innovation to counter new forms of crime. The development of new technologies has provided a major incentive for criminal innovation to create new crimes and adapt traditional crime techniques and radically altering criminal practices. One of the notable characteristics of criminal innovation acknowledged by leading law enforcement agencies is the high degree of flexibility and adaptability of individuals and groups perpetuating crime and the speed at which they can identify new opportunities, victims or evade detection or countermeasures (Europol, 2019). Technology has unlocked new avenues for criminals to commit crime through innovations that maximise revenues from crime, operate more efficiently and minimise risks and risk of detection (Europol, 2018).

In addition to the external context of cybercrime, internally a number of organisational issues in law enforcement has constrained the development of digital competencies resulting in a lack of consistency and coherence in overall capability to respond to cybercrime. The relationship between technology and law enforcement has traditionally been complex and occasionally contentious (Heal at al., 2016; Fatih and Bekir, 2015). Criminals appear able to take advantage of new technologies more rapidly than police whose ability to adapt to technological advances is more constrained (Robertson, 2019).

In particular existing training for police is ill prepared to address the needs of digital societies (House of Commons, 2018; Timpf, 2014). According to needs assessment research for police the most widespread need is training and knowledge in digital technologies (Cockcroft et al., 2018). Conversely evidence shows that technological competencies are frequently not a recognised part of police training (Cockcroft et al., 2018; Koksal, 2009). White and Escobar (2008) identified the need for police agencies to improve their current training curricula to ensure officers possess the knowledge and skills to utilise digital technologies effectively.

Against this knowledge gap, law enforcement agencies are failing to offer the correct quantity and depth of training which is impeding both the development of a continuous pipeline within agency workforces and the professional development of police officers in different roles. Law enforcement lacks competencies to operate in the digital world and effectively prevent and investigate cyberattacks on CPI (Robertson, 2019). A society which is so highly digitised has requirements for police officers who have both the technological resources and skills to address the demands of that society (Hitchcock et al., 2017; Custers, 2012) nevertheless digital skills are not yet an integral part of conventional police training and development (Harkin et al., 2018; Bossler and Holt, 2012) so that officers are frequently left without help to develop necessary digital skills (Sanders and Hannem, 2012; Schafer and Boyd, 2007).

In particular training on cybercrime or digital cyber security skills is fragmented and inconsistent across programmes (House of Commons, 2018; Palmiotto et al., 2000). Until now cyber security curricula have faced challenges to maintain pace, as they lack the methods and tools to rapidly integrate material on new skills or emerging threats (ENISA, 2019). Some research shows that there is a need for redefining educational and training pathways and unifying standards for cyber security however this is hampered by low availability of cyber security courses, misalignment between educational provision and market demands and focus on theory in place of practical training. Students experience constraints in developing a holistic cyber security skillset due to the need to specialise in either societal or technical cyber security issues (ENISA, 2019). Therefore current methods in training have failed to ensure that officers are effectively prepared to combat digital crime (House of Commons, 2018; Wolf, 2013).

Studies have also found that police officers are expected to be effective first responders to cybercrime however have little experience or training in these cases (Holt and Bossler, 2012; Craiger et al., 2005). Digital competencies remain largely unrecognised as a core competency with training concentrated on specialised units rather than organisation-wide. The literature emphasises the resources continuum (Williams et al., 2013) and the frequent tensions between specialist cybercrime units vs non-specialists (Willits and Nowacki, 2016). Digital skills in cyber security have yet to feature as a comprehensive component of law enforcement curricula (Stoetzer and Robertson, 2019). In the UK College of Policing, of over 170,000 courses completed in 2014-15, only four focused on cybercrime modules (Hitchcock et al., 2017).

This issue in turn may well be influenced by a broader cultural mindset in law enforcement that places emphasis on behavioural and militaristic cultures and a focus on officer attributes that emphasise physical strength, command, and crime control (UK Gov, 2018). Where cybercrime and digital literacy has been prioritised this has been in a highly specialised way. More broadly in the job market cyber security is a relatively new and dynamic sector and job specifications are linked to the specific context in terms of organisation sector and size (Pedley et al., 2018). Thus in general cyber security has been viewed as a highly specialist role which exists in large firms that may well be reflected in law enforcement. Stokes (2010) argues that specialisation can allow police organisations to save considerable cost in redundant training, provides greater expertise and enables skilled staff to follow and progress in individualised career pathways (Robertson, 2019).

Specialised cybercrime units are the most prevalent policing model and increasingly implemented globally (Robertson, 2019; Harkin et al., 2018). The need for organisation-wide upskilling of law enforcement both beyond traditional policing and specialist cyber-crime has yet to be recognised (Harkin et al., 2018, p. 529). In this context law enforcement officers cannot maintain pace with continuous criminal innovation and counter the threat to CPI. Moreover this creates major risks for law enforcement linked to mismanagement of digital evidence, inappropriate utilisation of technology and social media, resource wastage and delays (Stoetzer and Robertson, 2019). Traditional methods to fight crime would be unlikely to match the more advanced techniques employed by cyber criminals (Willits and Nowacki, 2016).

Analysis of CPI cyber security skills has identified the need for training across all CPIs including: awareness raising; vulnerability assessment; identity and access management malware analysis; incident response management; forensics analysis; data protection; data security; network analysis; cloud security; web app security; wireless security; ICS/SCADA Security; device and endpoint security; intrusion prevention and detection; threat intelligence; supply chain security; security of outsourcing; protection against advanced persistent threats (APT); and protection against distributed denials of service (DDoS) attacks (Piesarskas et al., 2019). The significance of digital competencies for law enforcement is underlined by the fact that law enforcement around the world lacks understanding of digital trends, threats and skills.

This context underlines the need for a broader and deeper level of competency for law enforcement (Gluschke et al., 2018; Willits and Nowacki, 2016). There is a major scarcity of law enforcement agents who understand security implications associated with CPIs and required processes to effectively assess and investigate cyberattacks. Moreover the necessary competencies to operate in the digital environment and respond to cybercrimes and attacks are not clearly defined in existing law enforcement roles (JCNSS, 2018). A diverse range of specialist skills and strong technical expertise is needed to secure CPIs against evolving and varied cyber threats. Responses require innovative ideas and initiatives and new forms of collaboration among public sector agencies (von Solms and Van Niekerk, 2013). While some commonalities exist different sectors have context-specific issues, concerns and risks requiring differing approaches to cyber security (Gjesvik, 2019).

Law enforcement needs to understand the specific risk and threat to CPIs and to possess the knowledge and skills to respond to cyberattacks. The protection of CPI requires a broader range of technological competence. Emphasis has been placed on comprehension of the risks, technologies and actors and the increasing cyber security requirements associated with the complex domain of critical infrastructures (Weed, 2019). There is a need for flexibility and speed at strategic level to prepare for events in the dynamic cyber context (Pöyhönen et al., 2020). Enhancing situational awareness (SA) depends on information sharing between the different actors involved and improves incident planning and management. Law enforcement response depends on their level of ability to detect and classify threats which in turn depends on a high level of security awareness drawing on different sources of information to identify and categorise patterns of cyber activity (Gjesvik, 2019).

However law enforcement can lack the ability to sufficiently understand the threat landscape and the sophisticated campaigns and patterns of cyberactivity (Gjesvik, 2019; Smith, 2018). Law enforcement may lack the digital capabilities to respond efficiently and effectively and investigate cyberattacks which often require analysis through a complex network of systems. For instance, CPI supply chains are characterised by complex systems of systems that have interrelated interdependencies and networks. In general organisational networks and work processes are large logistical frameworks composed of interrelated elements (Poyhonen et al., 2020).

Traditionally, UAE law enforcement has focused on preventing failures in CPI caused by accidents or natural disasters. However, as a result of increased digitisation, there is an urgent need for additional research in safeguarding CPI within UAE against growing threats of cyberattacks (Brown et al., 2006) to enhance security, reliability and resilience of UAE's CPI against cyberattacks. Further there is a need to identify the organisational and technical interventions required by UAE public sector organisations to enhance cyber security with a focus on both proactive and reactive approaches. Law enforcement requires understanding of preventative measures so that they are able to advise and support the protection of CPIs. In general across all sectors, while cyber security threat awareness and its perceived importance is identified to be high the extent of efforts to address cyber security risk are often differentiated across sector and organisation size. Just under half of organisations have introduced new policies to mitigate risks to cyber security and an even lower proportion (43%) have implemented risk assessments and analysis of impacts to quantify potential threats (Gluschke et al., 2018).

The protection of critical physical infrastructures is associated with a number of core functions which in law enforcement may be severely limited. Protection of CPIs requires competencies related to identification and understanding of cyber threats to systems, activity monitoring and detection, the implementation of protective measures, responding to incidents, and recovery and restoration (NIST, 2018). Law enforcement lack the specific competencies in each of these broad areas in order to effectively undertake their role to prevent and investigate cyberattacks. In some countries such as the UK information about the nature of the cyber security skills gap in the CPI sector is primarily anecdotal. There is no detailed analysis available of which CPI sectors are most affected, in which disciplines and at which levels of expertise the shortage is most acute (JCNSS, 2018).

1.4 Research Questions

This problem is consistent with a knowledge gap in the literature in the understanding of digital competency of law enforcement for CPI (Ala-Mutka, 2012; Ferrari et al, 2012). There remains a lack of clarity in the literature and practice in what ways law enforcement needs to develop digital competences to be able perform its role effectively in a digital environment. Based on the research context and problems three research questions are formulated that guide the focus of this investigation and ensure a significant contribution in this field:

1. What are the function and roles of law enforcement in Cyber Security for CPI?

2. What key domains and elements of digital competency for cyber security can be identified that are critical for law enforcement to perform its role in protecting CPI?

3. What framework can be developed to guide policy and the development of law enforcement in the UAE and enhance its capability to perform its role effectively in a digital environment?

1.5 Research Aim and Objectives

To address these research questions this research aims to develop a digital competences framework for UAE law enforcement agencies to combat cyber security threats facing the UAE's critical physical infrastructure. To address this aim the research is directed towards three research objectives:

1. To investigate the key function and roles of law enforcement in cyber security for CPI

2. To define and validate the key dimensions and elements of digital competency for cyber security law enforcement to perform its role in protecting CPI

3. To develop a framework to guide policy and the development of law enforcement in the UAE and enhance its capability to perform its role effectively in a digital environment.

1.6 Research Contribution

The findings will have relevance to law enforcement training and performance policy both in the UAE and in the wider international context. The findings from this study will make a novel and significant contribution to both theory and practice. At a theoretical level this research contributes a novel digital competency framework for cyber security skills specific to law enforcement necessary for protection of CPI. This provides a unique understanding by making four major contributions that extend existing work. Firstly while there has been some work on digital competencies for cybersecurity (Cybok.org, 2020; JCNSS, 2018; Libicki, 2007) the findings will be unique in terms of identifying digital competencies for cybersecurity specifically in the context of law enforcement. In particular this study provides empirical analysis that identifies and prioritises categories of digital competencies and associated specialties and work roles critical for law enforcement to ensure cybersecurity protection of CPI. This points to the second unique contribution in terms of providing a response to protection of CPI for law enforcement. The goal of the empirical analysis is to identify and prioritise the specific digital competencies, specialty areas and work roles for law enforcement that will most allow them to effectively protect critical physical infrastructure. The resulting framework addresses a knowledge gap in understanding and mapping digital competencies that are required for different law enforcement roles in terms of cyber security of CPI. The framework contributes a comprehensive reference of the set of knowledge, skills, and abilities necessary for law enforcement that defines structured pathways for understanding and developing them. The outcomes of this research further contribute a holistic framework that integrates the theories of cybercrime linked to CPI protection. The literature shows that the majority of frameworks focus attention on either the technical aspects of cybercrime or less technical aspects such as organisational, human, and leadership (Boin and McConnell, 2007). The proposed framework takes into consideration organisational, leadership, managerial, and resource driven digital competences (Skogan and Hartnett, 2005; Weisburd and Lum, 2005). A unique contribution will also be made in terms of identification of key implementation factors for a digital competencies framework for law enforcement in the context of cybersecurity for CPI. This will address the planning and implementation context by identifying multiple planning factors that are critical to establish an effective and efficient design and implementation for a digital competency framework.

Fourthly the framework provides a novel contribution by extending understanding in the context of an Arab and developing country, and specifically in the context of the UAE. The importance of this research is linked to concerns over the UAE government's ability to provide adequate protections against cybercrime (Rajan et al., 2017). Further despite the significance of developing digital competences of enforcement agencies, there is limited analysis or empirical evidence in this area within the UAE context. While traditionally, UAE law enforcement has focused on preventing failures in CPI caused by accidents or natural disasters a rapid and widespread increase in digitisation underlines an urgent need for additional research in safeguarding CPI within UAE against growing threats of cyberattacks. This study makes a contribution by addressing the need to identify the organisational, technical and development interventions required by UAE law enforcement to enhance cyber security.

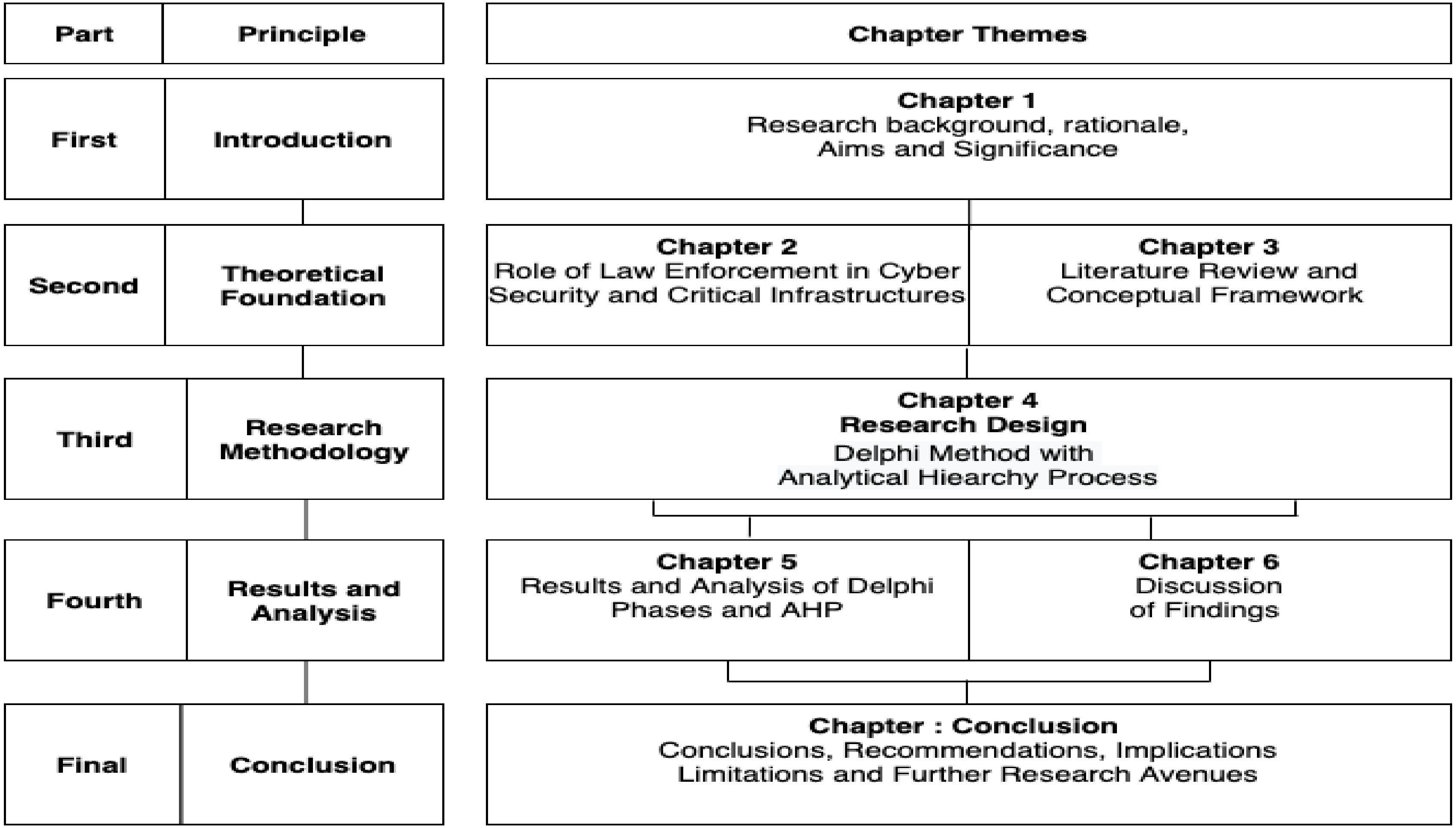
The findings will also have a range of managerial implications in increasing the capacity of law enforcement agencies to address cybercrime and protect CPI. The framework can promote consistency and common reference across all agencies for development of DC and support practitioners to make informed decisions and raise standards. The framework represents a tool that supports development of law enforcement to maintain pace with the cyber security landscape and enables law enforcement to adapt and develop to operate in the digital environment.

Further it offers practitioners a tool to assess and evaluate the digital competencies for law enforcement personnel and promote a holistic understanding of cyber security for CPI. This can support benchmarking and allow law enforcement organisations to understand organisational needs and identify skills gaps in different areas and roles relating to CPIs and ensure a consistent and efficient approach for development of digital competence for law enforcement in cyber security of critical physical infrastructures.

Across all law enforcement functions the framework can support the development of policies and procedures, tools and implementation of measures that increase the capability of law enforcement to protect CPI. Finally, this research can contribute to defining nationally recognised behaviours and values in the UAE, and represents a consistent foundation for a range of local and national processes and ensure expectations and improved standards of law enforcement for the protection of CPI.

1.7 Thesis Structure

This study presents the research goal and the research process across seven chapters. The first chapter provides an introduction to the study including background and problem context, the research rationale and the research aims and objectives and significance. The next two chapters provide the theoretical foundation for this study. Chapter 2 provides a background to the role of law enforcement in cyber security and critical infrastructures which is necessary to understanding the requirements for digital competences. Chapter 3 presents a review of relevant literature, theories and concepts in relation to competencies and digital and cyber security competencies and presents the conceptual framework for this study. Chapter 4 concerns the research design and methodology for this study and outlines the mixed method approach incorporating qualitative and quantitative data that is collected using a Delphi method and the different phases of this approach. A comprehensive overview is given that explains the research approach, methods and procedures utilised to achieve the research aims and discusses the methodological considerations and rationale that underpinned the research process throughout all phases of this study. Chapter 5 presents the results of the data analysis for the several phases of research outlining key themes in relation to cyber security competencies for law enforcement. This is structured in line with each phase of the Delphi method. These results are then discussed in Chapter 6 in the context of prior literature and theory. In the final Chapter 7 the thesis is concluded summarising the key findings, contributions and implications emerging from this study as well as key recommendations, limitations and avenues for future research.



Part	Principle	Chapter Themes
First	Introduction	**Chapter 1** Research background, rationale, Aims and Significance
Second	Theoretical Foundation	**Chapter 2** Role of Law Enforcement in Cyber Security and Critical Infrastructures **Chapter 3** Literature Review and Conceptual Framework
Third	Research Methodology	**Chapter 4** **Research Design** Delphi Method with Analytical Hiearchy Process
Fourth	Results and Analysis	**Chapter 5** Results and Analysis of Delphi Phases and AHP **Chapter 6** Discussion of Findings
Final	Conclusion	**Chapter : Conclusion** Conclusions, Recommendations, Implications Limitations and Further Research Avenues

Figure 1-1. Thesis structure

Chapter 2 Law Enforcement in Cyber Security for CPI

2.1 Introduction

The development of a digital competency framework for law enforcement for the purpose of enhancing cyber security for critical physical infrastructure (CPI) requires an understanding of the scope and underlying requirements that will shape such a framework. The purpose of this chapter is to provide a detailed background to the research focusing on understanding the criminal innovation, nature of cybercrime, cyber security in the UAE, CPI and the role and functions of law enforcement. A discussion of these topics in this chapter is essential to researching and developing a digital competence framework that addresses the cybercrime context and challenges and focuses on the necessary competencies for law enforcement in the area of CPI.

2.2 Cybercrime Definition and Types

The changing role of technology continues to redefine the role of the state and its enforcement agents globally. Cybercrime is a broad term that identifies the incidence of a harmful action that is conducted using or facilitated by information and communication technologies (ICT) (Wall, 2007). The expression has been utilised to represent a range of different concepts at differing levels of definition. Broadly the term can refer to any illegal activity resulting in either pecuniary or non-pecuniary loss such as violent crime, vandalism, or blackmail. It can also be employed to allude exclusively to nonviolent crimes leading to a monetary loss where for instance a financial loss is incurred due to hacking into a system and accidentally or intentionally deleting files or records associated with financial accounts. According to the definition by Wall (2007) cybercrime depends on an understanding of how technologies impact on society, social systems and behaviours. It is evident that the Internet and digital space is continuously changing and evolving creating new opportunities for criminal activity. This has implications for the competencies of organisations and agencies either engaged or connected to cyberspace or responsible for governing and regulating this space (Jahankhani et al., 2014; Yar, 2006).

Wall's (2007) classification of cybercrime by level of opportunity and type of crime shows cybercrime can be considered broadly in terms of four impacts: computer-related (acquisition theft/deception); content-related (obscenity); content related 2- (violence); integrity-related (harmful trespass). Further, digital space offers opportunities for more traditional crime to be perpetrated through communications and creating opportunities for traditional crimes to be perpetrated across borders and boundaries; or novel opportunities for emerging kinds of crime.

The complexity of cybercrime can be seen through different perspectives that underline the potential threat on CPI. More widely the literature categorises four overarching categories of cybercrime defined in terms of the relationship between ICT and the crime: the computer or device as the target; the computer or device as the instrument of crime; the fraudulent use of ICT systems; and crime linked to the prevalence of computers (Jahankhani et al., 2014). When applied to CPI the computer can become the target of attacks, be used to perpetrate crime, used fraudently or used to steal critical data about CPI or other facilities.

Other definitions of cybercrime suggest more specific types of attacks on CPIs. The Convention on Cybercrime Treaty adopted by the Council of Europe in 2001 alludes to several activities considered to represent cybercrime offences such as: intentional but unauthorised access to computer systems and interception of private transmission of digital data; intentional damage to system functioning and unauthorised inputting, deletions, alteration or suppression of digital data; and the creation, sale, procurement, or distribution of devices or data aimed at committing such crimes (CoE, 2001). One definition by Yar (2006) underlines the issue of CPI and identifies "crime against the state" as a form of activity which breaches laws protecting the security and stability of national infrastructure such as espionage, disclosing state secrets and terrorism.

Cybercrime can also be understood in terms of the cyberattack methods and tools that can be used to target CPI (Kamat and Gautam, 2018). Cybercrimes can be perpetuated through different methods and tools such as malware, automated software applications (bots), Internet messaging and chats, spyware, viruses, and code (Jahankhani et al., 2014). Common methods that have implication for competency of law enforcement include:

- E-mails: one of the main tools that provide a most efficient form of spamming and phishing, that facilitate devastating attacks on organisational networks with tremendous ease and speed. E-mail based attacks can be content based targeting HTML or exploiting scripting features and vulnerabilities.

- Buffer overflow attacks: these send data packages that exceed the fixed-size memory buffer of the e-mail recipient, to exploit the chance that the overflow data rather than being safely discarded overwrites critical information.

- Shell script attacks: these can be invoked when code fragments embedded in message headers are executed by the mail client.

- Staged downloaders: these allow for installation of malicious codes onto a compromised computer to stage any number of attacks such as Trojan against other systems to relay spam.

- Keyloggers: these record and relay information

Competency for cybercrime for can also be understood in terms of awareness of cybercrime and of different motivations and intent of perpetrators targeting CPI. Jahankhani et al., (2014) offer a taxonomy for motives that defines: financial, political, moral, self-actualisation, exploitation and promotional. Awareness of these offers a basis for situational awareness that can assist law enforcement in successfully investigating cybercrimes. Financial drivers for cybercrime are associated with fraud and financial gain but can also be linked to financial system disruption. Political motives relate to support or opposition for governmental agendas and activities and can encompass espionage, propaganda or state sponsored attacks. In terms of moral motivations these can be connected to activities which oppose exploitation or oppression or work to uphold freedoms and rights. Motivations in this category may be linked to religious systems in terms of attacks conducted by religious groups on other religious or belief systems or attacks on religious groups against their belief systems (Jahankhani et al., 2014).

2.3 Criminal Innovation

As criminals adapt and capitalise on the opportunities provided by new technologies police forces are also under pressure to continually innovate and change and update to address different forms of criminal innovation (Jackson et al., 2020). The global value of organised crime alone is estimated at over $4 trillion dollars a year, which is twice the world's military budgets combined (MP, 2019). Cybercrime is the top domain for criminal activity with cybercrime costs estimated to reach $6 trillion dollars in 2021 (WEF, 2020) and $10.5 trillion annually by 2025 (Morgan, 2020). Thus responding effectively to criminal innovation and use of technology to commit crime is rapidly becoming a key priority for policing, driving a need to keep pace with emerging technologies, new crimes and a dynamically changing threat landscape (Europol, 2019). Thus a wide range of criminal innovation represents a major impetus for police digital capabilities to counter evolving threats to CPI.

Digital competency of law enforcement needs to maintain pace with technological advancements. The development of new technologies has provided a major incentive for criminal innovation creating new forms of crime, adaption of traditional crime techniques and radically altering criminal practices. One of the notable characteristics of criminal innovation acknowledged by leading law enforcement agencies is the high degree of flexibility and adaptability of individuals and groups perpetuating crime and the speed at which they can identify new opportunities, victims or evade detection or countermeasures (Europol, 2017). Technology has unlocked new avenues for criminals to commit crime through innovations that maximise revenues from crime, operate more efficiently and minimise risks or risk of detection (Europol, 2018). It is evident that technology has become a key component of most, if not all crime. Criminals have applied new practices and technologies in the way they communicate, creating new forms of anonymity and the employment of readily available secure apps and end-to-end encryption across all crime areas (UN, 2015). Application of ad-hoc technological solutions and utilisation of myriad communication channels provides the ability to share information covertly and perpetuate an unprecedented volume of transgressions against victims (Europol, 2019).

Cyber security of CPI also has implications for financing in digital context of criminal activity related to CPIs. The financing of criminal operations and management of the funds of crimes has also been subject to significant transformation and innovations. Criminals are exploiting a diverse range of complex payment options that provide higher levels of anonymity, speed and global mobility spanning many jurisdictions. These new forms of payments such as cryptocurrencies are contributing to the opportunities provided to criminals for establishing new methods and ways to finance and expand criminal activities (Ozkaya and Islam, 2019). Cryptocurrencies are increasingly being exploited for illegal enterprise due to their rapid processing and encryption and anonymisation tools, which can hide the origin of illicit funds and allow them to be reinvested into the legal economy. Cryptocurrencies are the only currencies acceptable to the majority of darknet marketplaces (Europol, 2017).

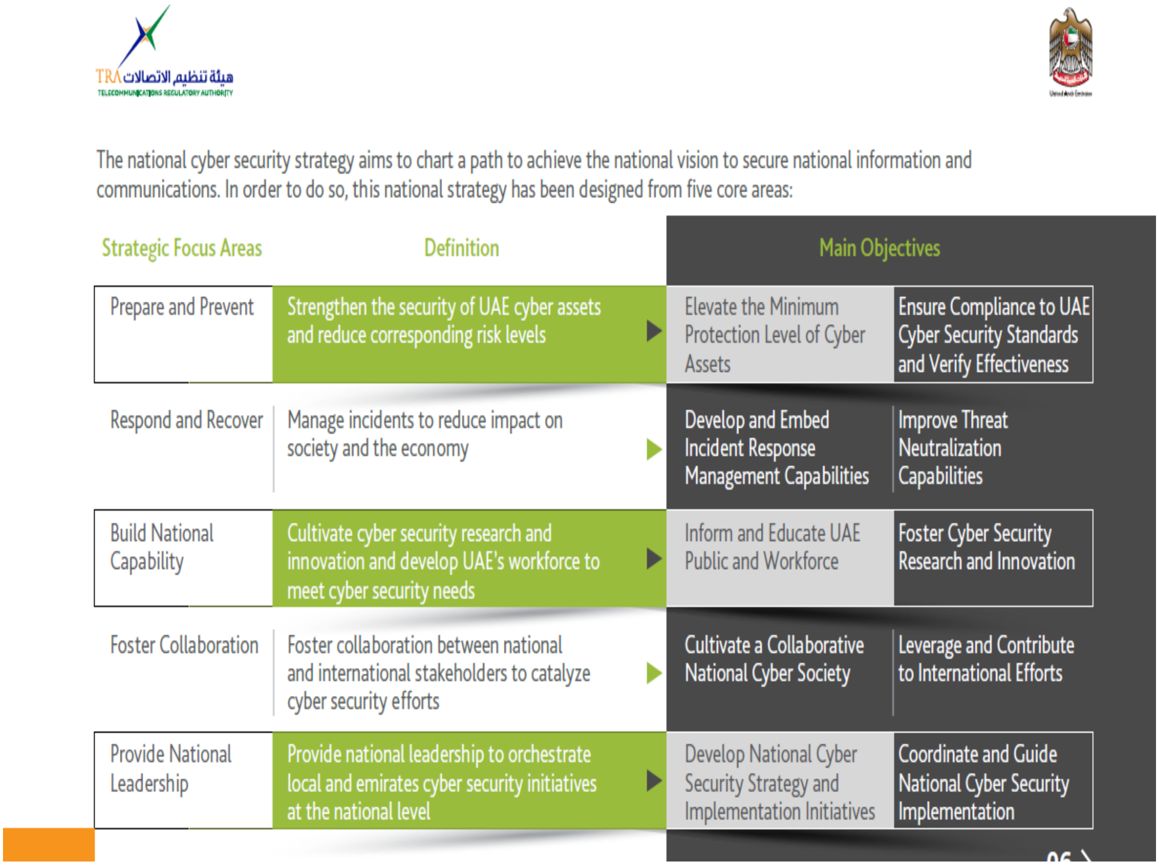
Cyber security skills for law enforcement are also related to structures and patterns of criminal organisations in the modern era. Traditional hierarchical structures and organisation of major crime groups is now being challenged with new, more dynamic and flatter structures and the adoption of service-based models to perpetuate crimes online (EPO, 2014). The criminal environment is now increasingly characterised by entrepreneurial culture and new possibilities provided by evolving technologies. This has witnessed new entrants from across the social spectrum who have been emboldened by the anonymity of the Internet and the ability to hide behind multiple identities and entities (UN, 2015). This has resulted in the growth of new entities that are fluid and flexible based on virtual and highly distributed and fragmented criminal structures. There has been a marked shift from groups to individual operators. A new culture of work has evolved based on service-orientated principles and addressing market needs and partnerships and joint ventures within a vast interconnected online network of myriad communities (UN, 2013). Criminals often come together on an ad-hoc basis for specific criminal projects or criminal services and for sharing knowledge and expertise (Europol, 2015; UN, 2013).

2.4 Cyber Security in the UAE

The UAE national cyber security strategy has evolved to encompass policies, standards, and strategies guiding frontline practitioners. The National Cyber Security Strategy (NCSS), shown in Figure 2-1, has a clear aim to secure the national information and communications across the UAE as set by Telecommunications Regulatory Authority. The NCSS is guided by a number of umbrella bodies and policies that support implementation in different areas and sectors: The National Information Assurance Framework (NIAF) whose main goal is to ensure a minimum level of information assurance; the Critical Information Infrastructure Protection Policy (CIIPP) whose aim is to identify and develop the necessary application programmes to protect critical information infrastructure; and the National Information Assurance Standards (IAS) whose main goal is information protection and management. This includes aspects such as compliance, certification and accreditation, business information continuity, and disaster recovery. The NCSS is based on five focus areas:

- Prepare and prevent: Aims to raise the minimum protection level of cyber assets and ensure compliance to the UAE’s cyber security standards
- Respond and recover: Aims to develop incident and response management capabilities and improve threat neutralisation capabilities
- Build national capability: Aims to inform and educate the public and workforce about cyber security and promote research in the field
- Foster collaboration: Aims to collaborate with international bodies to catalyse cyber security efforts nationally and internationally
- Provide national leadership: Aims to develop initiatives to guide the implementation of the National Cyber Security strategy (UAE Gov, 2019).

In addition to the national strategy on cyber security for the UAE individual Emirates have introduced specific initiatives. For example Abu Dhabi operates a vital centre referred to as the Critical Infrastructure & Coastal Protection Authority (CICPA). It has the main duty of assessing all the security procedure and breaches across Abu Dhabi’s infrastructure in land, sea, petrol establishments, and maritime logistics.



TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY

The national cyber security strategy aims to chart a path to achieve the national vision to secure national information and communications. In order to do so, this national strategy has been designed from five core areas:

Strategic Focus Areas	Definition	Main Objectives	
Prepare and Prevent	Strengthen the security of UAE cyber assets and reduce corresponding risk levels	Elevate the Minimum Protection Level of Cyber Assets	Ensure Compliance to UAE Cyber Security Standards and Verify Effectiveness
Respond and Recover	Manage incidents to reduce impact on society and the economy	Develop and Embed Incident Response Management Capabilities	Improve Threat Neutralization Capabilities
Build National Capability	Cultivate cyber security research and innovation and develop UAE's workforce to meet cyber security needs	Inform and Educate UAE Public and Workforce	Foster Cyber Security Research and Innovation
Foster Collaboration	Foster collaboration between national and international stakeholders to catalyze cyber security efforts	Cultivate a Collaborative National Cyber Society	Leverage and Contribute to International Efforts
Provide National Leadership	Provide national leadership to orchestrate local and emirates cyber security initiatives at the national level	Develop National Cyber Security Strategy and Implementation Initiatives	Coordinate and Guide National Cyber Security Implementation

Figure 2-1 National Cybersecurity Strategy

(UAE Gov, 2019).

CICPA was established in 2007 and has embarked on the task of ensuring threats to cyber security have been mitigated or repelled. CICPA works in collaboration with the UAE’s enforcement agencies to ensure regulations and implementation of policies leading to securitisation and protection of the nation’s critical infrastructure.

2.5 Cyber Attacks and Critical Infrastructure Protection

The rate, scope, and magnitude of cyberattacks directed at critical national infrastructure have escalated in recent years (Rudner, 2013; Brown et al., 2006). This is because national efforts to improve infrastructure efficiencies through interlinked automation and networks have created new vulnerabilities in terms of physical and computer-related attacks (Radvanovsky and McDougal, 2010, p.3). Motivation for cyberattacks has been linked to malicious intent emanating from a broad range of wrongdoers that includes hacktivists, dissatisfied insiders, international terrorism, domestic militants and state sponsored espionage/sabotage (Rudner, 2013). Attacks on critical national infrastructure are an attack on the entire population with a capacity to inflict maximum suffering at unprecedented speed to targeted countries (Rudner, 2013; Brown et al., 2006).

Approaches and strategies adopted to protect critical physical infrastructure are as varied as the cybercrimes perpetrated. Multiple methods have proven their effectiveness to deter or mitigate coordinated or accidental attacks caused either by hackers and criminals or natural disasters (Radvanovsky and McDougal, 2010, p. 4). Methods range from preventive to reactive in order to minimise the impact of cascading failures in a complex network. Where threats are deemed likely to escalate, responses have included deactivating affected critical infrastructure such as power grids, transmission lines, telecommunications networks, or computer networks (Li et al., 2013).

A widely implemented approach to improve the defence systems of critical infrastructure draws on teams to model Attacker-Defender scenarios to develop an optimal solution (Brown et al., 2006). Such models often address criticality, vulnerability, reconstitutability and the threat being posed so that a critical infrastructure may be declared robust and resilient against potential attacks (Brown et al., 2006). These approaches support a strategy of developing digital competences through simulated systems and scenarios based on cognitive heuristics and information availability that uses experimentation and problem-solving to understand the effectiveness of possible attacks and defences. While such approaches can provide useful insights a determined adversary seeking gaps or ambiguities within the limit of cognitive heuristics may still be able to perpetrate an effective coordinated attack (Brown et al., 2006). A number of criticisms are advanced that suggest a sole dependence on this approach to protect critical infrastructure could be problematic. Brown et al., (2006, p.543) state that: “If we base defensive measures on heuristically identified, near optimal attacks, we risk an attack by an aggressor who is smarter than our heuristic". According to Radvanovsky and McDougal (2010, p.2) attackers of critical infrastructure are generally assumed to be determined, creative, resourceful and flexible and "able to learn how to target vulnerable areas while avoiding those that are more protected and predictable". Zhang and Ramirez-Marquez (2013) attempt to address this weakness in the development of a multi-objective optimisation model that takes into consideration the attacker's intelligence. This models critical infrastructures as networks and protection as a game with two phases staged between a guardian and an attacker with incomplete information.

Another approach focuses on backup of redundant assets to enable rapid reconstitutability and recovery following damage inflicted by a cyberattack (Brown et al., 2006). This is based on the proposition that developing analytical competence which could be used to assess vulnerabilities, conduct risk analysis for remediation and mitigation relative to infrastructure protection is more significant than any unique set of intelligence collection method or unique integrated intelligence function (Radvanovsky and McDougal, 2010, p.1). Adopting this strategy would have implications for the design and development of digital competence training that prioritises analytical competences over intelligence collection and sharing.

While CIP protection can often be characterised as a reactionary response to various hazards, risks, threats, or vulnerabilities, preventive measures and countermeasures form a key dimension of protecting critical infrastructure (Radvanovsky and McDougal, 2010, p.4). This is because keeping pace with advances in cybercrime is highly complex and deteriorating infrastructure is vulnerable to newer and advanced tools. Proactive and preventive policies and measures can strengthen, upgrade and prolong the life span as well as the quality of the infrastructure against failure or collapse which might arise due to unintentional or intentional attacks or disruptions (Au-Yong et al., 2014; Al-Najjar and Wang, 2001).

2.5.1 National Response Mechanisms

Increasing CPI vulnerability has driven global efforts to create assurance mechanisms that provide validation for optimal defence through a range of strategies including continuous testing and evaluation of the critical infrastructure and its vulnerability (Radvanovsky and McDougal, 2010). The Global Cybersecurity Index (2021) reports that to achieve a further level of assurance countries from around the world are investing in digital competence professional training in cyber security as shown in Figure 2-2.

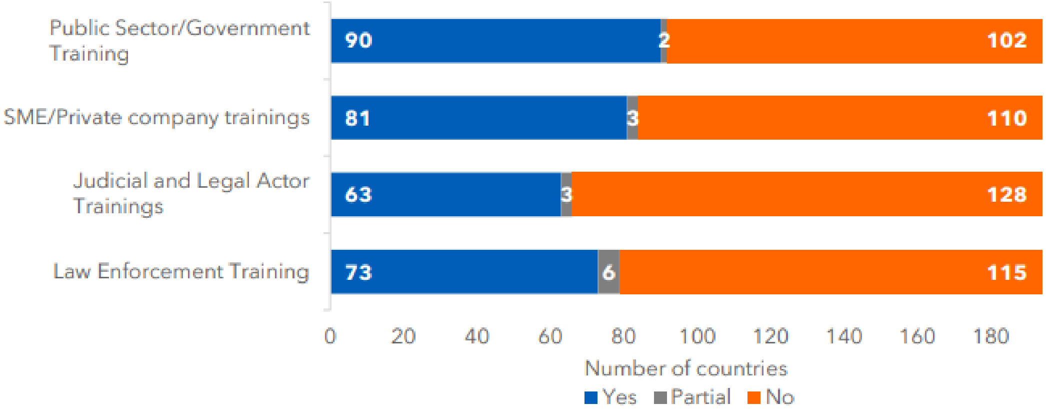


Figure 2-2 Professional Training

(Global Cybersecurity Index, 2021, p.17).

Governance of cyberspace and information represents a further national level response to protecting critical infrastructure from cyberattack. Cyberspace governance is highly complex especially in relation to critical infrastructure and challenging as infrastructure networks and communication are not organised through the institutional apparatus of the state (Deibert and Rohozinski, 2012). While a sovereign state can claim ownership and sovereignty over a certain material infrastructure, in reality they are never fully in control of the entirety of the cyberspace (Deibert and Rohozinski, 2012). Governance becomes more problematic as the ‘architecture’ itself is distributed with overlaps between private and public organisations and there is no single point of control (Dutton and Peltu, 2007). Actors from the private sector in multiple countries operate the majority of the key infrastructural cyberspace constituents. Consequently the structure of cyberspace governance consists of a network of organs that include numerous stakeholders such as governments, businesses, and civil society networks. These address issues of copyright and intellectual property regulation, content filtering, and spectrum allocation, as well as cyber-crime (Deibert and Rohozinski, 2012, p. 17).

Unlike other spaces such as land, sea, or air, cyberspace allows for the addition of generative technologies and ideas to the network giving rise to constant variation, which often presents more complexity in regards to regulations and governance (Deibert and Rohozinski, 2012). Despite the challenges presented by the nature of cyberspace, attempts at controlling and monitoring it frequently commence with physical infrastructure interventions at "key internet chokepoints" (Deibert et al., 2008). This places emphasis in the UAE on strengthening digital competences in regards to legal measures to enhance cooperation and facilitate rapid governance and intelligence sharing regionally and globally. The global Cyber Security Index 2018 depicted in Figure 2-3 shows that the Arab region scored low in regards to the commitment to strengthen cybercrime legislations especially with links to critical infrastructure.

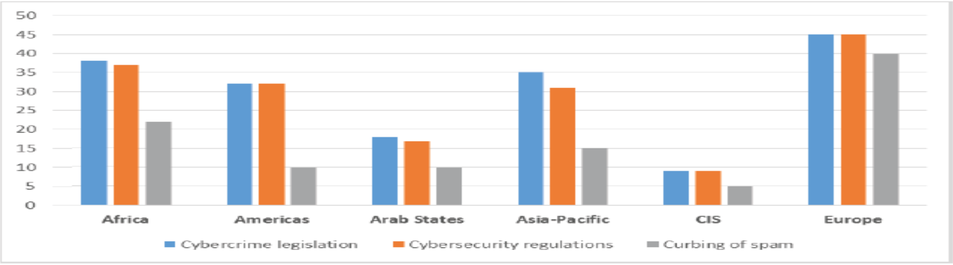


Figure 2-3 The Commitment Level per Pillar in Six Regions

(Global Cybersecurity Index, 2018, p.31).

2.5.2 Cybersecurity Challenges in Cloud Computing

The nature of cloud computing presents numerous challenges for law enforcement agents in relation to CPI protection (Battistoni et al., 2016; Martini and Choo, 2012; Dykstra and Sherman, 2012). This is because cloud computing enables cybercriminals to store data abroad challenging law enforcement agents' ability to investigate and enforce (Battistoni et al., 2016; Martini and Choo, 2012; Dykstra and Sherman, 2012). The virtuality and geographical spread of cloud computing presents law enforcement agents with technical and jurisdictional challenges in terms of identification, seizure, acquisition, and analysis of evidence by digital forensics in a timely fashion

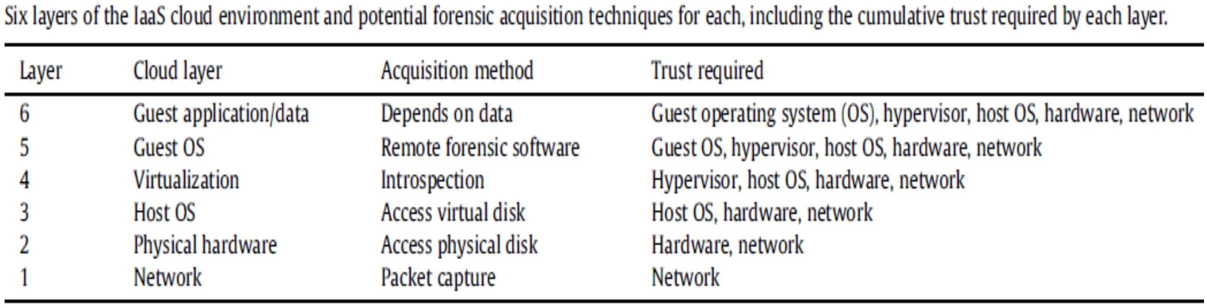
(Garfinkel, 2010). There is urgent need for police officers to develop technical competences in regards to cloud network digital forensics on the one hand, and procedural competences in terms of cooperative and legal reforms (Martini and Choo, 2012). Cloud computing poses a problem to forensic investigations as stored evidence can be tampered with (Taylor et al, 2011).

While no definition of cloud computing is universally accepted the following definition appears to be widely accepted and utilised by government agencies and experts: "ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (AGIMO, 2011, p.10; NIST, 2020). Cloud computing can be deployed under different service models; software, infrastructure and platform (Martini and Choo, 2012). From a security perspective IaaS allows the user to provide for themselves the infrastructure with control over processing time, storage, and speed and upon which they can run the software operating system of their choice (Mell and Grance, 2009). This is generally considered safest since through the IaaS portal the user may have control over CPU, RAM, and network access (Martini and Choo, 2012).

Despite the potential to ensure the security of users a number of concerns have been raised in regards to safety within the cloud environment. Six layers of trust have been defined to ensure integrity and authenticity of data that is trustworthy and forensically sound (Dykstra and Sherman, 2012), as shown in Table 2-1. However unlike a situation where the forensic examiner has remote access to the evidence contained in virtual machines (VM) for further analysis online and off line, conducting forensic investigation in the IaaS cloud environment in which the VM is not easily or directly accessible the investigator "requires trust that the guest operating system, hypervisor, host operating system, underlying hardware, and network produce complete and accurate evidence data, and are free from intentional and accidental tampering, compromise, or error" (Dykstra and Sherman, 2012, p.92).

Therefore in addition to the six layers of trust experts have proposed that sources of evidence be corroborated from multiple sources (Garfinkel, 2006). Following a cross examination of the layers of trust the investigator needs to determine the layer with highest technical competence to launch and execute the forensic process as well as gather the evidence required. Once this choice has been established the investigator can proceed accordingly to retrieve, reassemble, and report evidence from mediums at different layers (Dykstra and Sherman, 2012, p. 93). Within each data type it is essential that the data adheres to a strict chain of custody and includes mechanisms for checking its' integrity (Dykstra and Sherman, 2012).

Table 2.1 IaaS Cloud Environment Comprised of Six Layers



Six layers of the IaaS cloud environment and potential forensic acquisition techniques for each, including the cumulative trust required by each layer.

Layer	Cloud layer	Acquisition method	Trust required
6	Guest application/data	Depends on data	Guest operating system (OS), hypervisor, host OS, hardware, network
5	Guest OS	Remote forensic software	Guest OS, hypervisor, host OS, hardware, network
4	Virtualization	Introspection	Hypervisor, host OS, hardware, network
3	Host OS	Access virtual disk	Host OS, hardware, network
2	Physical hardware	Access physical disk	Hardware, network
1	Network	Packet capture	Network

(Dykstra and Sherman, 2012, p.92).

Both PaaS and SaaS allow for a platform to develop and host user applications and software environment and to operate without any control over the underlying infrastructure (Martini and Choo, 2012). The nature of user needs often determines the nature of cloud computing services in use. PaaS and SaaS would need additional layers of trust to account for the trustworthiness of their platform or services provided accordingly (Dykstra and Sherman, 2012). This underlines the imperative for the UAE to develop digital competences in all three areas (IaaS, SaaS, and PaaS).

While a range of cloud computing forensic frameworks have been introduced (Kent et al, 2016; McKemmish, 1999) in addition to good practices around the world there is minimal consensus in this area (Martini and Choo, 2012). Kent et al., (2016) and McKemmish (1999) share similarities in regards to stages of digital forensics: Identification of digital evidences (e.g. type/format); Preservation of data using correct methods and from original devices so that evidence remains unchanged; Analysis and storage of data in original formats; and finally presentation to court with expert testimony of the analysed data (Martini and Choo, 2012). Nonetheless, some scholars argue that applying traditional digital forensics to cloud environments is not fit for purpose as the cloud computing environment is characteristically different from traditional computer network environments (Dykstra and Sherman, 2012; Birk and Wegener, 2011). The key challenge for law enforcement agencies (LEAs) is that data in cloud environments are stored and distributed across a range of data centres in geographically diverse environments with different legal jurisdictions making forensic evidencing difficult (Dykstra and Sherman, 2012; Taylor et al., 2011). In order to resolve this issue Martini and Choo (2012) proposed an integrated framework from the works of McKemish (1999) and Kent et al., (2016). Their framework proceeds with a principle of *iteration* in mind at every stage of the digital forensic investigation which encompasses the following phases (Martini and Choo, 2012):

1. Preservation and identification: once the usage has been identified in an initial iteration the second iteration immediately preserves on an on-going basis. This is vital as the data usage could change as the investigation unfolds.
2. Collection: this phase enables the LEAs to separate between collection of evidences from different sources such as from physical devices (export of hard drive, memory), as well as extraction from the sources recovered.
3. Examination/Analysis: at this phase emphasis is placed on analysis of usage from the cloud source leading to more iterations
4. Reporting/Presentation: this final stage is about how evidence is collected and presented legally.

Another challenge to cloud computing forensic investigation is in regards to the possibility of time of events (ToE) alteration by the adversary (Battistoni et al., 2016). Such attempts could render digital forensic investigation in the cloud difficult as the adversary may be operating in geographically dispersed regions with different timelines making timeline alterations easier (Thorpe and Ray, 2012). Adversaries can for example sustain a privileged escalation attack such that they commit crime at one time and switch on virtual machine (VM) guest session and show that at the time they were equally busy writing elsewhere; or create a file system time stamp alteration in which case the adversary changes time span to fake activity (Battistoni et al., 2016). Either of the time alteration mechanisms utilised could render evidence invalid or void for forensic evaluations (Battistoni et al., 2016).

In order to limit the occurrences of ToE alterations Battistoni et al. (2016) developed a model referred to as CURE based on time controller/time stamp service, secure channels, and heart beat channels. The key utility of the CURE framework is in regards to its ability to detect and send security warnings during a potential malicious attempt (Battistoni et al., 2016). The implication of this model/framework for LEAs is to channel and develop competences on cloud infrastructure with the architecture of guest-host continuum on one hand, and time alteration forensic evaluations on the other (Battistoni et al., 2016).

2.5.3 Critical Infrastructure Protection: Good Cyber Practice

A number of good practices in regards to critical infrastructure protection can be identified around the world. One approach to CPI protection is cooperation and collaboration between government, law enforcement and industry that involves information sharing between sectors and law enforcement. In the US for example a coordinated approach is adopted in the design of frameworks that facilitate partnership between law enforcement agencies, intelligence community, industry sectors and national coordination centres in respect of national critical cyber infrastructures (Homeland Security, 2018; Dutta and McCrohan, 2002).

Another practice is the development of specialist units within law enforcement to address cybercrime. In the UK for example dedicated e-policing units have been developed including the Police Central eCrime Unit (PCeU) based within the metropolitan agency, in addition to the National Cybercrime Unit (Wall and Williams, 2013). These have focused on cultivating digital competencies to a specialist level among police officers. Using social media as an information source is a further practice to extend existing policing practice. This has been encouraged in the UK, where police leaders have identified that investigations can benefit greatly from the information available, while Germany has developed a detailed legal framework for social media investigations and applied as training content for law enforcement agents.

The framework elucidates the relationship between law enforcement operations and the regulatory environment for commercial operators of social media platforms and differentiates between the right to privacy of personal data and telecommunications for individuals and varying levels of interference. The framework further distinguishes between various categories of usage and inventory information accessed by law enforcement to select the relevant law.

Legal approaches have also been adopted that represent good practice to combat cyberattacks on CPI in response to the new challenges presented by cloud computing to traditional digital forensics. This has implications for digital competences for information sharing and accessing systems between organisations and agencies across national boundaries. Rogue elements which may be domiciled in different jurisdictions are now able to target cloud systems for storing illicit/illegal data on a cloud, crack passwords and encryption, or use the cloud as a base for a brute force attack, making it more difficult to trace, police, and even enforce (Hooper et al., 2013). One approach to address these issues is demonstrated by the Australian government who, in collaboration with LEA's have undertaken legislative reforms that encompass access and disclosure of data, legal interception of data, and cooperation with LEAs in other jurisdictions (Hooper et al., 2013).

Other approaches go beyond policing in respect to critical infrastructure such as the EU Network and Information Security Directive (NISD). This requires that all critical infrastructure organisations apply more robust reporting in terms of security and breaches for ICS/SCADA/OT networks or risk being fined. In the case of the UK this can be up to £17 million or 4% of global revenue (CyberX Report, 2018).

2.6 Cyber Security Role of Law Enforcement

As an organisation responsible for the maintenance of law and order and detecting and preventing crime the police are confronted with significant challenges in addressing both old forms of crime enacted in the digital environment and new forms of criminal activity enabled by ICT (Quille, 2009; Wall, 2007). Existing approaches to fighting real-world crime are often ineffective or inapplicable when dealing with crimes committed in cyberspace (Wall, 2007). Generally police roles have been described in terms of four key functions of enforcing the law, prevention, detection and investigation (UN, 2011). These functions can also be applied at the specific level and to police roles in responding to cybercrime. Enforcement of the law in this context relates primarily to monitoring and detecting breaches of cybercrime laws.

2.6.1 Prevention Role in Cyber Security

Preventing and mitigating cybercrime involves a range of policing functions. Roles can focus on raising awareness and understanding of cybercrime among the private sector and individuals to enable them to undertake precautions to protect against risks. The majority of breaches and incidents are the result of known vulnerabilities or human errors which emphasises the importance of a preventative approach (Gjesvik, 2019). Much of the preventative measures for securing critical infrastructures is undertaken by specialists in the infrastructure organisations (FireEye, 2019). Nevertheless, law enforcement in general has played a key role in working with organisations and the public to promote a prevention mindset. For critical infrastructures there is an implication for digital competency for law enforcement both in terms of their ability to advise and guide cyber security specialists on new developments and emergent threats and to share technical information. Law enforcement has a part to play in providing information, standards setting and increasing awareness of companies operating in critical infrastructures (EU, 2020). To perform this role effectively law enforcement would require sufficient knowledge and understanding of preventative methods undertaken in order to report. When threats are reported it is vital that law enforcement can understand which and how such measures were circumvented. Law enforcement are in a unique position in terms of their access to specific details of incidents that can enable them to assimilate and describe the incidents and then to share security updates with key stakeholders (Gjesvik, 2019). Increasingly prevention roles involve collaboration and knowledge sharing with partners and other agencies at local, national and international level.

2.6.2 Monitoring and Detection

Another function is to monitor and analyse cybercrime trends as well as to alert and advise on cybercrime risks and crimes. Cybercrime detection comprises functions such as monitoring and identifying cyber threats and cybercrimes and analysis and profiling of cybercrime activity. To achieve this police functions may also focus on developing strategies, tools and operational measures to identify and analyse cybercrimes.

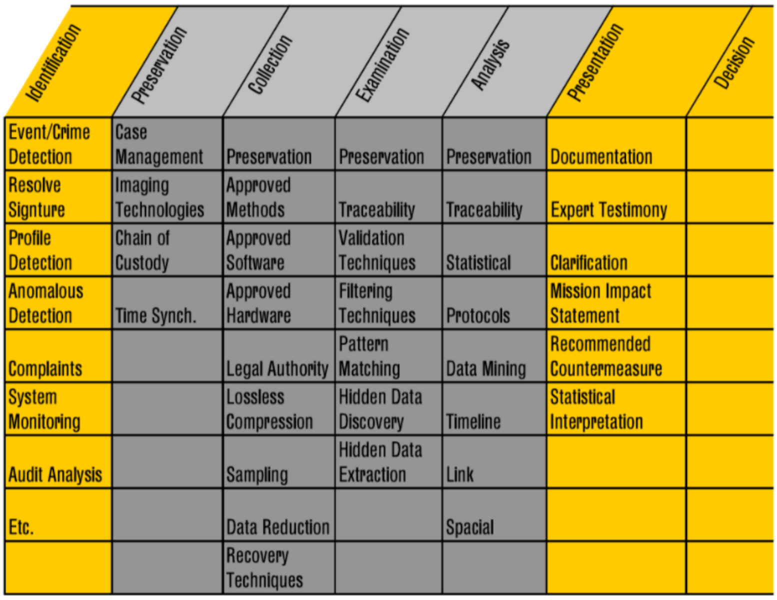
2.6.3 Cyber Attacks and Criminal Investigation

Criminal investigation reflects a complicated process that is highly complex to manage. Increasingly law enforcement need to possess capabilities to conduct investigations within a digital environment under each area of the criminal investigation process. Criminal investigation consists of a number of essential components: reported crimes; proactive investigations; information and evidence gathering; identification; witnesses and victims; covert techniques; database; trial preparation; partnership co-ordination; international partnership. Each of these areas has implications for CPI protection or responding to cyberattack in terms of possessing the necessary digital competencies in order to undertake these roles efficiently and effectively.

The US National Institute of Standards and Technology (NIST) identifies a four-phase process for conducting digital forensics: collection, examination, analysis and reporting (Kent et al., 2006). The law enforcement role in cybercrime investigation is founded on a digital forensic model which in turn is based on US FBI protocols for physical crime scenes. Undertaking digital forensics encapsulates seven key stages or processes of identification, preservation, collection, examination, analysis, presentation, and decision (Palmer, 2001, p.14) as depicted in Figure 2-4.

Cyber investigations are initiated in an identification phase that focuses on recognising and characterising cybercrime incidents through processes such as event/crime detection, profile detection, anomalous detection, monitoring and analysis (UNODC, 2019). Police next ensure that digital and physical evidence is securely preserved for analysis and presentation. This involves elements such as case management and chain of custody, imaging technologies and time synchronisation. The following stage focuses on evidence collection through the recording of physical and digital crime scenes using standardised procedures and techniques and approved methodologies, software and hardware (UNODC, 2019).

The evidence relating to the suspected crime is then subject to an in-depth and systematic search in the examination stage (Baryamureeba and Tushabe, 2004, p.3). Examination is accomplished by utilising processes and techniques such as traceability, filtering techniques, pattern matching, extraction of hidden data, or validation techniques (Palmer, 2001).



Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Figure 2-4 Phases of Cybercrime Investigations

(Palmer, 2001, p.24).

The evidence is then analysed and reconstructed using statistical techniques, data mining, timelines and protocols, the results of which are used as a basis to determine the significance of the evidence and to draw conclusions. Police are then required to present the evidence to judicial authorities for decision-making providing a summary and explanation of their conclusions. This involves documenting evidence in addition to providing expert testimony and clarification, and interpretations of the evidence (Baryamureeba and Tushabe, 2004; Palmer, 2001).

Cybercrime investigations have also been modelled as a five-stage process incorporating different sub-phases within each phase, as shown in Figure 2-5. In the Integrated Digital Investigation Model readiness is proposed as the initial stage which involves assessment of the capability of infrastructure and operations to undertake an investigation (Carrier and Spafford, 2003). In the deployment phase police detect the incident and following authorisation for an investigation assign human resources.

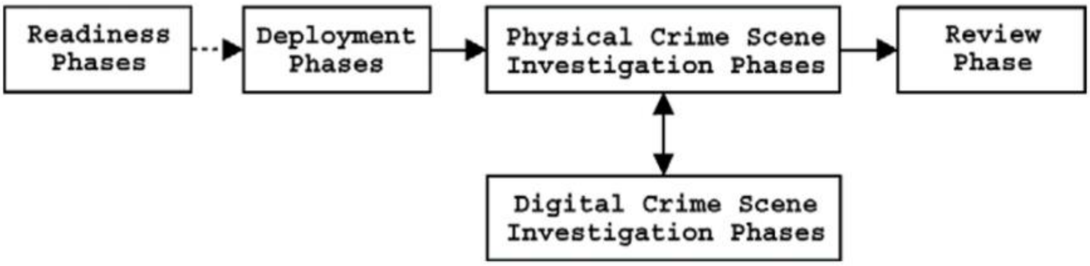

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 2-5 Phases of an Integrated Digital Investigation Process

(Carrier and Spafford, 2003, p.6).

The digital crime scene investigation phase mirrors the majority of phases in the previous model and involves securing and identifying digital evidence and documenting it, as well as acquiring and analysing it, reconstructing events, and presenting the findings in court. The model adds a final review phase aimed at assessing and identifying lessons to be learnt for future investigations (Carrier and Spafford, 2003).

Reporting of crimes for CPI incidents requires fast digital communications and understanding of escalations based on understanding of cybercrime incidents. Many law enforcement agencies have been challenged to respond effectively to cybercrime due to the complexity involved in defining it. As such offenses frequently exceed or lack traditional jurisdictions police agencies may be unaware that they need to respond or who should be the initial point of contact (Cross, 2019). In addition global entities may be in the best position to address certain types of cybercrime such as cyberterrorism or cyberwarfare (Brenner, 2006). In numerous situations understanding is lacking in relation to which types of cyber offenses are suitable to be addressed by municipal or state law enforcement.

Proactive investigations of cybercrime involve effective targeting, profiling, criminal intelligence and analysis of data. Information and evidence gathering involves analysis of digital crime scenes, software logs, databases or forensic analysis. Identification of perpetrators of cyberattacks will involve analysing a wide range of digital sources across computer networks and national boundaries. Covert surveillance requires a unique set of techniques to monitor and analyse patterns of activity across systems and may involve interception of digital communications, analysis of video records, use of online information, monitoring discussion groups, or nurturing informants online. Cybercrime investigations may involve accessing databases across agencies and co-operating internationally and in the public domain to gather intelligence and communication. They may also encompass developing automated algorithms to search and analyse activity and conduct deep learning, profiling or predictions (Cross, 2019; Carrier and Spafford, 2003).

2.6.4 Law Enforcement Cyber Security Challenges

The police face difficulties in tracing offenders in cyberspace due to the potential it offers for hiding identity within global ICT networks and the different methods and tools available for anonymous access, browsing, and communications (Lovet, 2009). Cybercriminals widely exploit opportunities for utilising proxy servers, anonymisers, and unprotected public wireless networks (Gercke, 2009). Crimes that have both an international dimension as well as hidden identities are complex and difficult to investigate (Tropina, 2017).

While criminal law and investigations are traditionally a question of national sovereignty cyberspace is borderless in that the criminals and victims of cybercrime may be located in different countries or even continents (Sofaer and Goodman, 2001). This implies cooperation between different countries involved in international investigations (Putnam and Elliott, 2001). Initiating investigations is difficult for police due to a lack of visibility of cybercrimes and a low level of reporting (Lovet, 2009) that for companies and organisations may be associated with several reasons: reputational damage, lack of knowledge that such crimes can be reported or lack of trust in the police (Wall, 2007; CSI and FBI, 2004).

Law enforcement agencies may further lack the resources to respond to cybercrime even where definitions are fully understood. Where agencies do not possess appropriate personnel and expertise to adequately investigate cybercrime victims may be less likely to report future crimes. This may have a deleterious effect as a lack of cybercrime reporting in sufficient numbers can undermine the motivation to commit police resources to cybercrime (Leppänen and Kankaanranta, 2017; Sommer, 2004; Wall, 1998).

Training is linked to resource availability and many police agencies may not possess well-trained officers who can respond to cybercrime. Recruitment of police officers does not focus on technological skills but rather aspects such as physical traits, critical thinking abilities, and emotional and psychological stability (Hogue et al., 1994). Moreover where training is provided it can be superficial and delivered in ineffective mediums (Forouzan et al., 2018). Debate exists within policing on whether all police officers should investigate cybercrimes or if this should be the responsibility of a smaller specialist group or team (Willits and Nowacki, 2016; Holt and Bossler, 2012). Evidence shows that officers having training in cybercrime are more likely to approach cybercrime seriously and spend longer in investigations (Lee et al., 2019).

Police officers also may not view cybercrime as seriously as traditional, real-world crime due to the lack of visibility and apparent harm, leading to the perception that such crimes do not involve ‘real’ police work. Some research indicates that police officers can shift responsibility for cybercrime to the victims or other elements of the criminal justice system such as courts. This suggests the potential for greater online precautions and more punitive sentencing from courts to have more effectiveness than police responses (Bossler and Holt, 2012).

2.6.5 Review of Cybersecurity Skills

Information security has been recently re-branded as cyber security or e-crime – which generates debates as to what extent is the difference between information security experts vs. cyber security expert (Wall, 2007). Some see the two as mutually exclusive – while others see the two as complementary and other group of scholars consider the two to be a continuation of one another – thus synonymous (Furnell et al., 2017).

Cyber security is broad with no one universally agreed definition, but entails a range of specific specialisations such as network security and architecture, digital forensics etc (Furnell et al., 2017; Willits and Nowacki, 2016; Hunton, 2012). While the debate continues in regards to semantic differences of terminologies (Wall, 2007; Hunton, 2012), there seems to be a consensus that police agencies have trouble finding suitable digitally competent cyber police (Furnell et al., 2017; Bhaskar, 2006; Wittes, 1994). In particular, studies have pointed to a global shortfall of up to 2.72 million security practitioners in 2021 (ISC2, 2021). This potential shortfall raises global concern in regards to shortage of cyber-security specialists as organisations with weak digital –cyber capabilities are likely to spend three times as much to recover from security breaches (Furnell et al., 2017).

The rapid evolution of cyber security intelligence means that there is consistent change in job-related requirements. Nevertheless the ongoing creation and definition of job roles in the profession has implications for the recruitment of expert talent. The need for cybersecurity expertise is growing, but with talent scarce and at a premium, it can be difficult, and in some instance unfeasible, for smaller businesses to hire full-time members of staff in security roles. However, one way that you can potentially bridge the gap is to provide training for your existing technical and IT staff in all aspects of cyber security. For example, if you have a web developer, it can be hugely valuable to improve their understanding of the latest types of web application security risks and how your business web site can be protected against them. Implement an on-going training programme that includes everything from specialist courses, attending industry events, reading and webcasts. It can be a good idea to set up a specialist development plan for individual team members to ensure that they are on the right track and have the knowledge they need. Mentoring is also a good option. Have junior employees spend time with colleagues that are more knowledgeable about cyber security for a hands-on learning experience. It is important to remember that every hiring decision that you make needs to be taken with cyber security in mind. If you are hiring staff in any kind of technical position you should make sure that you assess their knowledge of, and attitude towards, security during the interview process. This can help to ensure that new staff entering the business take the correct approach to cyber security and help to foster an awareness culture. If you are in a position to hire for a role with a specific emphasis on security you may also encounter the problem that you don't know exactly what skills you require. Without a security expert already in the business it can be difficult to know how to assess the knowledge and suitability of candidates. The fact is that the gap in cyber security skills comes at a time when cyber-crime is increasing, as is the sophistication and skill level of hackers and cyber-criminals. With cases of hacking and data theft on the increase, the cybersecurity skills gap can seem like a major problem. This is especially for smaller businesses without the resources to hire security-focused technical staff. Nevertheless, it is important to take action, as if your organisation lacks the knowledge and resources required to safeguard against the latest threats it could be become an easy target.

Cyber security represents a domain that should be entrusted to skilled professionals. This raises the questions of what skills are needed for a person to be a competent cyber security personnel (Furnell et al, 2017). For many years the major concerns within the cyber space has been on the technical point of view of networks. There is little emphasis on the human dimension of cyber security (Smith, G. 2018). Specific training and realistic exercises procedures and supporting systems are required to help a country to become more resilient in order to deal with cyber attacks. Cyber attack life cycle steps include reconnaissance, initial compromise, command and control, lateral movement, target attainment and exfiltration, corruption and disruption. No level of protection or prevention is full proof protection hence cyber security requires more that technical capabilities but also knowledge of awareness of the possible cyber threats (Nevmerzhitskaya et al., 2019).

This trend of demand for cyber security specialists outstripping the supply affects security agencies the most (McMurdie, 2010; Furnell et al., 2017), hence the urgent call by experts to invest more resources in training for digital competences and infrastructure.

The skill set necessary to carry out certain cybercrimes has implications for its detection. Traditional methods of combatting crime are therefore unlikely to enable effective detection and tracking of such crimes and most crimes emerge as a result of victim or observer reporting and are challenging to investigate even when known (Willits and Nowacki, 2016, p.106).

As discussed above, since finding cyber security experts/specialists presents difficulties, an alternative would be to develop and train in-house talent (Furnell et al., 2017). This call is vital since it is very difficult to for example find an expert with all varied specialisations and certifications in network security, digital forensics, information security etc. The fundamental question that arises is in regards to whether it is the breadth or depth of knowledge or skills that are most fundamental in a certain cyber security threat domain, in other words generalist vs. specialist skillsets (Falcone et al., 2002).

Kaspersky Lab report states that: “Care needs to be taken about how much we regard graduates as being directly ‘qualified to work’ in the IT security field. Even as degree graduates, I would not necessarily regard them as qualified practitioners. They should certainly have a good level of supporting knowledge and some of the skills, but there will equally be various aspects that they have not been able to put into practice ‘for real’ at that stage” (Furnell, 2017).

In view of the above, to tackle the shortage/skills gap, it is imperative to develop expertise in some of the following areas: a) network certifications to enable the policing of network security and risk management; b) certified ethical hacking techniques to enable the police to understand advanced hacking techniques employed by hackers; c) security essentials certifications for information security to enable the police to promote and comply with security practices with global standards and in addition be able to manage, design, oversee societies information security; d) certified information system security to enable police officers with deep proven technical as well as managerial competences, skills, and experience design, engineer, implement, and manage sophisticated attacks on the nations cyber infrastructural assets. In addition to above, it is also imperative for the security agency to categorise and prioritise their training in regards to skills groups as shown in **Error! Reference source not found.**.

Table 2.2 Knowledge, Skills, & Capabilities

Task	***Knowledge and Skills Required***	***Capabilities***
Threat Intelligence Assessment and Modelling	Level 1: Knowledge	Can describe concepts and principles of threat intelligence and modelling
	Level 2: Knowledge and Understanding	Experienced in applying threat intelligence and modelling principles in training in training or academic environment example test or examination
	Level 3: Apply	Can undertake routine threat intelligence modelling tasks under supervision
	Level 4: Enable	Can undertake complex threat intelligence and modelling without close supervision
	Level 5: Advice	Capable of managing threat intelligence in teams without supervision
	Level 6: Initiate	Leads, advises and reports threat intelligence to the Board or highest authority/example government

(adapted from Furnell et al., 2017).

Although there is no one universal framework for closing the knowledge/skills gap of cyber security the previous framework provides a useful guide. For example, it could enable UAE police force to first categorise their knowledge and skills gap based on priority and approach the training schemes identified in the preceding table.

2.6.6 Cyber Policing Strategies: Enforcement & Jurisdictional Challenges

The digital age is acknowledged by scholars as necessitating novel methods of enquiry, and the introduction of new understandings and concepts in relation to how individuals' digital selves are created, recreated and presented (Dholakia & Reyes, 2013; Hansen, 2013).

The concept of personhood (status of person in a digital real) had undergone change over the years due to technological advances (Kerrigan and Hart, 2016). These changes have profound implications in regards to policing cybercrime as individuals especially Millennial and digital natives tended to have multiple digital identities and poses more security challenges (Kerrigan and Hart, 2016; Liang et al., 2014; Wall, 2007).

The issue of multiple digital identities complicates investigations and digital/online surveillance by police due to nuances of meaning which arises when individuals choose to construct/represent themselves digitally but sharply contrasts self-reflection of self-provided by others (Kerrigan and Hart, 2016). For example, one could imagine the level of complexity involved in a law enforcement investigation where a supposedly digital person commits crime with multiple online identities in different legislative jurisdictions (Hunton, 2010). Such legislative complications must be resolved in the light of inter-jurisdictional cooperation of the police (Hooper et al, 2013). It is quite challenging as online identity could be likened to 'theatrical performance' leading to front vs. backstage personas (Goffman, 1959). The former (front – online representation) is driven by impression management, while the latter (backstage representation) is hidden and private (Goffman, 1959). Through impression management users on social media to selectively disclose 'fantasised' ideal self in multiple online spaces sometimes deceptively (Higgins, 1987; Leary & Kowalski, 1990; Donath, 1998). The big question for cyber police has now become to what extent can these fantasised 'ideal' self can be relied upon?

To answer the above, it is noteworthy for a police force to turn to theories of identity which that questions the notion of fixed identity, in favour of dynamic narrative and social time on a digital enclosure (Shankar et al., 2009). Our digital personhood is in continuous state of transition (liminality), making investigations in to digital traces and transitions difficult to achieve (Turner, 1960). Research on digital identity construction in social media uses a dramaturgical approach to examine biographical films of users and finds that it is quite challenging to sustain digital representations over time (Kerringan and Hart, 2016). The authors suggests strategies for dealing with temporal shifts and separation of selves (Kerrigan and Hart, 2016), but the temporal nature of digital identities (changing with time), presents greater challenge for police surveillance in a digital age especially if it focuses on a snapshot of an on-going situation (Ball, 2002).

Other additional challenges for cyber policing (social media) are confounded by social media leakage which often leads to misrepresentation or an undesired digital self as content change hands through processes of interpretive-re-enactment (gossips and rumours) (Solove, 2007; Belk, 2013, 2014). A misrepresented persona based on reflection of other digital natives could be counterproductive to cyber policing. This is due to the ubiquitous nature of the networked, nodal of cyberspace (Johnson and Sheering, 2003). There have been attempts internationally at reforming legislations to empower and give police more investigative powers as discussed in the subsequent sections.

As demands outstrip supply of cyber security specialists globally, the need to embark on strategies for long term solutions becomes crucial. Many experts point to the fact that there is gap which needs to be bridged. According to Bryant et al., (2008), police forces are unprepared to address growing cybercrime demands in terms of the availability of trained resources. It has been suggested that law enforcement remains badly-equipped at every level to deal with the extent of cybercrime occurring (McAfee (2008). The police now more than ever require new models of law enforcement investigations to combat cybercrime (Hunton, 2010). Despite scepticism expressed above, there some initiatives/strategies around the globe which could be considered a good practice (Yar, 2006).

Social media and policing is one approach to addressing the policing of cybersecurity for CPI. To have a detailed understanding of social media policing and strategy, one needs to utilise the theoretical interfaces of sociology, criminology (routine activity theory), as well as undercover (policing) (Trottier, 2011; Zedner, 2007; Yar, 2005). The ability of social media platforms to allow technology for domestication of everyday life presents interesting social dynamics with visibility to the police in ways unachievable before (Trottier, 2012; Ericson and Haggerty 1997).

Unlike traditional policing techniques with origins from military, the social media had origins in the sociology of human interaction, sharing, and visibility in University life (Trottier, 2012). Information about individuals that use to be institutionally invisible, have suddenly become a de facto tools for criminal investigations – through searchable ephemeral details (Trottier, 2012). Since social media platforms are social spaces before becoming de facto investigative tools, and then the role of sociological theories takes precedence.

For example, prior evidence suggested how visibility of social ties has become a source of evidence for investigators on one hand, and a source of insecurity for the criminal suspects (Trottier, 2012). This has increasingly become the case as the digitisation of social ties has enabled the police to make more sense of domestic relationships, peer-to-peer relationships, and identity (Trottier, 2012). Social media saturation have also made impossible to fully trace the authenticity of the 'digital personhood' – hence individuals could create believable narratives of themselves in a dramatic way (Goffman, 1959). However, experts argue that, by utilising range of tools undercover policing (through enrolling users) to aid conjointly in criminal profiling of digital footprints – police could minimise the tendencies of cybercrime perpetrated (Li and Bernoff 2008; Shirky 2008). For example, while social media enable rioters to mobilise support, it also help identify suspected rioters (Trottier, 2012).

Since social media platforms tend to act more like a digital enclosure – they provide an invaluable source of convergent information and mutual augmentation of social reality by a mere single act of lateral surveillance (Andrejevics, 2005; Trottier and Lyon, 2011). As public interactions, relations, and events and other related social life activities are mediated on social media platforms – they present the police with more visible and useable information to aid investigations and surveillance (Trottier, 2011). In so doing, and in the context of theoretical criminology, it can be argued that social media platforms aid pre-emptive policing (Zedner 2007).

The above suggests that, it is imperative for social media police to be able to engage in investigation and surveillance by social association of network of friends, sites visited, groups belonged, fans club etc (Andrejevic, 2005; Ball, 2002). Social media policing is therefore associated with the capability of the police investigators to piece together a big picture of 'socio-technical self' and digital identity of perpetrators of crime online through surveillance (Lyon, 2001). The approaches employed in social media policing is underpinned in sociological theories of narcissism – since even people with issues to hide tend to share their lives with others (Cheng, 2010).

Social media content have now been scrutinised to investigations of quality of social life in for example investigations of insurance fraud (Millan, 2011), to extreme private cases of divorce (Popken, 2011). Some successful strategies used includes 'fake persona' (so called authentic fake profiles online –based on fictional identity) and deception : to enable investigators befriend suspected users on social media, possibly circumventing targets privacy settings, enabling them to place themselves in a context of information sharing and disclosure thereby maximizing investigative gains with low risk (Zetter, 2010; Kerringan, 2011). United States Homeland Security have utilised this strategy to enable them create and manage several authentic fake profiles online – often scrutinizing applicants for citizenship (Kerringan, 2011). In addition to above, social media have made the practice of 'snitching' (a barter system between police and public in which targets are approached through their peers) less risky for informants (Shirky, 2008; Natapoff, 2009).

Having mentioned that social media platforms are increasingly gaining traction as de facto tools for investigations – critiques argue that, there is still no universal consensus on its content interpretation on issues regarding digital enclosure, privacy, and exploitation (Andrejevic, 2009). Some scholars express scepticism in regards police utilisation of social media content as basis for investigation and surveillance – since digital personhood is highly contentious (Kerringan and Hart, 2016). The real person behind the post – could be an 'idealised' instead of 'authentic' version of self and could use pseudonyms to hide their identity (Goffman, 1959; Kerrigan and Hart, 2016; Bullinghan and Vasconcelos, 2013).

Another criticism had been labelled against police use or tapping in to interpersonal vulnerabilities which might arise out of genuine social need to mitigate for distant relationship, coping with isolation, maintain bonds, and seeking validation (Trottier, 2012). Another criticism arises as experts express that sometimes the visibility of social networks like memorial groups for murder investigations on social media further complicates investigative process when near lead is shared through perhaps photographs/videos etc. (Trottier, 2012).

2.7 Conclusion

The purpose of this chapter was to present a detailed research context that elaborate on the drivers and the goals that influence the development of digital competency framework for law enforcement in the area of CPI. Firstly, cybercrime was defined and discussed in terms of the categories, types and techniques that have implications for cyber security practices and necessary digital competencies to combat different cyber security threats to CPI. A discussion of criminal innovation underlines the different and evolving patterns of cybercrime that has implications for development of digital competencies to maintain pace with rapid change. In addition, this chapter provides a discussion on the critical infrastructures and CIP in relation to the key dimensions and challenges that inform the development of digital competencies. Finally, the role and function of law enforcement was discussed in terms of the broad roles and responsibilities, cyber security and in relation to cyber security of CIP. This has implications for defining digital competencies in relation to different functions of policing in cyber security and in relation to CIP. In conclusion, this chapter provided an essential underpinning to focus the literature review and research process on the digital competences relevant to law enforcement in the specific area of cyber security for CPI.

Chapter 3 Review of Seminal Literature on Digital Competencies

3.1 Introduction

The purpose of this research is the development of a digital competency framework for law enforcement that enhances the cyber security of critical physical infrastructure (CPI). This chapter undertakes a review of the literature to establish existing knowledge and theory that is relevant to this research goal. Firstly, the concept and theory of competency is reviewed to provide a broad conceptualisation of competency and specifically to define and identify key elements and models of digital competency. A second area of this review focuses on defining and classifying cyber security competencies and explores the theories and models in this area. Thirdly, this review examines extant knowledge in the literature focused on digital competencies for CPI and identifies the key concepts at different levels and areas. In reviewing the literature a digital competency framework for cybersecurity in CIP for law enforcement is lacking. Based on this review a conceptual framework is developed that integrates the different theory and concepts for competency, digital competency, cyber security and CIP to guide the research investigation to determine the constituent elements of a framework relevant to the different functions of law enforcement for CIP.

3.2 Competency

Competences represent a mechanism for organisations to guide the development of employees that aligns with sector or organisational needs (Petersen et al., 2020). The dictionary definition of competency states it as the capability and possession of sufficient skills or training to perform an activity (Ala-Mutka, 2011). Competency also refers to the proven ability to use them in work or study situations and in professional and personal development (Piersarskas et al., 2020; Ala-Mutka, 2011; European Parliament and the Council, 2006). A broad definition of competency is the capability to use knowledge, skills, abilities, behaviours, and personal characteristics to effectively carry out key work tasks, specific functions, or operate in a particular role or position (Newhouse et al., 2017). Modelling competencies depends on a number of factors including considering the organisational context, goals, future job requirements, rigorous job analysis and defining different levels of competencies (Campion et al., 2011, p230).

Knowledge, skills and abilities (KSAs) are identified as three core components of competency. Knowledge, skills and abilities are associated with the possession of relevant education, training or experience (Ala-Mutka, 2011). Knowledge is directly employed in the performance of a function and represents product of information assimilated from learning and comprises a body of facts, principles, theories and practices related to a specific area of work or study (European Parliament and the Council, 2008). Skills refers to the ability to employ knowledge and know-how in the resolution of problems and completion of tasks (Ala-Mutka, 2011). Skills can refer to tangible capabilities such as physical manipulation of tools, instruments or methods and processes (Petersen et al., 2020) or logical, intuitive and creative thinking (European Parliament and the Council, 2008). Skills can also be defined at a sector level such as cybersecurity skills (Petersen et al., 2020). Ability as a competency component refers to the competence to perform an observable behaviour or a behaviour that results in an observable product such as completion of a task (Newhouse et al., 2020, p.6).

Competency can also be characterised as attitudes that influences knowledge, skills and abilities. In the European Qualifications Framework (EQF) attitudes is a key component alongside knowledge and skills. This is consistent with the OECD (2005, p.4) which explains that: “A competence is more than just knowledge and skills. It involves the ability to meet complex demands, by drawing on and mobilizing psycho-social resources (including skills and attitudes) in a particular context”. Attitudes are considered the motivators of performance and include values, ethics and priorities which provide the foundation for ongoing competent performance (Ala-Mutka, 2011).

The literature also characterises different levels of competency. The NICE framework (Petersen et al., 2020) for cybersecurity education identifies three levels of competency which are based on the performance of behaviours and the degree of knowledge and awareness. At the basic level performance demonstrates a fundamental knowledge/awareness of the competency. At an intermediate level substantial knowledge/awareness is demonstrated in the performance of individuals who are considered fully and independently capable to perform work. At advanced level individuals exhibit exceptional knowledge/awareness of the competency and are considered experts.

Tobey et al., (2012) advances a multidimensional model of competency knowledge, skills and depth and consistency of knowledge. Competency can be categorised from novice to master based on performance in each of these dimensions. For instance in Figure 3-1 a master will have consistent skills, a deep knowledge of strategy or procedure and a broad ability to transfer across domains.

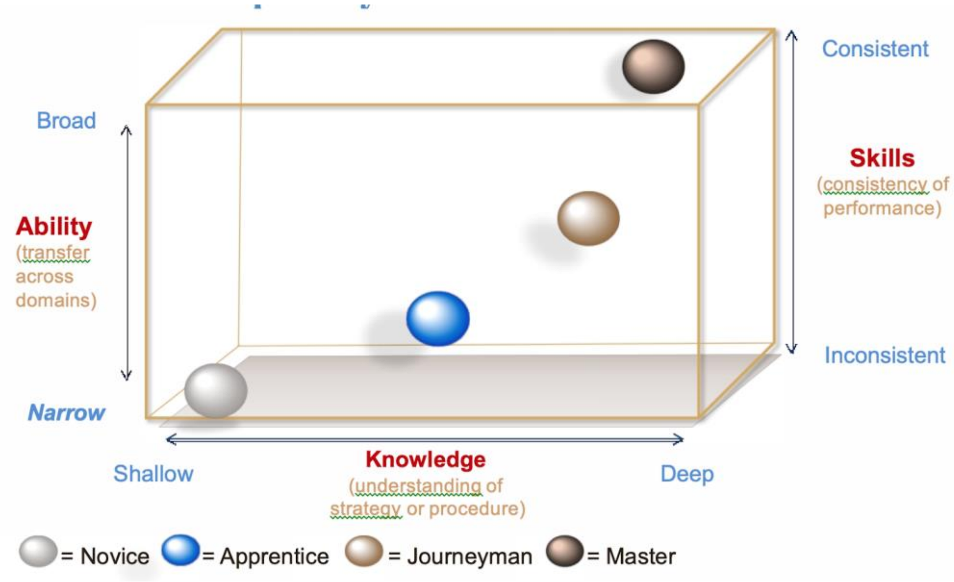


Figure 3-1 Tobey et al., (2012) Competency Model

(Tobey et. al., 2012, p.6).

In the area of policing competencies have similarly been divided into levels reflecting a cumulative process from low to higher level. For instance in the UK policing college, a competency framework addresses different roles of practitioner, middle manager and senior manager (College of Policing, 2018).

3.3 Digital Competency

The concept of digital competence is novel and has yet to be clearly defined given that only a modest number of studies have examined this phenomenon in respect of digital competence or digital skills (Ilomaki et al., 2016). Recently discussion has increasingly centred on the concept of digital competence as a measure or frame to comprehend the understanding and skills people require in the current digital society. The term digital identifies information that is formatted in a numerical manner and predominantly employed by computers, and literacy means the capacity to read and understand media and to produce data and images by means of digital manipulation as well as being able to assess and utilise new knowledge acquired from digital environments (Ilomaki et al., 2016).

In turn digital competence is the latest concept applied to technology-related skills following the use and evolution of several other terms including technology skills, information technology skills, ICT skills, 21st century skills, digital skills, information literacy, and digital literacy (Ilomaki et al., 2016; Ilomaki et al., 2011). It can be a reflection of both governmental beliefs and desires in relation to future needs as well as the economic competition in which the term has its roots, wherein new technologies are considered to be both opportunity and solution (Ananiadou and Claro, 2009; Sefton-Green et al., 2009; Punie, 2007). The term digital competence is often employed synonymously with digital literacy (Adeyemon, 2009; Krumsvik, 2008). Some terms such as “Internet skills” identify a specific area of digital technology while others such as media and literacy have broader meaning. Jenkins et al., (2006) explore digital skills in terms of skills needed in the modern era placing emphasis on social skills rather than individual technical skills.

Further, it is evident that digital competence reflects a multidisciplinary concept reflecting a range of elements from different fields as shown in Figure 3-2. In a review of terms used in the literature to describe digital competence, digital literacy emerges as the most utilised expression followed by new literacies, media literacy, multiliteracies and digital competence (Ilomaki et al., 2016). Digital literacy remains difficult to define, nevertheless UNESCO have identified digital literacy as “the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship" (Law et al., 2018, p.3).

Digital literacy is identified variously as information literacy, media literacy, ICT literacy, and computer literacy (Robertson, 2019). Such definitions imply digital literacy is a combination of skills and competencies (Sharma et al., 2016; Reedy and Goodfellow, 2012), and is a cognitive operation that goes beyond practical skills to integrate higher level cognitive skills such as analysis, processing, and generation of information and understanding (Xiong, 2016; Osterman, 2013; Davies, 2011).

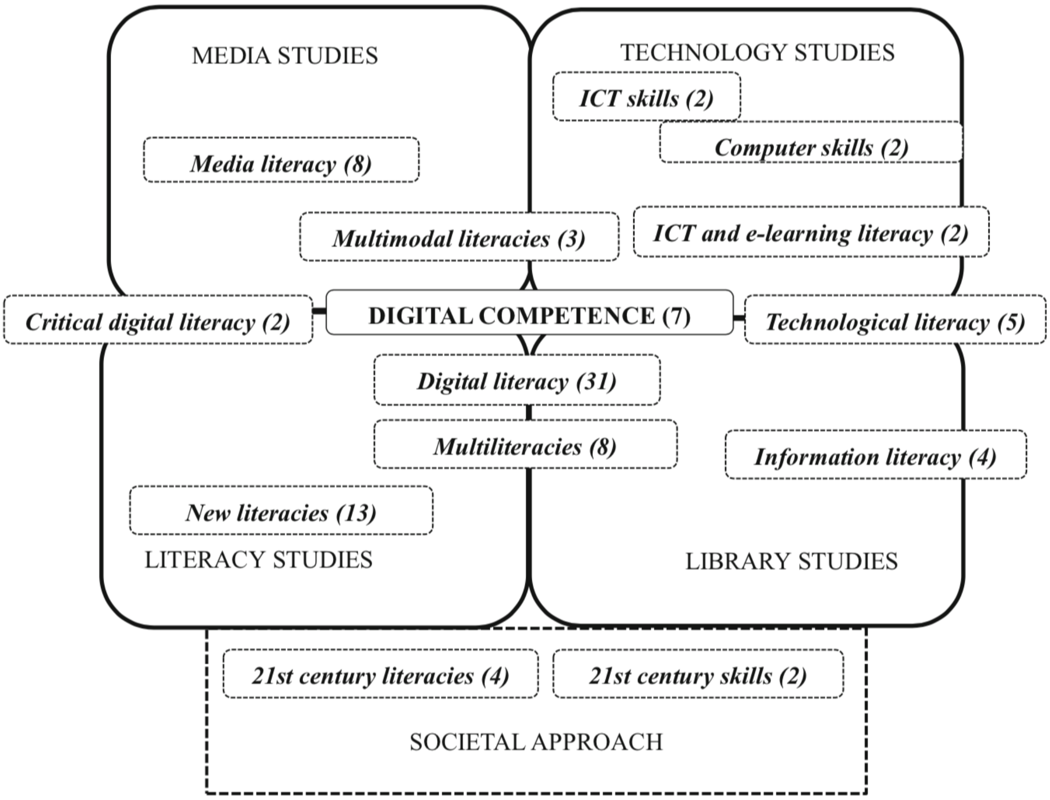


Figure 3-2 Multidisciplinary View of Digital Competence

(Ilomaki et al., 2016, p.670).

As shown in Figure 3-3 digital literacy is also characterised in terms of social interactions and connections combining both information skills and communication skills (Van Es and Schafer, 2017; Reedy and Goodfellow., 2012) or collaboration, teamwork, and social awareness. Leu et al., (2004) contend that the new literacies associated with ICT and the internet enable individuals to distinguish critical questions, find information, evaluate its utility, synthesise the information to address these questions and further transmit the answers to others.

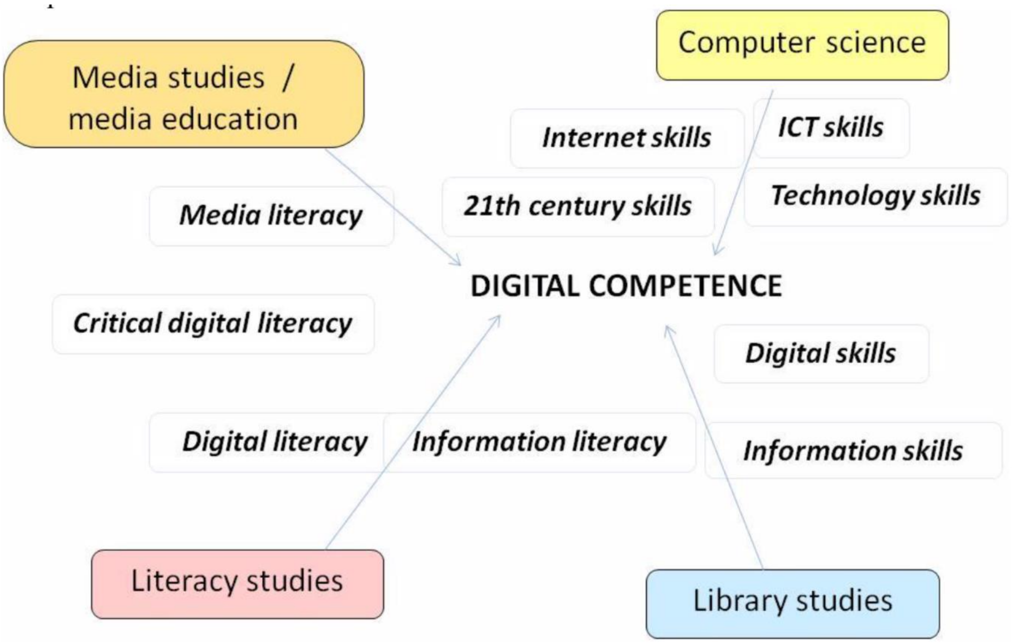


Figure 3-3 Digital Competence and Related Competence

(Ilomaki et al., 2011, p5).

One definition by Jones and Flannigan (2008) situates digital literacy in the specific context of digital environment that represents a person's ability to perform tasks effectively in a digital environment. Other research on digital literacy further characterises it in terms of: information technologies, understanding information, search abilities, communicating information (Bawden, 2008; Campbell, 1990); critical thinking (Campbell, 1990; Hague and Williamson, 2009). The concept of digital literacy has been employed in some law enforcement agency development programmes as a distinct component. In Canada a review of Police Sector Council (PSC) competency framework resulted in a proposal for the inclusion of digital literacy as a core competency alongside cognitive, behavioural and leadership (Stoetzer and Robertson, 2019).

Media studies is another field which contributes to the concept of digital competence. Work by Lee (2010) centred on media literacy terms and contents and identified the competences required by a media literate individual in the 21st-century including awareness of the influence of media and understanding of the operation of media. On a broader level computer and ICT skills have been defined as a component of digital literacy and digital competence (Delfino, 2011). The term 21st-century skills or competence is almost synonymous with digital competence and has a similar background in terms of identifying policy or societal requirements for delineating and enhancing core competences within a fast-moving digital society (Annetta et al. 2010). On a practical level however what digital competence actually entails is less clear (Janssen et al., 2013). At the very least there is commonality with general descriptions in that digital competence can be defined in terms of knowledge, skills, and attitudes which can be organised in a hierarchical manner (Cheetham and Chivers, 2005).

The increasing use in the literature of the term digital competence over digital skills signifies the shift towards a broader and more in-depth understanding of these concepts (Ilomaki et al., 2011). This is consistent with OECD (2005) definitions of competency which assert that it comprises more than just knowledge and skills but also psychosocial factors such as attitudes that can be mobilised in a specific context. This view is reflected in the most recent and broadest definitions of digital competency which propose that it entails not only digital skills but also social and emotional elements for understanding and using digital technologies (Ilomaki et al., 2011).

3.4 Models of Digital Competency

A number of digital competency frameworks are identified in the literature all of which are focused on the general public and define key components and concepts. A model of digital competency by Ala-Mutka (2011) comprises three broad components that range from lower order to higher order each of which define key skills and knowledge for that level. As shown in Figure 3-4 'instrumental' skills and knowledge comprise the basic skills necessary for engagement with digital technologies that in turn provides a basis for 'advanced' knowledge and skills. These are the core competencies that can be applied in all content domains and task objectives in the digital context. In the highest order theme attitudes are identified for the application of skills and knowledge that represent ways of thinking and motivations for undertaking actions that influence individuals' digital activities (Ala-Mutka, 2011).

Bawden's (2008) model focuses specifically on digital literacy and similar to Ala-Mutka (2011) incorporates three core components and critical competences for each component: instrumental skills and knowledge; central competences that integrate digital and information literacy; and attitudes and perspectives that support individuals to learn what is needed for their specific situation.

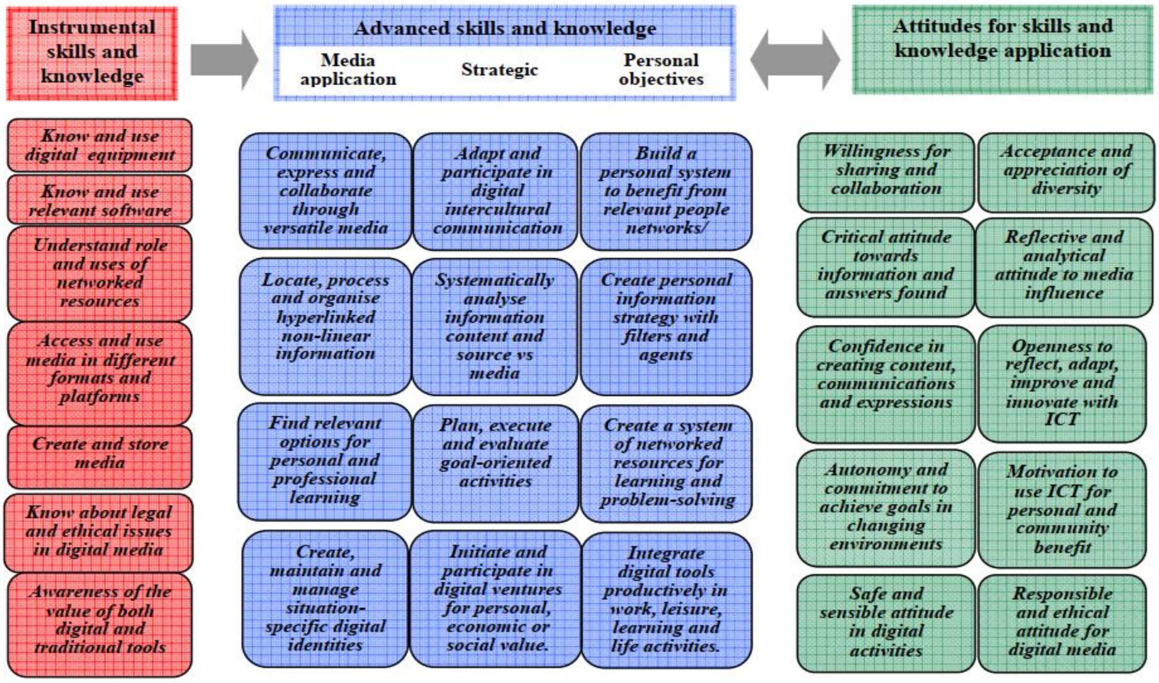

Instrumental skills and knowledge
Advanced skills and knowledge
Media application
Strategic
Personal objectives
Attitudes for skills and knowledge application
Know and use digital equipment
Know and use relevant software
Understand role and uses of networked resources
Access and use media in different formats and platforms
Create and store media
Know about legal and ethical issues in digital media
Awareness of the value of both digital and traditional tools
Communicate, express and collaborate through versatile media
Adapt and participate in digital intercultural communication
Build a personal system to benefit from relevant people networks/
Locate, process and organise hyperlinked non-linear information
Systematically analyse information content and source vs media
Create personal information strategy with filters and agents
Find relevant options for personal and professional learning
Plan, execute and evaluate goal-oriented activities
Create a system of networked resources for learning and problem-solving
Create, maintain and manage situation-specific digital identities
Initiate and participate in digital ventures for personal, economic or social value.
Integrate digital tools productively in work, leisure, learning and life activities.
Willingness for sharing and collaboration
Acceptance and appreciation of diversity
Critical attitude towards information and answers found
Reflective and analytical attitude to media influence
Confidence in creating content, communications and expressions
Openness to reflect, adapt, improve and innovate with ICT
Autonomy and commitment to achieve goals in changing environments
Motivation to use ICT for personal and community benefit
Safe and sensible attitude in digital activities
Responsible and ethical attitude for digital media

Figure 3-4 Model of Digital Competence

(Ala-Mutka, 2011, p.6).

Another model for digital competency by the DigEULit project focuses on mapping the development of digital competences onto the circumstances of the individual (Martin and Grudziecki, 2006). Three stages of development are proposed of digital competence (skills, concepts, attitudes), digital usage (professional/discipline application), and digital transformation (innovation/creativity) that describe generic, personal and professional competences (Martin and Grudziecki, 2006).

A model by Janssen et al., (2013) identified twelve digital competence areas based on experts' collective views. Figure 3-5 shows how these competencies relate and are arranged so that proficiency levels increase as the central blocks move upward. 'Core' competences related to every day usage are connected at higher levels to creative work and expression. These are supported on the left side by collaboration and communication competences which are mediated by technology, and competences in respect of information processing and management on the right.

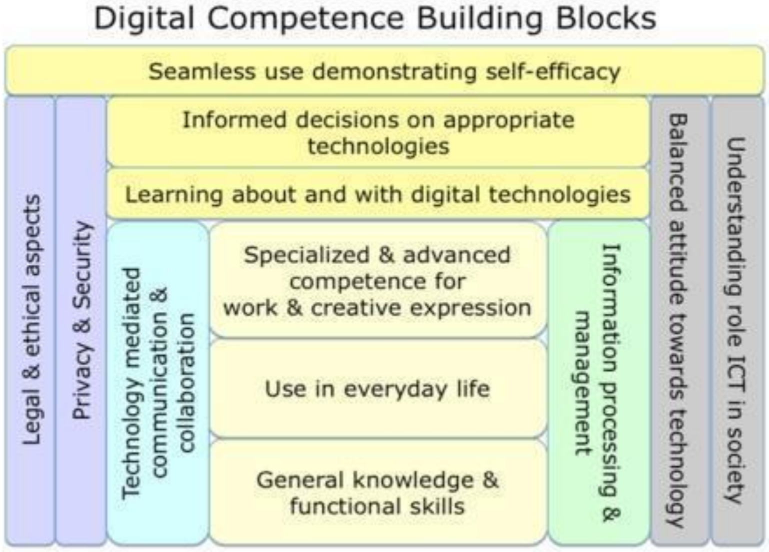

Digital Competence Building Blocks
Seamless use demonstrating self-efficacy
Informed decisions on appropriate technologies
Learning about and with digital technologies
Legal & ethical aspects
Privacy & Security
Technology mediated communication & collaboration
Specialized & advanced competence for work & creative expression
Use in everyday life
General knowledge & functional skills
Information processing & management
Balanced attitude towards technology
Understanding role ICT in society

Figure 3-5 Digital Competence Building Blocks

(Janssen et al., 2013, p.6).

Van Deursen et al.'s (2010) model of digital competence centres on Internet skills and defines four primary categories presented in order of complexity: operational skills and formal Internet skills, which are medium-related; and content-related skills of information Internet skills and strategic information skills. In Europe a digital competence model for its citizens consists of 21 different competences in five areas: content-creation; information; communication; problem-solving; and safety (Ferrari, 2013). Investigation of frameworks describing digital competence development has identified seven overarching competence domains: communication and sharing, collaboration, information management, content and knowledge creation, technical operations and ethics and responsibility (Ferrari et al., 2012).

3.5 Cyber Security Competencies

Cyber security is a multi-dimensional, complex and highly subjective concept (Bogdanoski et al., 2019). It is defined as “the protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so” (UK Gov 2018, p.20). Study of the varied technical and non-technical requirements for cybersecurity skills for organisations identified cybersecurity skills as the “combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to:

- Understand the current and potential future cyber risks they face
- Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation
- Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face.
- Meet the organisation’s obligations with regards to cyber security, such as legal obligations around data protection
- Investigate and respond effectively to current and potential future cyberattacks, in line with the requirements of the organisation”

  (Pedley et al., 2018, p.11).

Cybersecurity skills have been addressed by different frameworks that have attempted to provide a comprehensive guide to the types of skills required to ensure cybersecurity. Two frameworks have been developed in both the US and Europe focused on comprehensively defining competencies for professionals and organisations in cybersecurity.

3.5.1 National Initiative for Cybersecurity Education (NICE)

Frameworks specific to protection of critical infrastructure are still under consideration by some governments with the option to apply the United States’ National Institute for Cybersecurity Education (NICE) as a model (JCNSS, 2018).

NICE (Petersen et al., 2020) provides a national level cybersecurity framework that offers a common language of the cybersecurity work and of the individuals who carry out that work. It defines seven categories of functions across thirty-three areas of speciality that professionals should be competent to perform. This describes the knowledge, skills and tasks required to undertake cybersecurity work by teams and individuals and enables organisations to develop their workforces and learners to engage in appropriate learning activities to develop their cybersecurity knowledge and skills. In turn this development is advantageous for employers as well as employees by identifying career pathways and documenting how to prepare for cybersecurity work using the data of Task, Knowledge, and Skill (TKS) statements bundled into Work Roles and Competencies.

The competences in the NICE cybersecurity workforce framework defines knowledge, skills and abilities associated with cyber security necessary for work tasks based on the structure in Figure 3-6.

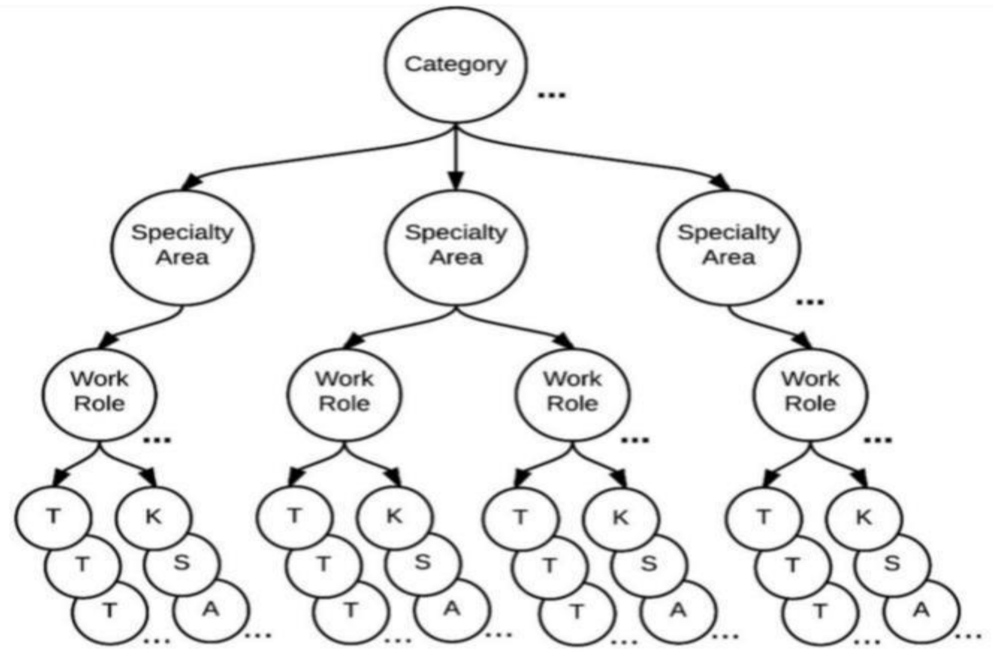


Figure 3-6 Structure and hierarchical relationships of NICE Framework

(Petersen et al., 2020, p.6).

Within a speciality area different work roles each provide a detailed grouping of cybersecurity work that incorporates a requisite list of competencies divided into knowledge, skills, and abilities (KSAs) and tasks performed in that role. According to the framework: “Competencies define the skills/capabilities critical for successful job performance across cyber roles, and the behaviours that exemplify the progressive levels of proficiency associated with these competencies” (Petersen et al., 2020, p.4). The NICE is the most comprehensive cybersecurity skills and education framework consisting of 7 top level cybersecurity functions; 33 speciality areas reflecting distinct areas of cybersecurity; 52 work roles that provides detailed sets of cybersecurity identifying specific knowledge, skills, and abilities (KSAs) that are necessary for these work roles.

3.5.2 Europe Model of Cybersecurity

The SPARTA framework of cybersecurity competencies shown in Appendix 1 aligns with that of the NICE framework and contains seven skills categories of: analyze; collect and operate; investigate; operate and maintain; protect and defend; securely provision; and oversee and govern. Each category is associated with several speciality areas which in turn are linked to descriptions of the key activities and skills.

3.5.3 Cyber Security Body of Knowledge

Developed by academics and experts in cybersecurity the Cyber Security Body of Knowledge (CyBOK) depicted in Figure 3-7 is a comprehensive model of cybersecurity competences that aims to codify the cyber security knowledge which underpins the profession (Cybok.org, 2020). In total 19 knowledge areas are described in relation to systems, infrastructure and software security that further incorporate human, organisational and regulatory aspects of cyber security on the one hand and technical areas of attacks and defences on the other.

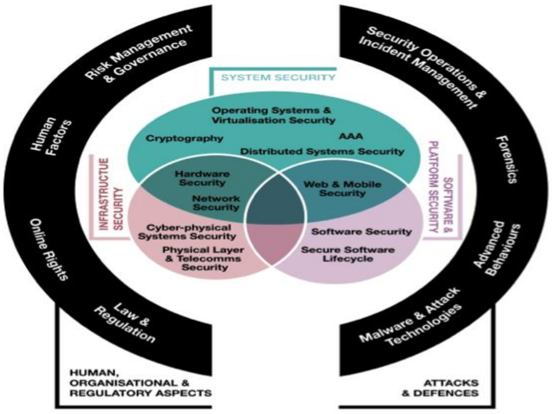

Risk Management & Governance
Human Factors
Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEM SECURITY
Operating Systems & Virtualisation Security
Cryptography
AAA
Distributed Systems Security
INFRASTRUCTUE SECURITY
Hardware Security
Network Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Advanced Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Figure 3-7 CyBOK Knowledge Areas

(Cybok.org, 2020).

3.5.4 Technical Models of Cyber Security

Some models of cybersecurity emphasise a system or technical focus. The Open Systems Interconnection Reference Model (OSI) by Libicki (2007) structures communication protocols for cyberspace into four layers of physical, syntactic, semantic and pragmatic each served by the layer below. A fifth cognitive layer was later added to take into account the networking needs of organisations (Lehto and Neittaanmäki, 2018). The Stenmap model introduced by Mases et al., (2018) classifies cybersecurity competencies based on four quadrants as shown in Figure 3-8.

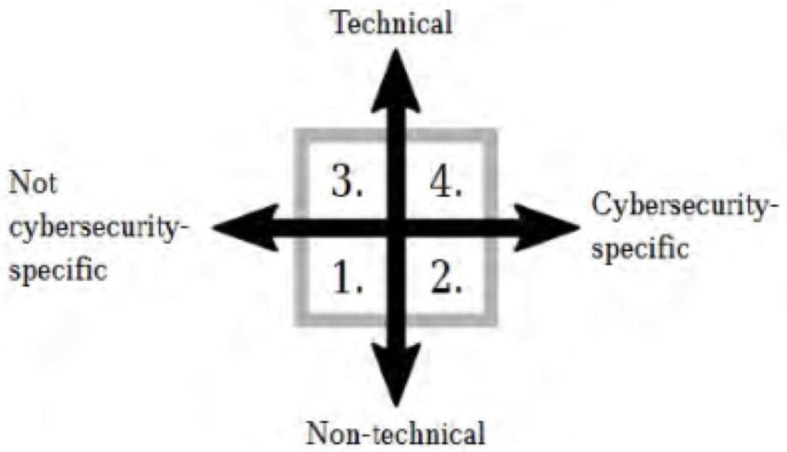


Figure 3-8 Classifying Cybersecurity Skills

(Frydenberg et al., 2020, p.34).

Each quadrant contains a different level of cybersecurity and technical skills ranging from non-cybersecurity specific and non-technical in quadrant 1 to cybersecurity specific and technical in quadrant 4.

3.6 Digital Competences for CPI protection

The fourth part of the literature review focuses attention on the role of recruiting, training, and development of qualified law enforcement agents and training (Hinduja, 2004; Merrick, 1997; Pickhard, 1995; Rana, 1999). This generates insights in regards to cyber policing competences linked to other skills, behaviours, and organisational commitment required for effective CPI protection (Dick and Metcalfe, 2001). Scholars have suggested that for developing competences it is imperative to identify both ‘technical’ as well as ‘behavioural’ needs of the organisation (May, 1999). In addition to the technical competences a CPI protection framework/model must take into consideration the role of committed law enforcement agents who “are less likely to be absent, and are more likely to be concerned with improving both individual and organisational performance” (Dick and Metcalfe, 2001, p.113). The technical digital competences for the protection of critical physical infrastructure could be equipped with domain experts, digital forensics, network investigators, and technical enquirers (Willits and Nowacki, 2016), while behaviourally could be equipped with highly motivated, committed, and loyal staff (Dick and Metcalfe, 2001). In so doing, academic debates on the roles of organisational, managerial, leadership, digital competences, and resources allocations and their relevance for CPI protection have been reviewed.

3.6.1 Organisational Digital Competences for CPI Protection

Training that targets organisations as a unit of analysis tend to ensure a reservoir of ‘knowledge’ and ‘skills’ necessary and collectively acquired by the organisation. Organisational theorists argue that cybercrime policing cannot be understood in isolation of organisational theory and structure (Willits and Nowacki, 2016). Such scholars found that “all organizational variables, including agency size, type, percentage of officers assigned to patrol, material technology use, and specialization are statistically significant predictors of the use of a cybercrime unit" (Willits and Nowacki, 2016, p. 118).

The acquisition of knowledge and skills could influence the collective knowledge necessary to confront adversaries with greater synergistic strength (Schwandt and Gorman, 2004; Bolden and Gosling, 2006). There are concerns however that police organisations established on the basis of similarity of organisational practices and digital knowledge competences could increasingly resemble one another by converging in one direction of '*cognitive lock-in*' (Asaba and Lieberman, 2008). Homogenisation and mimicry of digital competences within a police organisation could negatively affect adoption rate of police innovation and discourages novel action (Asaba and Lieberman, 2008; Tolbert and Zucker, 1983). Population ecologists argue that, when such practices solidify they have the tendency to inhibit and resist organisational and technological innovations and tend to be passed from one generation of law enforcement agents to another, leading to inter-generational cognitive lock-in or collective blindness (Staber, 1997).

To avoid the above tendency, police organisations that develop their organisational digital competences taking in to consideration '*multiple*' specialisations of digital competences are more likely to support each other during an unprecedented cyberattack on a critical infrastructure. This is particularly important as cyberattacks tend to take place often in uncharted territories requiring unscripted actions. In addition, when such organisational competences accumulate they are more likely to enable law enforcement agents to act efficiently with innovation during a cyberattack. Previous research on 'organisational memory' supports the above in regards to speedy vs. novel actions during improvisations. For example one study finds that while "the greater the procedural memory level, the greater the likelihood that improvisation will produce speedy and coherent action" on one hand, while "the greater the procedural memory level, the greater the likelihood that improvisation will produce speedy and coherent action" on the other (Walsh and Ungson, 1991, p.61). The former refers to "for how things are done" or memory for "things you can do" and the latter is "memory for facts, events, or propositions" (Walsh and Ungson, 1991, p.62).

3.6.2 Managerial Digital Competences for CPI Protection

Police forces have often attracted criticism for their inability to foster suitable management competencies to address the evolving nature of policing especially linked to the rise of cybercrime (Merrick, 1997). This is a vital issue as research has shown that the IT competence of a police manager is directly related to ability of implementing information security management (Change and Ho, 2006). Given the internationality of organised cybercrime and the jurisdictional challenge it possesses, it often requires more than dealing with the law enforcement agencies to encompass other actors (Hartfield, 2008). In so doing, coordination of organised crime policing requires managerial competences (Hartfield, 2008). Digital forensic investigation requires high degree of managerial competences including police managers' ability to manage a collaborative enquiry, facilitate effective decision, communication, and coordination (Bednar et al., 2008). Managers play a crucial role in moderating and managing relationships and expectations in regards to public-private partnerships leading to sharing of common security issues in addition to solutions and best practices (Dutta and McCrohan, 2002).

Collaboration is imperative thus Dutta and McCrohan (2002, p. 76) remark that, "managers' role is first to recognise that critical infrastructure protection is an essential component of corporate governance as well as organisational security, and one that is beyond their direct control. This statement applies to senior management in both the private and public sectors; hence they each have a vested interest in collaboration".

The role played by manager's organisational and cultural barriers often inhibits a smooth collaboration crucial for critical infrastructure protection (Dutta and McCrohan, 2002). Another vital role managers play is in regards to crisis management during a cyberattack on a critical infrastructure. When a critical infrastructure breaks down the need for law enforcement agents with crisis management abilities and resilience cannot be overestimated (Boin and McConnell, 2007).

At the immediate aftermath of a CPI breakdown the traditional top-down models of planning and prevention are often rendered ineffective, hence the need for law enforcement agents with competence capable of contingency planning, situational informational assessment, inducing public –private collaboration with owners, and ability to influence adaptive behaviour of citizens (Boin and McConnell, 2007). Hence scholars suggested that, for greater resilience, prior to attack on critical infrastructure, law enforcement agencies should engage in joint preparation, joint training, continuity planning, and working with communities and private owners (Boin and McConnell, 2007).

3.6.3 Leadership Digital Competences for CPI Protection

There is an imperative for policy and organisational leaders to expand their ability to foster organisational resilience during crises. A major element is preventing the emergence of traditional leadership pathologies linked to crisis events that can inhibit adaptive behaviours and stimulate blaming behaviours (Boin and McConnell, 2007).

Police leadership in key areas of digital competence is essential to the development of effective cybercrime solutions (Willits and Nowacki, 2016). This is because often at times when critical infrastructure is attacked the response could be chaotic and in need of a strong leadership for stable direction. "While organizational practices likely matter, there are reasons to expect police leadership and the availability of funding and especially federal grants to matter here as well" (Willits and Nowacki, 2016, p. 119). Leadership development strategies however are wide ranging as the definition of leadership itself. It is possible to identify leadership at multi-level of police individuals vs. teams.

Some scholars from the functional leadership school of thought (McGrath, 1962), suggests that leadership training program should be designed in such a way that it leads to the development of "cognitive activities leaders need to foster in order to promote team-goal achievement while teams are dealing with task-related problems" (Santos et al., 2015, p. 471). The preceding study compares 45 trained vs. 45 untrained leaders in various functions and the results showed that "compared to the non-trained leaders, the trained leaders registered an improvement in their enactment of leadership functions" (Santos et al., 2015, p. 470). At individual levels law enforcement agents are expected to equip themselves to succeed in the new environment of cyber threats (Densten, 2003; Willits and Nowacki, 2016). An emerging approach of leadership competences development, developmental leadership, attempts to establish links between individuals and teams within the police organisation and is increasing in popularity (Bass, 1985).

The above approach focuses on ensuring an enabling organisational environment with a tendency to stimulate the development orientation of followers to be successful cybercrime leaders in their chosen aspects of cyber policing (Willits and Nowacki, 2016; Bass, 1985). Developmental leadership emerged from transformational leadership with an emphasis on development orientation (Bass, 1985). Despite its significance it has rarely been given attention in the literature (Rafferty and Griffin, 2006). Because developmental leadership is not the only leadership competence with links to transformational effects, it has overlapped with other related constructs such as supportive leadership (Rafferty and Griffin, 2004). While supportive leadership focuses on providing supportive environment around employees to handle empathy, emotional well-being, and general social support on one hand, development leadership focuses on support infrastructure influencing the development of employees including mentoring, career counselling, attending courses, and recording followers progress on the other (Rafferty and Griffin, 2006). Supportive leadership is output driven aimed at supporting employees under stress and is linked to occupational stress research (Rafferty and Griffin, 2006). Developmental leadership is more process driven targeting specific individual developmental behaviours and ‘learning in process’ (Rafferty and Griffin, 2006). In many ways developmental leadership could be used as a reflective practitioner tool for developing continuous competences linked to mentoring and peer coaching (Parker et al., 2008; Barnett, 1995). Developmental leadership is found to be linked to self-efficacy, affective commitment, and career certainty (Rafferty and Griffin, 2006). Developmental leadership works best when applied to reflect a 360-degree view encompassing employee’s supervisors, colleagues, and subordinates (Boe and Holth, 2015).

Nonetheless, the application of developmental leadership as a tool for evaluating leadership digital competences is contentious. On one hand, developmental leadership questionnaire approach (DLQ – hereafter referred to as the standard approach), could reinforce the developmental trajectory of a leader through feedback (DeRue and Wellman, 2009). This is vital since empirical evidence suggests that without valuable feedback employees' developmental trajectory is subject to diminishing return (DeRue and Wellman, 2009). Feedback ensures that cognitive resources are 'not' diverted to other non-leadership activities (DeRue and Wellman, 2009). On the other hand, it is very difficult to conclude that leadership potential could be limited to a DLQ questionnaire scope given its many shortcomings (Turner, 2007). Law enforcement peers might have different motives for presenting themselves the way they did, or even worse when staff collude in inter-rater appraisals to favour their friends (Bolden and Gosling, 2006).

Error of judgement could also arise since the perceivers might be using different lenses to assess the same individual's competences (managerial, organisational, and behavioural), depending on their functional roles in the organisation (Bolden and Gosling, 2006). It can be argued that DLQ does not reflect an accurate representation of all digital leadership potential of a police force especially where for example an officer had commenced gradual withdrawal from organisational citizenship due to a certain discontent about the organisation as a whole (Nadiri and Tanova, 2010).

The advantage of developmental leadership is such that it could allow for the emergences of multiple leaders across the police force without having to rely on a mono-styled leadership competence 'cult' built around a particular '*charismatic leader*' (Groves, 2007). Most traditional police forces generally tend to have the tendency to establish leadership 'locked in' around a particular charismatic leader or leadership style (Fox and Granda, 2008; Drodge and Murphy, 2002). Scholars have argued that the leadership charisma style and the "friend" impression that this can give to employees is less effective for fostering high performance (Fields, 2008). With advances being made in regards to developmental leadership and the declining role of charism, it is possible for police organisations to develop leaders across several digital competences and it is more likely for cyber investigation to be carried out in a unified direction.

3.6.4 Resources Allocation for CPI Protection

Research points to insufficient availability of knowledge, skills and resources to identify, comprehend and address cybercrime risks and cyber security (Hunton, 2012). One of the key vital factors leading to successful protection of critical infrastructure is linked to resources investment in key strategic areas of cyber policing (Hunton, 2012). For example some intelligence information for a potential threat of attack on critical infrastructure could be revealed by social media police with a range of undercover policing tools (such as through enrolling users) to aid conjointly in criminal profiling. While this practice is valid to repel or minimise the tendencies of cybercrime perpetrated on critical infrastructure it is resource intensive (Li and Bernoff 2008; Shirky, 2008).

In view of the above, Hunton’s (2012) resource matrix identified key technical roles necessary for police departments to consider for effective cybercrime policing namely: network investigator, digital forensic examiner, forensic technician, technical enquirer, as well as technical domain expert. Long-term investment in aforementioned technical expertise areas could speed up cybercrime investigation and enforcement investigation (Fahsing et al., 2008). The nature of cybercrime is such that it mostly has no specific single crime scene making investigations more challenging as it transcends jurisdictions and legislations (Brenner, 2007). This is vital for crime investigators to overcome since a nation’s network security infrastructure and cloud computing could be subjected to frequent attacks by cyber criminals who are capable of hijacking, storing and distributing criminal data, in so doing increasing the volume of digital evidences needed for a comprehensive investigation, law enforcement scrutiny and hence resources (Choo, 2010). Law enforcement agencies that invest additional resources in key relevant technical knowledge and skills areas could likely recover quicker from an attack (Boin and McConnell, 2007, p. 55).

3.7 Conceptual Framework

A review of the literature reveals that a comprehensive framework for digital competency for law enforcement in the cybersecurity for CPI has yet to be established. Such a framework would contribute to knowledge on the key competences and implementation factors that enhance cyber security in law enforcement for CPI. The existing body of knowledge underlines a criteria for the development of digital competences of UAE law enforcement agents to protect critical physical infrastructure. The conceptual framework in Figure 3-9 proposes three dimensions that influence the development digital competency framework. Digital competencies are influenced by the organisational and external contexts.

The conceptual framework outlines the external and organisational contexts that influence the development and implementation of a digital competency framework for law enforcement. Externally the development of digital competencies is underlined by the legal and regulatory environment and is shaped and directed by the mandates for law enforcement that define the roles and functions. Legal reforms and law relate to seizure, acquisition and analysis (Battistoni et al., 2016; Hooper et al., 2013; Martini and Choo, 2012; Dykstra and Sherman, 2012; Garfinkel, 2010) and information sharing (Trottier and Lyon, 2011; Zedner, 2007; Yar, 2005). Cybercrime and cybersecurity threats represent an evolving context that has implications for the development of digital competencies for law enforcement to maintain pace with such developments. As cybercrime advances and in the face of technological and criminal innovation, policing must be fully prepared to tackle all potential threats. In so doing, it is vital to organise cybercrime policing in such a way that it leads to a higher level of crime control, reactive approaches, fear reduction, and community partnerships (Moore and Stephens, 1991).

At an organisational level the literature emphasises multiple factors that influence the development and implementation of digital competencies of law enforcement in cybersecurity. Development planning is influenced by a strategic approach and the wider culture which has implication for resourcing, enabling conditions, technological innovation, structures and layers of ownership. This framework extended this multi-level approach by grouping the levels/phases of attack to factors that could moderate the outcome of CPI policing and protection including organisational (structure, culture, memory); leadership (style); managerial (sense making, experience); as well as technical resources allocation (investment in digital competence training, technical resources).

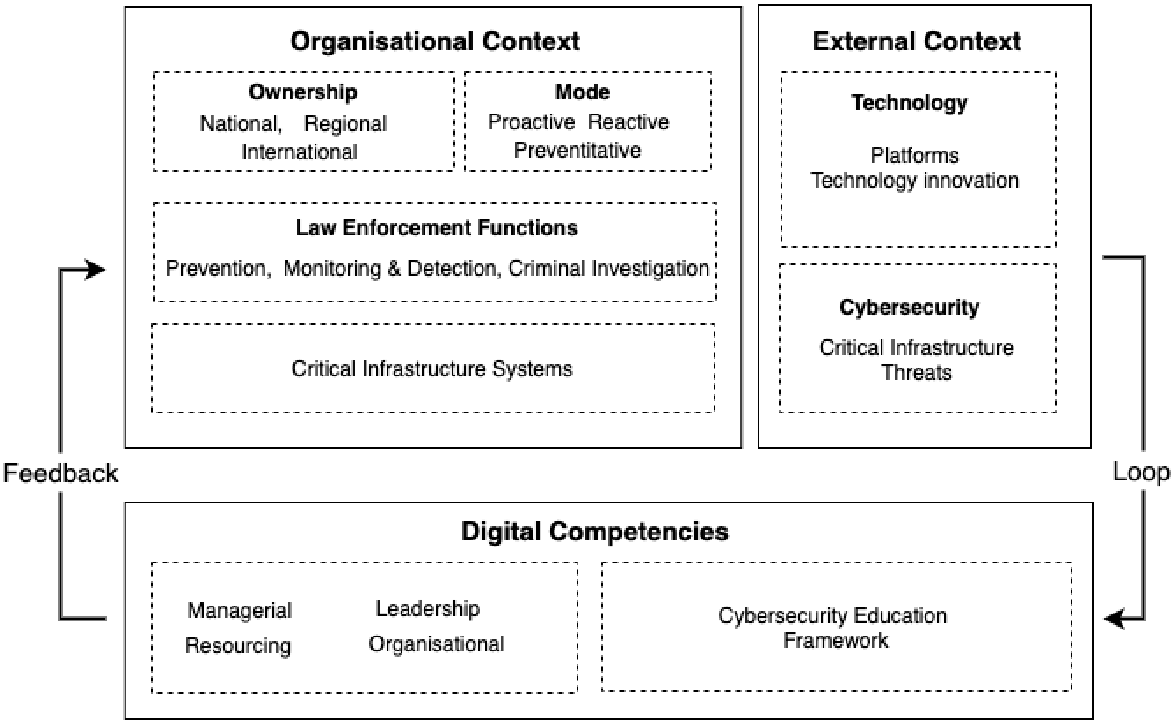


Figure 3-9 Conceptual Framework for Digital Competency Development for Law Enforcement to Protect Cybersecurity of CPI

These factors can influence the scope of digital competency development in law enforcement, for instance whether competencies are defined as specialised or generic. Specialist or single ownership and responsibility of the IT function and solutions strengthens only one cornerstone namely technology, at the detriment of other key cornerstones namely organisational and critical infrastructure (Dutta and McCrohan, 2002). Strategic development of training in key identified areas promotes critical mass of expertise. The framework aligns with the notion that "continuous training in the police system aimed at consolidating specialized knowledge of the policemen, expanding their general knowledge, as well as maintaining their skills and their specific work abilities at a high level" (Udrea, 2014, p.600).

Organisationally in terms of critical physical infrastructures, the nature and challenges faced by different CPI guides the development of digital competencies. Theory of CPI protection suggests a multi-level protection approach with links to levels of preparedness encompassing pre-attack, aftermath, and recovery (Boin and McConnell, 2007). These factors underpin human resource planning and training in key areas requiring critical mass of digital competence (Moore and Stephens, 1991). This approach to human resource planning and development in strategic areas also ensures that all areas required towards protection of critical infrastructure are considered. Without key strategic, distinct specialist structural units focusing and specialising in different cybercrime threats, cyber security initiatives and implementation to protect critical infrastructure would remain fragmented (Dutta and McCrohan, 2020). Additionally, investment in the development of key technical areas of digital competences has a higher probability of quicker recovery from a cyberattack on critical infrastructure. The above is supported by extant theory of resources allocation for speedy investigations across jurisdictions/legislations, cooperation and implementations (Fahsing et al., 2008; Brenner, 2007). CPI recovery is associated with resources allocation for training and in certain key technical expertise. This is vital given the distinct lack of available resources allocated to the development of skills, knowledge and training for digital competences of police forces (Hunton, 2012).

The literature underscores an evolving external and internal context of cybersecurity and the importance of recovery, learning and feedback. Critical infrastructure is a system that has the capacity to document the learning from previous failures, obstacles and challenges (Sommer et al., 2017) with implications for the type of competencies and resources to counter future threats and maintain pace (Sommer et al., 2017, p70). This component of the framework posits the digital competency framework as situated within an ecosystem (Broadhead, 2018; Kraemer-Mbula et al., 2013) that is continuously changing based on learning and feedback loops (Sommer et al., 2017). Most attacks on critical infrastructure are different from previous and therefore require improvisation and innovation to resolve but also capability of a system to quickly document the accumulated learning for a flexible preparation for future similar attacks (Harvey, 1999). The model situates digital competency within innovative culture that fosters receptivity to learning, and compatibility with other policing philosophies (Scheider et al., 2009). This is in line with theory of the learning organisation in which the law enforcement agencies in the UAE will be positioned to share ideas and knowledge leading to more organisational commitment (Atak and Ertugut, 2010). Learning police organisations invest in continuous training to encourage experimentation and new approaches of policing, systemic problem solving, learning from past experience and history, learning from best practices and outside experiences, and transfer and sharing of knowledge for organisational commitment, ‘emotional’ ‘normative’ and ‘continuous’ (Atak and Ertugut, 2010).

The digital competencies component represents the development of knowledge skills and abilities (KSAs) relative to the prevailing organisational and external contexts. Firstly, this framework posits digital competency beyond individual level capabilities to institutional level competencies that consider the digital policing policy framework; digital policing governance framework; digital policing regulations framework; digital policing collaborations framework. The framework places emphasis on strengthening management and leadership competences such as sense making and discursive through training and experience which provides a higher probability of high level coordination when protecting against a cyberattack on critical infrastructure. Development of crisis management has a higher probability of high level resilience in the aftermath of the breakdown of a critical infrastructure while digital developmental leadership competencies across several roles have a higher probability of protecting against cyberattacks on critical infrastructure with unified direction (Dutta and McCrohan, 2002). By placing management roles at the centre of responsibility this can help to ensure asset identification, risk monitoring and assessment of CPI, technical, control environment, and operational balance (Dutta and McCrohan, 2002). According to the theory of managerial sense making managers' competences in engaging subordinates through discursive practices improves communication (Rouleau and Balogun, 2011). By extension therefore the framework enables development of a deeper level of understanding in regards to "middle manager discursive competence; a middle manager's ability to knowledgeably craft and share a message that is meaningful, engaging, and compelling within his/her context of operation" (Rouleau and Balogun, 2011, p. 954).

In addition to managerial and governance dimensions of digital competency, the model emphasises a cyber security education framework as the basis for defining sector and role specific competencies. The cybersecurity education framework establishes an initial foundation that defines 7 cybersecurity functions, 33 speciality areas and associated work roles that are associated with a specific set of KSAs. The organisational context based on the key functions of law enforcement in the area of critical infrastructure protection influences the identification of KSAs. By applying the conceptual framework the organisational and external contexts provide the necessary parameters for determining digital competencies requirements for law enforcement for enhancing cybersecurity for CPI.

Finally, this framework incorporates a learning and feedback loop for developing digital competency that reflects the evolving nature of cyber security and changing competency requirements. An intelligent system of protecting critical infrastructure is a system that has the capacity to document the learning from previous failures, obstacles and challenges (Sommer et al., 2017).

This is vital as research has found that "learning activities in law enforcement are mainly directed toward daily police work and normal emergencies, and do not sufficiently prepare police officers and commanders to manage major novel crises such as the terrorist attacks" (Sommer et al., 2017, p. 70). The framework posits the police as an organised system within an ecosystem (Broadhead, 2018; Kraemer-Mbula et al., 2013) which must continue to learn (Sommer et al., 2017). A dynamic police system which focuses on learning in such a way can produce a variety of competences within the system (Martin and Sunley, 2007). Most attacks on critical infrastructure differ from previous attacks and therefore require improvisation and innovation to resolve, but also system capability to rapidly document learning for a flexible transition and preparation for future similar attacks (Harvey, 1999). Learning police organisations invest in continuous training to encourage experimentation and new approaches of policing, systemic problem solving, learning from past experience and history, learning from best practices and outside experiences, and transfer and sharing of knowledge (Atak and Ertugut, 2010). The development of law enforcement agents based on feedback loops and learning influences an innovative culture, receptivity to learning, and compatibility with other policing philosophies such as community policing (Scheider et al., 2009).

3.8 Conclusion

This chapter provided a review of the relevant literature for this study to establish the body of existing knowledge for the subject of interest. The previous chapter outlined the background context that is foundational to the direction of this research. The development of digital competency to enhance cyber security of law enforcement in critical infrastructure is shaped by the evolving nature of cybercrime, the national context and understanding of the role of law enforcement in cybercrime and in cyber security of critical physical infrastructures. A review of the literature in this chapter explored the concept of competency that contributed to a broad multifaceted understanding and identification of its constituents. Further, research into digital competencies shows it to be an evolving concept with wide multidisciplinary underpinnings underlying different perspectives and models of digital competency: technical, media, informational, social or cognitive. In the area of critical infrastructures the literature underlines different dimensions of competency: organisational; managerial; leadership; and resource allocation. In the area of cyber security different frameworks for development or education identify comprehensive requirements for digital competency but studies have yet to address a digital competency framework that is either specific to law enforcement or that addresses law enforcement cyber security for critical infrastructure protection. While accurate definitions exist of cyber security few clarify the skills required for individuals working within different areas of cyber security. Research into the range of technical and non-technical requirements for cyber security skills for organisations established a more detailed definition of cyber security skills as a combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills. Cyber security competences may need to be defined for specific organisational contexts either for law enforcement generally or specific to critical infrastructure contexts. The literature underlines organisational level and environmental considerations for the development of competency frameworks. Finally, drawing the conceptualisation of competency and digital competency a conceptual framework was developed that guides the focus of this research to exploring and validating digital competencies for cyber security that align with the role of law enforcement and critical infrastructure protection. In the next chapter this framework is integrated in a Delphi methodology and expert panel that identifies and validates key components of the digital competency framework.

Chapter 4 Methodology

4.1 Introduction

Methodology entails the “overall approach to the research process, from theoretical underpinning to the collection and analysis of data” (Collis and Hussey, 2003, p.55). Methodology enables a researcher to systematically organise and generate a body of knowledge (Saunders et al., 2007) as it comprises the plan and structure of investigation to address the research questions. The purpose of this chapter is to present and discuss the research methodology employed at all levels of the research process focused on the development of a digital competencies framework for law enforcement in the area of cyber security for critical infrastructure. This chapter provides a comprehensive description and rationale of each aspect of the research process in this study describing the methodological procedures adopted and the justification.

4.2 Research Process

To underpin the research process the research onion model, shown in Figure 4-1, has been applied (Saunders et al., 2007). This model provides a comprehensive overview of research as connected layers that are essential for the selection and design of an appropriate and rational research approach.

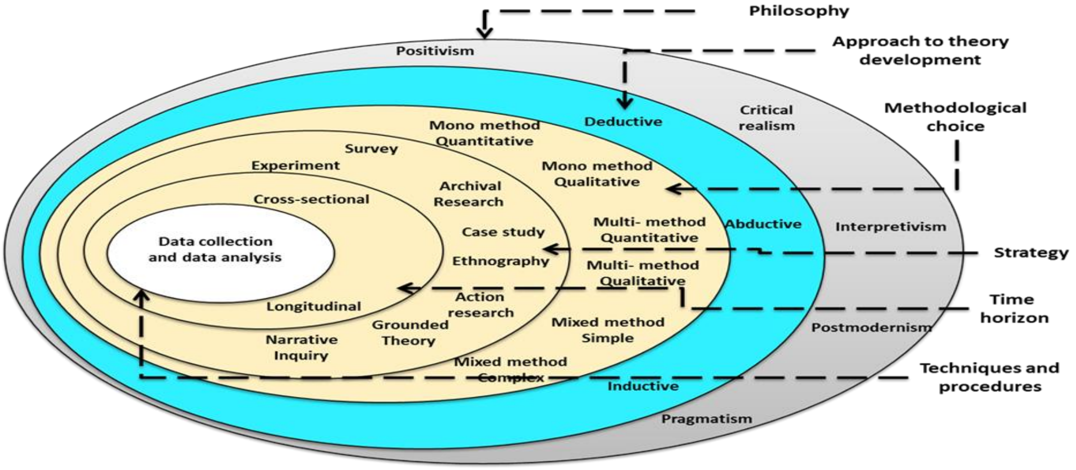


Figure 4-1 The Research Onion Model

(Saunders et al.,2016, p.15).

Based on the research onion for this study a research design has been developed that adopts a pragmatist research philosophy incorporating an inductive approach and mixed methods methodological choice as shown in **Error! Reference source not found.**. A case study research strategy is employed that combines both qualitative and quantitative methods in the course of cross-sectional research.

4.3 Research Philosophy

Research philosophy refers to beliefs about the way in which data on a phenomenon should be collected, analysed and used. It assumes a central position in guiding the design of the research and the methods and procedures chosen to fulfil the research goals and generate valid knowledge (Bryman and Bell, 2007). The choice of research approach frequently focuses on two fundamental philosophical choices of positivism and interpretivism (Burrell and Morgan, 2017).

Positivism advances a scientific and empirical approach based on the notion that observation and measurement are the basis of social science research. This reflects the assumption that reality is objective and stable and is external to human consciousness (Saunders et al., 2016). Under this perspective detached researchers can obtain 'objective' truth through the use of scientific methods of experimentation and testing of hypotheses. A key assumption of positivism is that only measurable phenomena are considered the proper subject of scientific research (Eriksson and Kovalainen, 2008). Associated primarily with theory-testing and quantitative approaches the key assumption is that science is essentially value-free and the major goal of research is to uncover patterns and relationships between variables (Eriksson and Kovalainen, 2008). Under this approach digital competencies are objective phenomena that can be simplified into key elements that can be isolated, measured and tested in an empirical way.

A key criticism of positivism is its lack of ability to capture subjective truths in unique social settings (Burrell and Morgan, 2017; De Laine, 2000). This is based on the argument that positivist approaches oversimplify complex situations and how far they can be reduced to their simplest elements (Creswell, 2009). Adopting a positivist approach may fail to produce the rich and in-depth data that can provide a more detailed explanation (Bryman and Bell, 2007). This has implication for a holistic understanding of digital competencies to inform a framework for law enforcement if the perspectives of social actors involved in this area are not explored and captured.

In contrast an interpretivist philosophy is rooted in the assumption that reality is comprised of the continuous actions and practices of human beings as social actors. Under this perspective people create their own meaning of a particular phenomenon resulting in the generation of multiple and equally valid realities (Bryman and Bell, 2007). That reality is obtainable only from the subjective interpretations of people within their particular context (Saunders et al., 2016). The researcher is instrumental as a subjective interpreter of that meaning and is embedded as an essential element of the research context (Collis and Hussey, 2013). Applying interpretivism to this study would generate rich and in-depth data that could allow for increased understanding of the underlying influences, motives and factors (Robson, 2002).

Saunders et al., (2007) argue that it is difficult for social science research to be neatly tailored into one single paradigm. In relation to digital competencies for critical infrastructure cyber security there is a rationale for providing a more comprehensive understanding of this research phenomena by adopting a pragmatist philosophical position that allows for the combination of both positivist and interpretivist approaches in a single study (Tashakkori and Teddlie, 2009). Exploring and drawing on the perspectives of participants in this context may provide a deeper and more holistic perspective of digital competency dimensions, however a sole dependence on an interpretivist approach would challenge the capacity to precisely and quantitatively establish the particular importance of different dimensions of digital competencies in relation to each other that can validate a digital competencies framework for UAE law enforcement.

4.3.1 Rationale for the Research Philosophy

For the purposes of this research a pragmatist position has been adopted. The rationale for this approach is underpinned by a number of reasons. Predominantly a pragmatic approach is selected because applying a single approach on its own would not provide the knowledge needed to fully address the research goals. Positivism would only allow for identification and quantification of key variables that would provide a simplified and incomplete picture of the digital competencies required by law enforcement for critical infrastructures and would not capture the underlying reasoning and justification. Interpretivism on the other hand is highly subjective and while providing rich data would not allow for precise understanding of the significance of specific competencies. Therefore by adopting a pragmatic approach this research is able to draw on the strengths of both paradigms to obtain a comprehensive view of digital competencies for law enforcement. Positivism enables understanding of what is important, while interpretivism is a major complement to positivist data as it promotes understanding of why and how. By drawing out rich and in-depth data it allows for understanding of dependencies, underlying complexities, barriers and the issues associated with them.

Furthermore the focus of research is a novel topic that has yet to be fully explored in the literature. Given the fragmented nature of CPI protection, there is as yet no consensus or convergence on critical elements and dimensions to influence the development of a national framework. There is a strong rationale for providing flexibility in approaches to allow research participants to contribute data and perspectives in different ways to generate a comprehensive picture of the research phenomenon. Experts involved in this research have the opportunity to express their views in a quantitative way while also providing qualitative data that can generate rich insights on the underlying reasons and factors. Furthermore adopting a pragmatic approach allows for a measure of triangulation that can minimise the biases inherent in either of these two philosophical approaches and reinforce the validity of the findings.

4.4 Research Approach

Research design can also be considered in terms of the extent to which deductive and inductive reasoning is applied. Deductive research aims to explore a known theory or concept and test if that theory is valid in given circumstances (Wilson, 2010). Inductive approaches in contrast aim to build theory based on the data collected

(Saunders et al., 2016). This study is primarily inductive in nature as the aim is to generate data to develop theory of and establish the key components of digital competencies for law enforcement for critical infrastructure protection. Key themes and dimensions are developed from the primary qualitative data collected from participants with the aim to advance theoretical understanding and develop an overarching model/framework on the nature of cybersecurity competences within the context of CPI (Corley and Gioia, 2011; Eisenhardt, 2007).

4.5 Research Methodological Choice

The methodological choice for this study is based on a mixed methods simple design combining qualitative and quantitative methods in a sequential manner (Saunders et a., 2007). For this study the research design represents a methodological choice that influences the balance between quantitative and qualitative methods. Multiple design options can be considered when undertaking mixed methods research including: convergent parallel mixed methods; explanatory sequential mixed methods; exploratory sequential mixed methods; and multiphase mixed methods (Creswell, 2009). For this study an exploratory sequential design is selected that begins with a qualitative research phase that explores the views and perspectives of participants to enable the generation of themes and identification of key dimensions in relation to digital competences for critical infrastructure cyber security. This aligns with the essentially exploratory nature of this study in an area where there is little established theory or understanding to draw on. Data is collected on what participants consider are the key factors and strategies for effective development of a national digital competences framework. This data is then analysed and the results incorporated into the second, quantitative phase. In this phase participants systematically prioritise and rank these dimensions assigning numerical rankings in order to understand their relative importance. The quantitative approach enables the quantification of perceptions in regard to the importance of different components of the framework being developed.

Literature shows that the mixed method approach is valid and widely used in circumstances where the research requires both types of data (Brewer and Hunter, 1989). The main advantage of mixed methodology is that it enables the researcher to gain a comprehensive view of the phenomenon from quantitative and qualitative lenses (Frevel, 2014). Furthermore this approach allows for a combination of data that potentially reinforces the strengths and minimises the weaknesses of any single data source (Platt, 2007; Yin, 2009). Therefore the outcomes of mixed method research may be of greater quality than those based on a single research method. Moreover the use of mixed methods could enhance quality through providing a measure of triangulation as the combination of different methods and data sources may help to gain a truer and more nuanced understanding of the research phenomena (Saunders et al., 2016).

4.6 Research Strategy

This research adopts a holistic case study design using multiple methods to generate qualitative and quantitative data. A case study is defined as *"an empirical enquiry that investigates contemporary phenomena within its real-life context especially when the boundaries between phenomenon and context are not clearly evident."* (Yin, 2003, p.13). The value of this strategy is associated with the flexibility to use a range of both quantitative and qualitative research methods to closely examine situations to achieve in-depth insights and descriptions that can result in the development of theory (Fearn-Banks, 2007). A case study approach allows for identification of the key competencies necessary for law enforcement while allowing exploration of the underlying reasoning. The Delphi method is employed as the primary data collection technique that is implemented over several phases of research. This method consists of a process employed to arrive at a group view or decision by surveying a panel of experts. These participants respond to multiple rounds of questionnaires and after each round the results are aggregated and shared with the panel. The Delphi design employs a number of methods to generate group opinion and decisions including: open-ended questionnaire; semi-structured questionnaire; an Analytical Hierarchy Process; and a focus group.

Using this approach can enable the development of a comprehensive and multidimensional understanding of the components, factors and dimensions that can inform a national digital competences framework. A case study can best address the research focus on a narrow or unique case of digital competences and training linked to CPI protection (Yin, 2009). Through systematic application of this design, the researcher can gain insights not only about the threats posed by newer technological advances, but also barriers and challenges to competent cyber security such as lack of education, awareness and training. The ability of case studies to allow for in-depth investigation can also support development of further insights on digital competences of law enforcement agents in the UAE including but not limited to aspects of investigation, cooperation and information sharing, legislative reforms, and other non-technical competences (organisational, managerial and leadership).

The specific context for this research is situated in UAE law enforcement in the area of cyber security for critical infrastructures. The decision for a single holistic case study design is appropriate in this context which focuses on one environment in which the UAE law enforcement agents and security stakeholders operate to ensure national critical infrastructure protection.

Application of this design enables the researcher to determine patterns that exists across all the seven Emirates (Abu-Dhabi, Ajman, Dubai, Fujairah, Ras Al-Khaimah, Sharjah, Umm Al Quainan) of the UAE police departments (Yin, 2009). Different interpretations of what makes an effective digital framework have led to identification of key influential factors informing the development of a national framework/model (Frevel, 2014). Comparing multiple views in the same operating environment of CPI security means that the research avoids isolated instances (Tashakkori and Teddlie, 2007; Eisenhardt, 2007; Saunders et al., 2007).

The context and premise for the holistic case study design in this research is drawn from the regulatory and operational environment which is unique to the UAE digital policing and CPI settings. The holistic nature of the agencies working closely with law enforcement agents enables the researcher to generate insights taking into consideration the UAE’s information as well as critical physical infrastructure strategies.

The sample for this case study focuses on police officers with designated roles or associations with The National Information Assurance Framework (NIAF) whose main goal is to ensure a minimum level of information assurance (IA); and Critical Information Infrastructure Protection Policy (CIIPP) whose main goal is to identify and develop the necessary application programmes to protect critical information infrastructure. In addition, police officers with links to the National Information Assurance Standards (IAS) whose main goal is information protection and management aspects (including business information continuity, disaster recovery, compliance, certification and accreditation) have contributed to the study. This provides opportunity to gather rich sources of information for developing an overarching national framework/model for CPI protection (Yin, 2009).

The overall research design for this study is summarised in **Error! Reference source not found.** that identifies the research philosophy, research approach, research strategy, sampling and analytical procedures, as well as limitations and ethical issues.

Table 4.1 Research Design Process

Methodological Process	**Appropriate Approach selected for this Research**
Research Philosophy	Pragmatist
Research Approach	Inductive
Research Strategy	Holistic Single Case Study Design
Time Horizon	Cross-sectional
Sampling	Probability & Non- probability
Data Analysis	Descriptive Analysis, Narrative Analysis, Thematic Content Analysis; Group Model Building Analysis
Limitations	Bias, Value Judgement due to the researcher being law enforcement agent
Ethical Issues	Informed Consent; Confidentiality

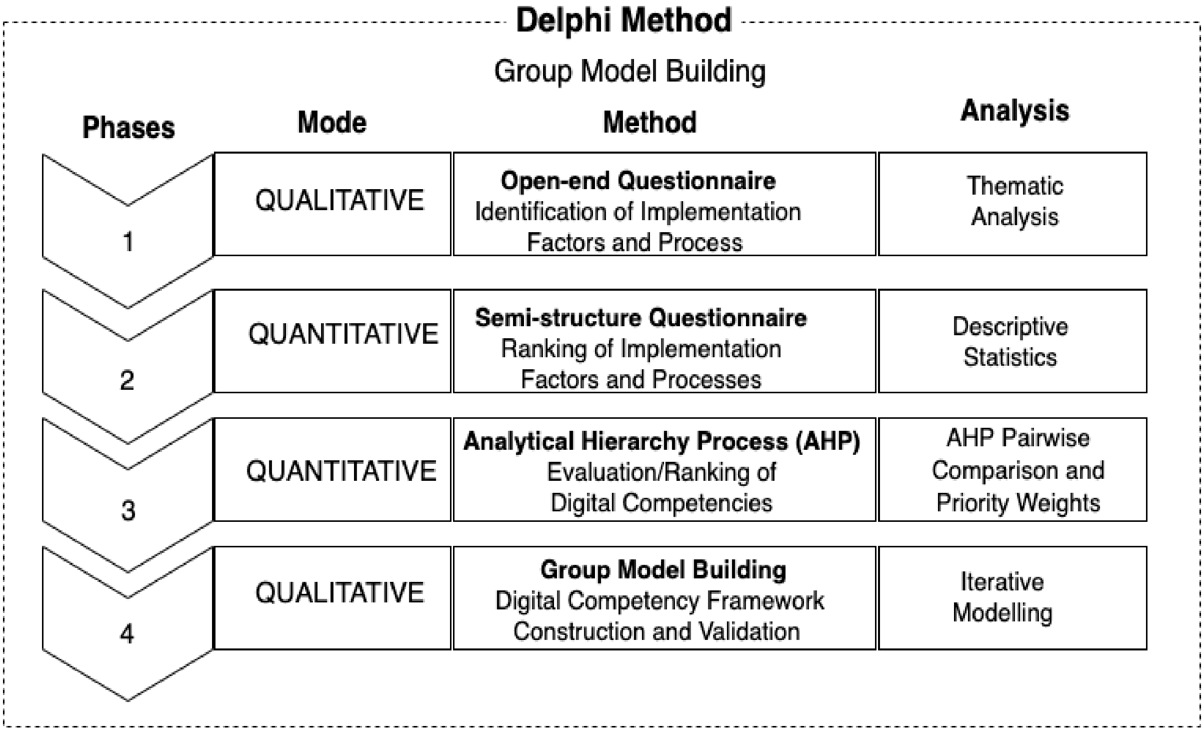
4.7 Research Methods

This research utilises a number of research methods for collecting qualitative and quantitative data. A Delphi panel is the primary method employed for collecting quantitative and qualitative data. Questionnaire methods, the Analytical Hierarchy Process (AHP) and focus group are incorporated into the Delphi to complete the research design. Figure 4-2 provides an overview of the research design and the relationship between these components.

4.7.1 Delphi Method

The Delphi method comprises a process applied over multiple stages aimed at achieving consensus of opinion among a group of experts or professionals on a particular real-world issue or problem (Hsu and Sandford, 2010). Identified as a process framework for problem-solving it is based on the outcomes of multiple rounds of questionnaires distributed to the expert panel. Their anonymous responses are aggregated after each round and shared with each panel member to afford experts the opportunity to modify their responses in later rounds in line with their interpretation of the group response (Linstone and Turoff, 2011). The Delphi method has been widely used in studies to identify, develop and validate solutions for critical infrastructure and cyber security related issues including protection, resilience, vulnerability, and interactions (Wells et al., 2016; Labaka et al., 2016; Turoff et al., 2014).

The aim of this research is to develop a framework/model of digital competences for the protection of critical physical infrastructure in the UAE. Delphi provides a systematic process of structuring group mutual communications towards developing a commonly agreed framework (Labaka et al., 2016). The systematic approach allows for multiple rounds of an iterative process of divergent as well as convergent participant views to resolve a complex problem (Linstone and Turoff, 2011; Skulmoski et al., 2007; Okoli and Pawlowski, 2004).



Delphi Method

Group Model Building

Phases	Mode	Method	Analysis
1	QUALITATIVE	**Open-end Questionnaire** Identification of Implementation Factors and Process	Thematic Analysis
2	QUANTITATIVE	**Semi-structure Questionnaire** Ranking of Implementation Factors and Processes	Descriptive Statistics
3	QUANTITATIVE	**Analytical Hierarchy Process (AHP)** Evaluation/Ranking of Digital Competencies	AHP Pairwise Comparison and Priority Weights
4	QUALITATIVE	**Group Model Building** Digital Competency Framework Construction and Validation	Iterative Modelling

Figure 4-2 Research Design Process

In the first round of Delphi an open-ended questionnaire was administered to the sample of UAE law enforcement agents engaged in the policing and protection of critical infrastructure. This sample are situated in a position as ‘gate keepers’ to share their knowledge and experience in regards to key factors and strategies considered to influence practices. As the goal at this stage is identification of key factors and strategies in line with research objective 1 an open-ended questionnaire was considered suitable. The outcome of the qualitative data from the Delphi round 1 lead to development of a table summarising all the key factors and strategies related to digital competences, training, skills, and Critical Infrastructure Protection (CIP).

In the second phase of Delphi a semi-structured questionnaire was implemented to allow for the ranking of factors and strategies identified in the first round while at the same time enabling the respondents to elaborate on cyber threats and skills gaps within the UAE police to establish the current state, aligning with research objective 2. The identification of cyber threats and skills gap added a dimension to areas of digital skills development training needed to be able to combat cyber threats and protect critical infrastructure.

In the third round of Delphi an AHP was implemented to identify the key digital competencies required by law enforcement to protect CPI based on the NICE framework (Petersen et al., 2020) which informed the composition of the matrix and pairwise comparisons for experts to evaluate. The inclusion of the AHP allowed for a quantitative component in which key components and dimensions of digital competences could be systematically evaluated and prioritised to reach a group decision on the importance of these dimensions in relation to each other.

In the final round of the Delphi a focus group involving a smaller number of experts from the Delphi panel (N=7) was used to enable group model building (GMB) to reach final consensus through workshop facilitation. This provided systematic decision-making support leading to the development of the digital competencies model/framework (Andersen and Richardson, 1997). The previous phases of Delphi identified and ranked the key competencies and factors and their degree of importance towards developing digital competences for CPI protection, leading to the development of a 'seed model'. Application of the GMB within the focus group aimed to engage a small group of experts to extend the seed model. First the GMB focuses on conceptualisation and formulation through brainstorming and designing of model structure (Andersen and Richardson, 1997). In so doing, the experts deliberated on key factors and strategies which can be utilised to close the digital competences 'skills gap' as well as the resources required within the UAE police.

In so doing, the researcher starts building a consensus table by eliminating certain factors with less attainment of consensus. While eliminating certain factors is a vital step, it is not sufficient in providing insights required for full consensus building. Thus, the researcher utilises the data to develop a 'seed model' of CIP taking into consideration current threats, skills gaps, and resources (Sekaran and Bougie, 2010).

The final workshop facilitated by the researcher aimed to ensure consensus is reached in regards to what extent the participants feel that the competencies, factors and strategies identified should be integrated to stages of national policy framework development namely: the policy formulations, the policy design, the sequencing, and the policy implementation.

The key policy frameworks considered here including the overall digital policing policy framework, digital policing governance framework, digital policing regulations framework, and digital policing collaborations framework. The results of Group Model Building exercises will lead to the development of a final integrated framework/model with policy options and feedback loop. This leads to the achievement of the final objective of this study to develop a framework to guide policy and the development of law enforcement in the UAE and enhance its capability to perform its role effectively in a digital environment.

4.7.2 Open-ended Questionnaire

In the first round of Delphi an open-ended questionnaire was employed to collect qualitative data on the digital competences experts perceived as essential for law enforcement to protect critical infrastructure. Open-ended or unstructured questions do not advance suggested answers but rather allow participants to respond in their own words (Saunders et al., 2016). In this study the use of open-ended questionnaires provided respondents the opportunity to generate responses that reflected their actual opinions and express what they considered to be important in regards to the key factors and strategies for effective development of a national digital competences framework (Saunders et al., 2007). The respondents have the flexibility to respond without constraints (Saunders et al., 2007) and to explore their own perspectives providing in-depth information about their perceptions, attitudes, and beliefs on the research topic (Bryman and Bell, 2007). This can result in a more authentic account that contributes to the reliability and validity of the findings (Saunders et al., 2016). The data collected was subject to thematic analysis to generate insights on emergent themes that would provide an initial broad understanding of the factors and strategies influencing the development of digital competencies required by law enforcement for ensuring critical infrastructure protection.

4.7.3 Semi-Structured Questionnaire

In the second round of Delphi a semi structured questionnaire was designed to collect both quantitative and qualitative data on the factors and strategies underpinning the implementation of training and development for digital competencies based on the data generated in the first round. A semi-structured questionnaire allows for the presentation of a predetermined set of questions that allows for a structured approach for the collection of data while providing the flexibility to explore more open-ended responses. For this study a semi-structured questionnaire employed both closed-ended and open-ended questions which afforded the opportunity for a quantitative judgement to be made on the characteristics of training and development for law enforcement while allowing respondents to further explain or reflect on their judgements (Saunders et al., 2016; Pallant, 2009). Including qualitative perspectives on assessments was important not only for generating a comprehensive and valid framework but also for obtaining the richness of detail to fully comprehend the underlying factors for training and development of digital competencies. While the quantitative data reveals the trends on one hand, the qualitative data provides in-depth critical insights that are hard to capture or measure including real life experiences and stories of the law enforcement agents protecting the critical infrastructure on a daily basis.

Quantitative questions were designed based on a response scale of 0 to 5 (0 being lowest and 5 being highest) to rank the degree of importance in regards to key factors and strategies (Saunders et al., 2007). The insights generated from this phase of the Delphi were refined and summarised to be used in the development of the framework.

4.7.4 Analytical Hierarchy Process

In the third round of Delphi the Analytical Hierarchical Process (AHP) was applied to prioritise and rank the key digital competencies required by law enforcement based on the NICE framework (Petersen et al., 2020) of digital competencies for cybersecurity. This enabled the application of an objective and systematic decision technique that supported development of the analytical framework for effective CPI protection in the UAE. The AHP is a comprehensive schema that provides decision-makers the ability to generate decisions on any number of alternatives based on multiple criteria and factors (Willyard and McClees, 1987). The approach aims to allow decision-makers to integrate both subjective, qualitative elements of complex problems into effective decision-making in addition to more objective and quantitative aspects. The AHP is applied across four key steps: the problem is first decomposed into a hierarchy as shown in Figure 4-3 that simplifies the problem and allows for systematic resolution; next evaluations of pairwise comparisons are conducted in which participants determine the importance or preference of elements within each hierarchy when paired against each other to establish the priorities among them; the results are then synthesised to obtain the overall ranking of alternatives to the goal; and finally the consistency of the judgements are evaluated (Saaty, 1978). The process has been employed to address a wide range of complex problems with various decision analyses, affording decision-makers the ability to identify and establish ratio scale weights or priorities while avoiding arbitrary assignment (Richey and Grinnell, 2004).

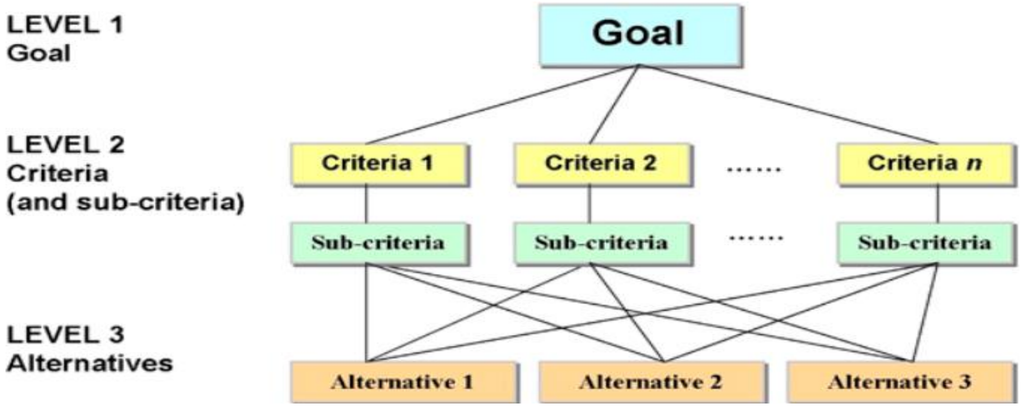


Figure 4-3 The Analytical Hierarchy Process

The rationale for employing the technique in this study is supported by multiple examples in literature where the AHP has been applied for the development of analytical frameworks across different domains: public services (Gompf et al., 2021); policing (Manning et al., 2013) and technology (Probert et al., 2003). Developed initially by Saaty (1978) the method is now one of the most widely applied tools to support multicriteria decision-making for decision-makers and researchers. AHP has formed the basis for extensive literature in a wide variety of domains (Gerdsri and Kocaoglu, 2007; Probert et al., 2003; Phaal et al., 2001). Highly relevant for this research context the AHP has been widely applied to strategic planning and modelling processes and the development of strategic frameworks (Sapkota, 2014; Gerdsri and Kocaoglu, 2007). The insights generated from this phase of the Delphi were refined and summarised to be used as a basis for the development of a ‘seed model’ to be utilised during the workshop facilitation for Group Model Building.

4.7.5 Focus Group

In the final phase of Delphi a focus group method was employed to review and refine the group evaluations from previous rounds and confirm the final framework. In this phase a smaller group of experts from the Delphi panel were contacted resulting in the participation of 7 experts, one from each Emirate. A focus group is a form of group interview that employs group communication and interaction to generate data on a clearly defined topic (Carson et al., 2001). Participants are encouraged to talk with each other, ask questions, exchange anecdotes and comment on each other’s perspectives and experiences (Kitzinger, 1995). The method allows for in-depth exploration of participants’ knowledge and experiences and is highly applicable for uncovering the underlying reasons for why they think what they do (Kitzinger, 1995). For this study the method is highly applicable for convening participants to act together to build and confirm the final framework.

4.7.5.1 Group Model Building

Within the focus group, Group Model Building (GMB) is integrated into the analysis to allow for the systematic development of consensus on the final framework. Group Model Building is a comprehensive method which allows for elicitation of knowledge from domain experts by enabling then to take part in model/framework building (Richardson and Andersen, 1995). It is an objective process which ensures the integration of a small group of expert views towards creating a framework that can provide a valuable outcome for improving digital competences for CIP. Essentially it provides a decision support mechanism for experts to agree on complex issues (Bryson, 2018; Bryson and Finn, 1995) such as CIP.

Engaging experts in the process of model/framework building helped to minimise bias and value judgement often prevalent in a framework or model generated by a single researcher. Data was collected by means of workshop facilitation with opportunity for discussions to reach consensus (Richardson and Andersen, 1995). The collaborative methodology enabled the researcher to elicit divergent and convergent knowledge residing in the minds of the expert group and later integrated into an aggregated model to inform the policies of digital competences and training for effective critical infrastructure protection in the UAE (Richardson and Andersen, 1995). For a successful GMB a schedule was developed for the day that comprised particular scripts, delivery techniques and tasks to be utilised (Andersen and Richardson, 1997).

4.8 Instrument Design

This study develops several research instruments that are employed across different rounds of the Delphi comprising questionnaires, an AHP form and focus group guide consisting of scripts to guide and manage the group model-building process. The design and structure of research instruments can influence response rates and the internal validity and reliability of the data collected (Saunders et al., 2007). In this study to maximise validity and reliability established design principles were applied that informed the design of the research instruments. Instruments drew on theory and concepts in the literature to develop the content and specific question items and where possible adapted or adopted previously employed and validated questions (Saunders et al., 2007). Questions were formulated to minimise ambiguity and ensure that they could be understood by the respondent in the way intended by the researcher (Foddy and Foddy, 1994, p.7). Consideration was also given to the presentation and structure of the instruments in terms of the order of content and a clear and attractive appearance. A pilot study was implemented that provided opportunity to modify the various research instruments in response to feedback on the instructions, the wording of question items and the structure of the instrument.

The first round of Delphi utilises an open-ended questionnaire comprised of nine sections that each contain at least two or three open questions. These questions collect data on the factors and strategies influencing development of digital competencies for CPI protection among law enforcement as well as significant factors or processes for protecting critical infrastructure. The first half of the questionnaire comprises different concepts and practices in the development of digital competences including: training plan; continuous professional development; training evaluation and monitoring; skills development and resources; and learning and feedback. The focus on training processes draws on numerous studies which have shown that the most urgent training needs for police relate to digital technologies (Cockcroft et al., 2018) which are frequently not a recognised part of police training (Cockcroft et al., 2018; Harkin et al., 2018; Hitchcock et al., 2017). Question 1 on digital competence training plan draws on literature that underlines different facets of a training plan including nature of specialisation (Willits and Nowacki, 2016; Hunton, 2012), degree of preparedness (Li et al., 2013; Radvanovsky and McDougal, 2010), nature of infrastructure (Marios-Panagiotis, 2016; Alneaimi et al., 2015), and technological innovation (Williams et al., 2018; Williams et al., 2013). Question 2 on digital competence continuous professional development is based on literature that highlights aspects such as frequency of training and recruitment of digitally competent law enforcement agents (Hinduja, 2004; Rana, 1999), and continuous testing and evaluations using exercises drills and simulations programmes (Radvanovsky and McDougal, 2010; Brown et al., 2006). Question 3 on digital training evaluation and monitoring is drawn from literature emphasising the importance of content, skills certifications and capacity building (Global Cybersecurity Index, 2018; Furnell et al., 2017). Question 4 on digital competency skills development and resources is based on research which underlines a lack of available resources for skills development in relation to identifying, understanding and responding to the growing threat of cybercrime and the implications of cybersecurity (Hunton, 2012). The question on learning and feedback is situated at the end of the questionnaire in Question 9 and draws on literature on the police ecosystem that emphasises learning from failures, receptivity to learning, and learning from best practices (Sommer et al., 2016; Atak and Ertugut, 2010; Scheider et al., 2009).

The second half of the questionnaire investigates concepts, factors and practices critical for protecting CPI consisting of: critical infrastructure protection phases of attack; critical infrastructure and cyber defence systems; critical infrastructure protection effectiveness; legislative reform and public engagement. Question 5 on phases of attack draws on Boin and McConnell (2007) who identify three separate phases of attack. Cyber defence systems in Question 6 is based on literature which underlines aspects such as partnership between law enforcement and other agencies (Homeland Security, 2018; Dutta and McCrohan, 2002) and with the public (Deibert and Rohozinski, 2010; Dutta and McCrohan, 2002) and cyber governance (Cavelty et al., 2016; Brown et al., 2006; Radvanovsky and McDougal, 2010). Question 7 on protection effectiveness relates to studies which point to dimensions of speed and novelty (Walsh and Ungson, 1991); coordination and resilience (Bednar et al., 2008; Dutta and McCrohan, 2002); shared vision (Boin and McConnell, 2007); and recovery and resources intensity (Hunton, 2012; Li and Bernoff, 2008; Shirky 2008). Question 8 on legislative reform draws on literature that underlines legal aspects in relation to interception and retention of data in real time (Cavelty et al., 2016; Hooper et al., 2013); sharing of cybercrime data for intelligence purposes regionally (Trottier and Lyon, 2011; Zedner, 2007; Yar, 2005); interception of cybercrime data stored on cloud platforms (Battistoni et al., 2016; Dykstra and Sherman, 2012; Garfinkel, 2010; Hooper et al., 2013); and lawful access and disclosure of digital data among law enforcement (Berkow, 2011).

In the second round of Delphi a semi-structured questionnaire is used as the research instrument. This integrates the competencies and factors and measures generated from the first round and thematically analysed. As in the first round the instrument contains nine sections and participants were invited to review and rate competencies and factors summarised from the thematic analysis using a six-part Likert scale to assign importance.

The quantitative instrument for the AHP in the third round of Delphi is based on the NICE framework (Petersen et al., 2020) that identifies the digital competencies required for cybersecurity. The framework identifies seven broad categories of competencies which are used in the AHP to determine priorities among them. The framework then identifies specialty competencies for each category included in the AHP instrument for experts to weight and prioritise. The final section of the AHP maps the work roles associated with each category based on the roles identified in the NICE framework.

In Delphi round 4 the research instrument comprises several scripts to manage and guide the group model building process. These scripts draw on group model building theory that identifies the importance of standardised protocols or “scripts” in group model building (Hovmand et al., 2011; Andersen and Richardson, 1997). Four scripts are employed in total that guide the process of conceptualisation of the model structure, eliciting feedback, testing and refining the model and integration within policy.

4.9 Sampling Strategy

For this study a non-probability approach is adopted using a purposeful sampling strategy to select expert participants for the Delphi panel. Widely utilised in qualitative research, purposeful sampling is employed to select participants based on specific criteria in order to target people with relevant in-depth knowledge of the research phenomena (Patton, 2002). The criteria for this study are based on six conditions that support the research objectives of this study: maximum amount of experience in terms of years; roles within cyber policing units; specific expertise (e.g forensic investigator, network administrator, threat monitoring); attended digital competences training; levels of seniority; links and association with CIP assignments.

The sample consisted of 24 experts drawn from all seven Emirates and specifically selected to ensure a diverse range of perspectives from different law enforcement organisations and from different roles and different levels of the organisation. The goal was to provide a holistic and inclusive account of digital competencies for critical infrastructure protection that could inform a comprehensive framework for law enforcement. Participants were drawn from a cross-section of policing agencies at federal and local levels that have key responsibilities for cybersecurity and critical infrastructure protection. The sample included police officers with designated roles or associations with The National Information Assurance Framework (NIAF) whose main goal is to ensure a minimum level of information assurance (IA); officers associated with the Critical Information Infrastructure Protection Policy (CIIPP) whose key objective is to identify and develop the necessary application programmes to protect critical information infrastructure; and police officers with links to the National Information Assurance Standards (IAS) whose primary purpose is information protection and management aspects including key processes such as business information continuity, disaster recovery, compliance, certification and accreditation. Officers were selected with varied knowledge in regards to digital competences, training and development, and from different hierarchical positions such as senior managers, middle managers, and frontline staff (Saunders et al., 2007). Officers were knowledgeable in areas of digital competences linked to CIP namely computer hacking, spreading malicious virus, spamming, network intrusion, software piracy, phishing, identity theft, and distribution of inappropriate images/contents.

4.10 Data Collection Process

4.10.1 Recruitment of Participants

The sample was drawn from HR personnel records of law enforcement agencies responsible for cyber security and critical infrastructure protection. Following organisational approval and with the cooperation of gatekeepers in these organisations the criteria for selection and details of the study were shared, resulting in the generation of a shortlist of personnel that met the criteria. Participants on the list were contacted and invited to participate in the Delphi panel in an email that also communicated the purpose of the study, how it was to be conducted and what participation would involve. Their rights as participants were outlined in a consent form attached to the email which participants could sign and return. Participants were additionally provided opportunities to obtain further information on the study and clarify any questions they may have had.

4.10.2 Delphi Round 1 – Open Ended Questionnaire

Round one of the Delphi process implemented an open-ended questionnaire that was emailed to all participants in the panel as shown in Appendix 2. The aim was to collect qualitative data and an in-depth perspective on the digital competencies and factors and strategies for law enforcement they viewed as significant for cyber security for critical infrastructure. Once completed, the unstructured responses from the questionnaires were subject to thematic analysis, with the outcomes forming the basis for an initial broad understanding of relevant competencies.

4.10.3 Delphi Round 2 – Semi Structured Questionnaire

In the second round of Delphi each participant was emailed a semi-structured questionnaire shown in Appendix 4 which integrated the competencies and factors and measures generated from the first round. This provided the opportunity to consider views and assessments and the integration of new ideas. Participants were invited to review and rate competencies and factors summarised from the thematic analysis using a six-part Likert scale to assign importance. The semi-structured format afforded opportunities for participants to offer a rationale for the rating and significance given to specific items (Jacobs, 1996). This phase created the basis for generating initial priorities among items and establishing early consensus on the priority of different competencies and factors (Ludwig, 1997).

4.10.4 Delphi Round 3 – AHP Matrix Questionnaire

In the third round of the Delphi process participants were asked to complete an Analytical Hierarchy Process form to identify the competencies evaluated as most important for the training and development of UAE law enforcement officers for effective cyber policing of CPI. The AHP was conducted online over two phases during which Delphi members were invited to complete AHP questionnaires. A form for structured responses as shown in Appendix 3 was provided to participants in which pairwise comparisons were assembled in an empty matrix to obtain priorities or weights for the items. Items were drawn from the NICE framework (Petersen et al., 2020) of digital competencies for cybersecurity.

Participants completed the form by comparing items against each other and allocating a numerical rating in accordance with their relative importance to the goal. For example participants could have to decide if Analyze competencies are more important, as important or less important than Collect and Operate competencies for the goal of CPI and assign a value to this comparative importance. Consistent with practice advocated by Saaty (1980), the design of the AHP incorporated a 9-point scale to evaluate pairwise comparisons as shown in **Error! Reference source not found.**.

Table 4.2 Rating Scale

Rating	Description	Explanation
1	Equal Importance	Two criteria contribute equally to the objective
3	Moderate Importance	Judgement slightly favouring one over another
5	Strong Importance	Judgement strongly favouring one over another
7	Very Strong Importance	A criterion is strongly favoured and its dominance is demonstrated in practice
9	Absolute Importance	Importance of one over another affirmed on the highest possible order
2,4,6,8	Intermediate Values	Used to represent compromise between the priorities outlined above

Therefore if a participant deems that Investigate competencies is considerably more important than Operate and Maintain competencies for law enforcement they will assign a rating of 9 and the latter will be rated as 1/9 in the matrix. A score of 9 indicates the significant importance of one component over another while a score of 7 points to an intermediate importance. A score of 1 reflects the equal importance of both components. Such pairwise comparisons were able to be depicted in matrix form.

4.10.5 Delphi Round 4 – Group Building

A group building method was employed in the final round of the Delphi to refine and revise participants' evaluations and confirm the final digital competencies framework based on the research findings. Due to COVID this could not take place face-face as planned and was restricted to online email, messaging and video-conferencing. This involved a total of seven Delphi panel members, one from each emirate, who are key domain experts within UAE law enforcement in terms of digital expertise of CI protection. The researcher acted as facilitator to guide the group discussion according to a predetermined set of topics (Saunders et al., 2016). A focus group guide was developed that incorporated questions, tasks and prompts for use by the facilitator that acted as a road map and memory aid. In group sessions the facilitator asked questions of the group and allowed time for participants to respond to each other’s comments. The focus group lasted for a day and responses were digitally audio recorded.

Group Model Building embeds tasks designed to engage the participants with a continuous stream of activity throughout the workshop, as shown in **Error! Reference source not found.**. These focused on engaging the experts to reach consensus through tasks that involved voting, box ticking exercises, and sketches of a simulated model structure (Andersen and Richardson, 1997). In so doing, the modeller employs a range of delivery approaches to facilitate brainstorming for ‘divergent’ related ideas, and then evaluation, integrative and design-oriented tasks for ‘convergence’ of ideas (Andersen and Richardson, 1997). For the brainstorming tasks a nominal group approach with plenary sessions was adopted, in which small groups of 2-3 are invited to discuss a list of ideas/concepts in regards to the ranked key competencies and influential factors. Through moving between subgroups to gather one idea from each individual participant, the researcher modeller reduces the number of key factors. This is achievable through voting for options to Agree, Partially Agree, or Disagree. Using video-conferencing software the focus group adhered more or less to the schedule outlined in **Error! Reference source not found.**.

The above provided the basis to expand the ‘seed model’ in activities requiring participants to simulate and design a model structure first in groups, and then collectively integrating central problems, solutions as well as policy options to the model/framework (Andersen and Richardson 1997, p. 111). The whole group were given opportunity for review to enable them to reflect, generate further dynamic insights, or simply clarify indistinct or overlapping ideas. Inspired by proposed model structures from the participants as well as the literature policy options scripts are presented to the participants in nominal groups for evaluation of feedback loops and potential model behaviour interaction. This is designed to enable the participants to discuss ways of informing national policy through implementation at various aspects and stages of UAE national policy frameworks in terms of digital policing, governance, regulation, and collaborations.

Table 4.3 Group Model Building Schedule

Group Model Building Workshop			
Time	Agenda	Team Tasks	
10:00-12:00	Introduction & Overview: Seed Model and influential factors	Brainstorm/Elicit Variable	Small Groups
			Plenary
		Voting options (Agree, Partially Agree, and Disagree)	Small Groups
			Plenary
Break (30 minutes)			
12:30 -1.30:	Simulate and Draw	Separate Model structures development	Individual Groups activity
		Integration of all model structures	Collective Group Activity
	Review, Test of Model Behaviour & Refinement	Structure – verification Test (Evaluation with check boxes)	Collective Group Activity
Break (30 minutes)			
2:00-3:00	Implementation: Feedback Loop & Policy Options	Loop 1: Digital policing	Plenary
		Loop 2: Digital Governance	Plenary
		Loop 3: Digital Regulations	Plenary
		Loop 4: Digital Collaborations	Plenary
Break (30 minutes)			
3:30- 4:30	Final integrated Model/framework with feedback loops	Integrating the model structures and Reflections	Road Map for Policy Implementation (Tactical, Strategic, Operational)-Collective

Overall multiple scripts have been used during the Group Model Building workshop namely 1) Scripts for conceptualising model structure; 2) Scripts for eliciting feedback structure; 3) Scripts for Model Refinement and Testing 4) Scripts for Policy Development (adapted from Andersen and Richardson, 1997).

4.10.5.1Scripts for Conceptualising Model Structure

Here the goal is to present a simplified 'seed model' and engage the experts to add successive layers of complexity. While doing so, the experts will be cautioned to use similar style and iconography of the original simplified version of the 'seed model' presented to them. This is to ensure uniformity and consistency of the final product.

4.10.5.2Scripts for eliciting feedback structure

Here the expert groups have been prompted to think about all the causal linkages and feedback loops in the model. Groups and plenary sessions have been used to encourage the expert participants to tell verbal stories about what controls key influential factors of CIP. Thereafter, the whole group collectively work together each beginning with variables/factors of interest in the (stock-flow) diagram and identifying causal influences to simulate and draw.

4.10.5.3Scripts for Model refinement testing

In this script a final model is presented to the expert groups in a paper sheet for a detailed model refinement process (Vennex, 1990). Once model refinement is completed the final refined model will then be tested through group tasks on structure verification using reference modes to the literature of CIP.

4.10.5.4Scripts for Policy Development

The final script use is the policy development script using matrices for ranking purposes. The script features a matrix which links policy levers to key system flows. The matrix system enables the experts to rank as well as tell policy stories where necessary. Prior to commencing the researcher introduces and discusses briefly policy levers in consideration namely digital policing policy, governance policy, regulations policy, and collaborative policy. Columns of the matrix will be labelled with key system flows within the white box diagram on one hand. The rows of the same matrix will be labelled with the key policy levers (Digital policing policy, governance policy, regulations policy, and collaborative policy). The matrix will be created both on the white board as on the worksheets handed to individuals. Their main task would be to decide if implementation of certain policies could lead to significant increase (++), small increase (+), significant decrease (--), small decrease (-), and no impact (0). Thereafter, the experts engaged in group discussions to present their findings. Where there is significant disagreement on the magnitude of an impact, the group discussions were intended to resolve such differences.

4.10.6 Pilot Study

A pilot study was undertaken which tested the different questionnaire instruments with the purpose of maximising the reliability and validity of the data collection process and results (Lancaster et al., 2004). Undertaking a pilot study supported the detection of potential problems and issues in the research protocols, procedures and instruments prior to implementation of the full study. It enabled the questionnaires to be refined and modified based on feedback from participants on the transparency of meaning of question items and the ease with which the questionnaire can be completed (Check and Schutt, 2012). The questionnaire designs for each stage of the Delphi process were tested among a small group of 5 police officer participants sampled from a single agency. The officers targeted are directly involved in the enforcement of virtual policing across the whole scope of activity. This enabled any issues with the structure and sequence, meaning and wording of the questions to be identified as well as understanding of the response categories and the average length of time needed for completion (Check and Schutt, 2012). Feedback was utilised to refine the instruments so that the final design consisted of a seamless and logical structure and clearly expressed questions that encouraged participant completion and valid and accurate responses (Check and Schutt, 2012).

4.11 Analytical Procedures

4.11.1 Thematic Analysis

Thematic analysis was utilised to analyse the qualitative data from the questionnaires applied in round one and two of the Delphi. This technique is widely adopted for identifying, analysing and presenting themes and patterns in the data (Braun and Clarke, 2006, p.79). Patterns are detected and assigned a code or theme and then iteratively rearranged into higher order categories. Thematic analysis provides a systematic and structured approach for analysing qualitative data that supports the validity and reliability of the results (Saunders et al., 2016). For this study it allowed large amounts of data to be addressed flexibly and efficiently while enabling the generation of a detailed account (Braun and Clarke, 2006) of the components and factors of digital competencies for critical infrastructure protection.

The qualitative data from round one and round two of the Delphi process was analysed to identify all of the digital competencies and factors that participants viewed as important. Analysis followed a structured approach incorporating a number of key steps as shown in Figure 4-4. Firstly, the data in the open-ended questionnaires were transcribed (Guest et al., 2014) and imported into Nvivo software that facilitated coding and analysis. The data sets were then read in-depth to generate initial ideas about items of interest following which the first round of coding was applied. Codes are words or short phrases assigned to sentences or small passages of text to convey core meaning (Ryan and Bernard, 2003). Different coding techniques can be used such as open coding, axial coding, or selective coding (Saunders et al., 2016). This research adopted open coding in order to capture the broadest possible range of underlying and contextual meaning of factors.

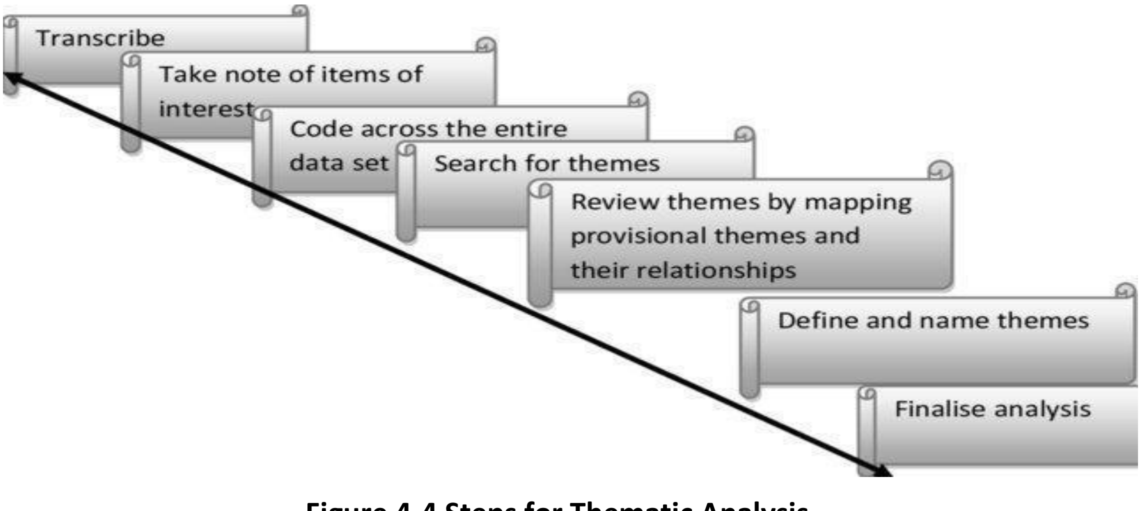

Transcribe
Take note of items of interest
Code across the entire data set
Search for themes
Review themes by mapping provisional themes and their relationships
Define and name themes
Finalise analysis

Figure 4-4 Steps for Thematic Analysis

(Braun and Clarke, 2006, p. 87).

The initial round of coding focused on a search for themes that were assigned a provisional code. This entailed identifying patterns in the whole dataset based on the themes emerging inductively from the data that are relevant to the research objective.

In a second round of coding themes were reviewed and refined and regrouped into higher order classifications (Ryan and Bernard, 2003). This process considered the relationship between themes and involved recombining and reconfiguring codes. In a final round of coding the definition and labelling of themes was finalised that identified the scope and focus of each theme (Braun and Clarke, 2006). The analysis of the results from the first round formed the basis for the investigation in the second round of Delphi. The qualitative data from this round was similarly analysed to determine the key themes in relation to the importance assigned to dimensions and factors of digital competencies. While thematic analysis is vital in generating insights, it has been criticised for relying on value judgements and assumptions of the respondents (Ryan and Bernard, 2003).

4.11.2 Narrative Analysis

Further, the researcher adopted narrative analysis to elicit the narrative as well as the stories UAE law enforcement tell in regards to the influential factors associated with cyber threats, skills gaps, and resources (Sekaran and Bougie, 2010). This provides the opportunity to integrate qualitative aspects to the seed model. In so doing, the researcher conducts a two level analysis namely at conceptual and relational levels. During the conceptual level analysis the researcher focuses on aspects critical to conceptualising the seed model through identifiable repetitive words, themes, and characterisations (Sekaran and Bougie, 2010). These have been coded accordingly to allow for a relational analysis and interpretation of coding categories (Sekaran and Bougie, 2010). The researcher conducted a cross examination of relationships and their meanings between concepts, texts, codes, and themes as basis for the development of the ‘seed model’ (Sekaran and Bougie, 2010). The outcome leads to a deeper level interpretation of what is being implied and invoked by the respondents and implications for CIP (Anderson and Warren, 2011). Narrative analysis allows for interpretation with emphasis on the ‘subject’ rather than the ‘object’ due to its explanatory power (Anderson and Warren, 2011).

4.11.3 Descriptive Analysis

The quantitative data from round two of the Delphi process was subjected to descriptive analysis (Pallant, 2005) to determine the scores for dimensions and factors of digital competencies. The ranked data were tabulated and presented in a descriptive analysis with details on mean, median scores, and frequency tables to determine the number of occurrences assigned to each ranked key factor. In so doing, the key factors that have the highest scores and number of occurrences will be given priority in the development of the ‘seed model’.

4.11.4 Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) employs mathematical techniques for analysing the quantitative subjective preferences of the decision-making group (De Felice and Petrillo, 2014). Analysis of the AHP results began by identifying the hierarchy of competence categories, specialty areas and work roles preceded by judgments on pairs of elements to attain a dominant element for each pair. This is expressed by obtaining ratio scales which can be utilised to identify the most preferential or most highly perceived alternative (Saaty, 1990). This process comprises three discrete analytical phases:

1) Pairwise comparison and evaluation of relative weights: Comparisons are undertaken between any number of pairs for every element at every level in terms of their importance or priority to the goal. According to Saaty (1980) comparison of any two elements can be achieved using a scale of 1-9 and can be depicted in matrix form
2) Priority vector: following completion of the pairwise comparisons the priority weight vector (w) is calculated
3) Estimation of consistency index: inconsistencies are likely to occur in the numeric values assigned by participants given that they are based on their subjective preferences and judgements. The threshold for the extent to which

inconsistencies can be accepted in AHP is determined by calculating a consistency ratio (CR). This is derived by comparison of the consistency index (CI) of the matrix under study with the consistency index of a random-like matrix (RI) for which inconsistency is expected to be high (Mu and Pereyra-Rojas, 2017). Recommendations in the literature suggest that a CR of 0.10 or less is satisfactory to proceed with the AHP analysis (De Felice et al., 2016; Saaty et al., 1990). In order to determine the CI of the matrix the calculation $CI = (\lambda max - n)/n - 1$., is used, where λmax is the largest eigenvalue of the judgment matrix A and n is the rank of the matrix.

4.12 Validity and Reliability

The validity and reliability of the research design and methods employed underpin the quality of the findings and conclusions in any study (Lincoln and Guba, 1985). Validity refers to the credibility or believability of the research in terms of whether the research measures what it purports to measure, while reliability alludes to the repeatability or consistency of the findings and if when repeated the study would yield similar results (Saunders et al., 2007).

This study is based on a mixed methods design that incorporates both qualitative and quantitative data. Qualitative research theorists have developed alternative concepts and measures to address reliability and validity in qualitative research. These identify notions of transferability, credibility, dependability and confirmability. Credibility centres on addressing the congruence of the research findings with reality (Merriam, 1998). For this study credibility has been supported through both method and data triangulation, in terms of employing a range of different qualitative and quantitative research methods and collecting data from varied data sources across different law enforcement agencies and different organisational levels. Transferability is broadly consistent with the idea of validity in positivist research, which is concerned with the application of the study findings to other situations and a wider population. To support transferability in-depth contextual information has been provided in the form of detailed background information on the law enforcement, critical infrastructure and digital competence context in the UAE. Dependability in qualitative research is closely related to credibility and concerns the consistency and repeatability of the study findings that contributes to its overall trustworthiness (Lincoln and Guba, 1985). Key measures have been adopted associated with the provision of a full explanation and rationalisation of the research design and implementation which enables readers to achieve a comprehensive understanding of the design and methods implemented and their effectiveness. This includes a complete explanation of the data collection procedures that enables the work to be repeated by other researchers. Confirmability concerns are analogous to objectivity considerations in quantitative research and comprise measures to ensure that the findings are reflective of the experiences and perspectives of participants and not the inclinations or characteristics of the researcher (Guba, 1981).

In addition specific measures have been undertaken in relation to ensuring the validity and reliability of the research methods adopted. In this study the Delphi method is the core method utilised that incorporates questionnaires, an analytical hierarchy process and focus group to collect data. The reliability and validity of the Delphi method was strengthened by applying several measures within the design. Firstly the selection of panel participants ensured that they were all experts in their field with lengthy experience and significant technical knowledge supporting the content validity of the Delphi outcomes (Lilja et al., 2011; Goodman, 1987). Moreover successive rounds of the Delphi enabled reasoned argument and assumptions and decisions to be challenged that helped to enhance validity (Hasson et al., 2012). Validity and reliability were further reinforced by maintaining anonymity among Delphi panellists until the final round. This helped to minimise judgement bias through preventing dominant or senior members from disproportionately affecting the results that can be a feature of face-to-face group methods (Akkermans et al., 2003; Dexter et al., 1993).

In the initial qualitative phase of the Delphi process the validity of the open-ended questionnaire was supported by its design which was founded on theory of digital competences and a systematic review of the literature to identify key themes and digital competence concepts. The design further strengthened reliability in ensuring that the questions were clear and unambiguous so that they would be interpreted in the same way by all participants, and the same questionnaire structure was applied to all (Saunders et al., 2007). Piloting of the questionnaires helped to enhance reliability as the feedback allowed modifications to be made to improve understandability and a collective interpretation (Bryman and Bell, 2007).

The design of the quantitative AHP phase was subject to specific criterion which reinforced the reliability and validity of the outcomes. The number of elements for pairwise comparison did not exceed nine in any of the AHP matrices which research shows influences consistency in judgements. More than nine elements and people have difficulty processing information which increases inconsistency (Ozdemir, 2005). In addition responses to the AHP were subject to statistical consistency tests specified in the literature (Saaty, 1980) and which support reliability by evaluating the extent to which the pairwise judgements are consistent with each other.

The validity and reliability of the focus group and the group model building stage was supported by several measures. Firstly the validity of the data was fostered through ensuring that minority or dissenting views were captured and included in deliberations and discussions. This helped to ensure that the effects of group polarisation were minimised and the convergence of group views were not unduly amplified (Turner, 1991). Further the researcher undertook training and practice in moderating group discussions which helped to ensure that discussions maintained relevancy in regard to the overall objective supporting validity and that one or more individuals did not dominate discussions (Kitzinger, 1995). Lastly questions and scripts were highly specific and precise helping to strengthen reliability and fostering accurate and detailed data that can be replicated (Smithson, 2000).

4.13 Research Ethics

The conduct of this study has been guided by consideration of the ethical issues and ethical principles of beneficence, autonomy, respect for privacy, justice, and confidentiality in every stage of research. The principle of beneficence refers to the obligation of researchers to act for the benefit of participants and prevent harm by ensuring that all measures of care are undertaken to safeguard participants (Belmont Report, 1979). This can include protection from physical harm or mental stress or loss of confidence (Diener and Crandall, 1978). In this study the risks of harm were minimised through assessing the design and implications of each stage of the research and implementing any necessary modifications. Potential discomfort from the questionnaire and AHP processes was mitigated by ensuring that processes were clearly explained and understood and participants were able to easily obtain further information and clarify any doubts. In accordance with the principle of justice which mandates that the risks and benefits associated with the research should be fairly distributed it is likely that participants and their organisations as well as the government of the UAE will benefit from this research as it can support increased knowledge and understanding of the digital competencies required to protect critical infrastructure. The knowledge arising from this research can be made accessible to all academics and practitioners both in the UAE and beyond.

Furthermore the research design was implemented to ensure that the rights of participants were safeguarded in respect of privacy and confidentiality and autonomy and informed consent. In terms of protection of privacy participants were made aware that they could refuse to respond to any question they perceived was too sensitive to answer (Bryman and Bell, 2007). Confidentiality was respected in the design of data collection so that the personal information of participants was not collected and all data remained confidential (Belmont Report, 1979). The data collected as part of this PhD study will be kept for 3 years after which it will be safely destroyed. To ensure maximum protection of data used in this research a number of measures were undertaken:

1) Fully anonymised all data by utilising codes, numerical identifiers, or pseudonyms so that individual participants could not be identified
2) Kept written record of data processing as well as a sound Data Management Plan (DMP).
3) Stored data in password protected computers and encrypted files to avoid unauthorised access. In particular, the researcher stored data only in the University’s research data storage facility.
4) Maintained a record retention schedule with clear outline on how long the data will be stored

5) Provided participants with full information on what will happen with the data collected

Safeguarding participants' autonomy is a major responsibility for researchers in terms of ensuring their rights to freely choose to participate in the study. Informed consent represents a critical procedure for ensuring that individual autonomy is respected (Belmont Report, 1979). To uphold informed consent participants were provided with full information on the study and its purposes, the benefits and risks and what their participation would entail to enable them to make a conscious informed decision on whether to participate. Information was provided in an understandable form and opportunity was given to solicit further information if needed (Belmont Report, 1979). Participants were also made aware that they could willingly withdraw from the study at any stage until completion.

4.14 Conclusion

The focus of this study is to investigate the digital competencies required by law enforcement to address the cybersecurity of critical infrastructure and develop a comprehensive framework that contributes to the training and development of digital competences of UAE law enforcement agencies. This chapter presented the research and methodological considerations that informed the research process to achieve the objectives of this study. The primary goal of this chapter was to establish a well-planned and methodical research design that upholds the credibility and validity of the findings of this study. This study was situated within a pragmatist philosophical paradigm that conferred importance on both positivist and interpretivist approaches. This has implications for a mixed method case study design that was systematically described in respect of the selection of research methods and all aspects of the data collection and analysis, and consideration of ethical issues. This chapter described a complete and systematic design that is most suitable for achieving the research goal and which enabled the development and verification of digital competencies for critical infrastructure protection.

Chapter 5 Results of Delphi Process

5.1 Introduction

This chapter presents the qualitative and quantitative results generated across the different phases of the Delphi process. This results are structured in accordance these four Delphi phases. In line with incremental group model building process, the expert panel were able review the collective data generated, revise their judgements to arrive at a consensus. Phase 1 provides the analysis of the expert panel's responses to the open-ended questionnaire, summarised in **Error! Reference source not found.**. The qualitative data from this phase was analysed and then reviewed by the panel who were able to revise their judgements and develop consensus on key themes. In Phase 2 a semi-structured questionnaire was developed based on the findings in Phase 1. The goal in this phase was to quantitatively rank the key factors identified in Phase 1 and generate qualitative data on those factors. The results from these two phases contributed knowledge on the key factors, issues relating to the design and implementation of digital competency framework for law enforcement for enhancing cybersecurity of CPI. Phase 3 of the Delphi process focuses on defining and prioritisation of cybersecurity digital competencies based on Cybersecurity Educational Framework. The results are presented for Analytical Hierarchy Process ranking the cybersecurity functions, skills, knowledge and activities relevant for law enforcement in respect of CPI. The final section of this chapter presents the results of group model building and validation of the model by the expert panel from Phase 4 Delphi process.

5.2 Delphi Phase 1 – Open-Ended Questionnaire

In the first phase of Delphi an open-ended questionnaire collected qualitative data on the factors and strategies that impacted the development of digital competencies and the protection of critical physical infrastructure. The data was thematically analysed from which eight key themes emerged of: 1) Balance, type, & relevance of training; 2) Futuristic training & unconventional techniques; 3) Mandatory certifications, digital knowledge and skills 4) Skills development and resources; 5) Proactive, reactive, preventative measures; 6) Socio-technical system (cloud, public, &

volunteer defenders); 7) Resilience, and 8) Adaptive learning. The first four relate to digital competence training and development while the latter four themes concern CPI protection.

5.2.1 Balance, Type and Relevance of Training

A key theme to emerge for digital competence development was balance, type and relevance of training for law enforcement experts in cybersecurity. Balancing the training of experts in internet security was noted by one participant to ensure there is enhanced diversity in acquiring and developing talent. Specific elements of digital development were identified to enhance balance in training and lead to effective development of digital competences: establishment of critical infrastructure protection digital expertise group/forum; categorisation and prioritisation of digital skills training needs; breadth and depth of training; sequence and order of training; parallel vs. vertical training; train the trainer routine; balancing private vs public company interests; trans-border digital competences training; benchmarking with global best practices; training for in-house talent development; 360 degrees training in all areas of digital policing; and number of updated digital training plans.

5.2.2 Futuristic training with the use of unconventional techniques

The analysis pointed to futuristic training with the use of unconventional techniques as a key theme for digital competence development. Establishing proactive mechanisms to address cybercrime was cited to positively change the way in which an organisation engages in cybersecurity.

Several strategies were identified as critical for effective development of digital competences to promote access to learning on innovations, technologies and practices including: accessible digital micro training and e-learning; Learning Management System (LMS); mobile learning; use of simulation exercises; gamification; industry 4.0 applications (IoT, Smart tech); incorporation virtual reality (VR), augmented reality (AR), artificial intelligence (AI) and robotics.

Table 5.1 Thematic Analysis Summary

Dimension		Key Factors
Digital Competence Training Plan	BALANCE, TYPE, & RELEVANCE OF TRAINING	● CIP digital expertise group/forum established ● Categorizations and prioritization of digital skills training needs ● Breadth and depth of training ● Sequence and order of training ● Parallel vs. vertical training ● Train the trainer routine ● Private vs. public interests ● Trans-border competences training ● Benchmarking with global best practices ● Training for in-house talent ● 360 degrees training ● Number of updated plans
Digital Competences Continues Professional Development & Training	FUTURISTIC TRAINING USING UNCONVENTIONAL METHODS	● Accessible digital micro training and e-learning ● Learning Management System (LMS) platforms ● Mobile learning ● Simulation exercise ● Gamification ● Industry 4.0 technologies application (IoT, Smart tech) ● Applying VR, AR, AI and Robotics
Digital Training Evaluation & Monitoring	MANDATORY SPECIALISATIONS &	● Guidelines for evaluation ● Capabilities) ● Specializations and Certifications

	CERTIFICATIONS	● Network security Certifications ● Digital forensic certifications ● Information security certifications ● Ethical hacking techniques certifications ● Information security certifications ● Information system security certifications
Digital Competency Skills Development & Resources	DIGITAL KNOWLEDGE & SKILLS	● Modeling and testing of threat intelligence ● Specializations in domain expertise ● Balance of knowledge vs. skills established ● Detecting,, investigating, and combining cyber-crime evidences ● Skills for social media policing (covert and overt) ● Generalist vs. specialist skills routes ● Intangible resources
Critical Infrastructure & Cyber Defence Systems Resources	SOCIO-TECHNICAL SYSTEM (CLOUD, PUBLIC, VOLUNTEERS)	● Strengthened cloud network infrastructure & forensic systems ● Establish National crime mapping for cyber-attack on CI system ● Systems of Partnership between ● Develop volunteer cyber defense system ● System of lateral surveillance on social media using pseudonyms ● Maintenance of time alteration forensic evaluations mechanisms ● Maintenance of Public Private Partnership arrangements systems ● Maintenance of periodic inspections of cloud infrastructure
Critical Infrastructure Protection Phases of Attack	PROACTIVE, REACTIVE, & PREVENTATIVE MEASURES	● Joint preparation and training ● Working with communities ● Undercover social media policing ● Contingency planning

		● Situational information assessment ● Cybercriminal profiling ● Volume of evidence ● Preventative measures for inter-jurisdictional investigation
CIP Effectiveness	RESILIENCE	● Readiness & Preparedness ● Speed to seizure, acquisition, analysis, and investigation ● Novelty in responding to CPI attack ● Resources intensity for investigations and recovery purposes ● Risk assessments, monitoring and evaluation ● Increased legislative powers to access, intercept and store data ● Increased cooperation for sharing intelligence
Learning & Feedback: Loop	ADAPTIVE LEARNING	● Learning from international best practices ● Receptivity and openness to learning new technology ● Peer to Peer Learning ● Learning from failure

5.2.3 Mandatory specialisms and certifications for law enforcement

Mandatory specialisms and certifications for law enforcement are identified as a critical component of cyber security management for critical physical infrastructure. Several participants noted the importance of knowledge of international standards governing the certification of digital content for cybersecurity competence development. In addition participants noted that all digital specialisations should be certified. Specific areas of digital specialisations and certifications were distinguished as central for developing digital competences for law enforcement: network security certification; digital forensic certification; information security certification; ethical hacking techniques certification; information security certification; and information system security certification.

5.2.4 Skills development and resources

The Delphi panellists identified a number of factors in relation to digital competency skills development and resources relevant for effective critical infrastructure protection. Key themes included: developing skills for modelling and testing of threat intelligence; developing expertise in all domains such as digital forensics, network investigation, and technical inquiry; achieving balance of knowledge vs. skills established; developing skills for detecting, investigating, and analysing cyber-crime evidence; developing skills for social media policing (covert and overt); and achieving a balance between generalist vs specialist skills routes.

5.2.5 Reactive, proactive, and preventative measures against cyber-attack on CPI

Key factors and strategies were also identified in relation to protection of critical physical infrastructures against cyberattack in terms of the reactive, proactive and preventative measures that could be implemented. Seven key factors emerged in the analysis: joint preparation and training; working closely with communities; covert social media policing; contingency planning; situational information assessment; cybercriminal profiling; volume of evidence; preventative measures; provision of resources for inter-jurisdictional investigation.

In terms of joint preparation and training participants identified that the scale and rapid development of cyberthreats emphasised a need for training mechanisms which are more flexible, adaptive, operational, and strategic. Advanced training technologies were noted to be necessary for effective development of digital competences. Working closely with communities was noted by participants to relate to all levels of employee and different functional specialisms and areas to develop understanding of how to judge and detect a threat before it actually occurs. One participant mentioned the establishment of a secure development lifecycle (SDL) that is meant to create cohesion between the members of the organisation to ensure the security policy is accepted by everyone in the community. The inclusion of SDL would enhance aspects such as threat modelling, security up front testing, and security significance. Measures to enhance cybersecurity further included the implementation of undercover policing on social media. This was associated with the use of these platforms globally to conduct cybercrime.

Policing on social media using undercover pseudonyms was identified as a key mechanism forming a system of lateral surveillance on social media**.** Security agents were noted to frequently use fake accounts to launch investigation against a suspected hacker or a perpetrator of other cyber-related crimes. The need for cyber security contingency planning was linked to protection of information technology equipment, services and data against natural disaster or security breaches. This was identified as a written risk management document which provides instructions, recommendations and considerations for a company on how to recover their IT services and data should a breach occur. Participants noted the importance for developing a contingency plan of identifying vital information systems and data, possible types of risks and threats and controls to be put in place to mitigate these threats.

Situational information assessment of the cyber security threat is another mechanism considered vital when conducted correctly and in a timely fashion. Understanding the nature of threats likely to face the organisation through critical assessment and analysis was noted to allow all stakeholders to gain awareness of the situation and likely impacts of the threats. Experts suggested that many organisations employ STIX ontology to act as a symbol or visualisation for interpreting cybercrime information and to signify the most significant qualities embedded in the cyber situation. Information was considered to be an essential element that helps critical decision makers to arrive at situation awareness and the most concise and effective decisions.

Cybercriminal profiling was believed to contribute to the effectiveness of a cyber-security strategy and according to experts was a highly preferable mechanism which helps to identify perpetrators associated to the crime and profiles them against their actions. Cybercrime profiling was noted to help to classify and differentiate between petty criminals and cartels of professional information hackers.

Some participants drew attention to the volume of critical information available on electronic devices that can become evidence in criminal cases. While digital evidence was mostly used to address electronic crimes, nowadays it is used in all types of crimes. Participants suggested several measures to ameliorate risks of evidence tampering, considered easy with digital evidence and therefore requiring special care to secure and preserve it. Records should be kept and devices given specific numbers and the evidences should be left in the state they were found. This would allow for the acquired data to be intact upon its use in the court.

Preventive measures included social technical aspects based on a belief that due to the complexity of CPI systems measures should not be limited to technical factors only but also encompass social aspects. In so doing participants identified the following factors considered as critical for effective CPI defences systems. Firstly a strengthened cloud network infrastructure and forensic systems were considered critical to strong security in an ICT organisation. The ability of an organisation to withstand an attack was viewed to primarily depend on the strength of its cloud network infrastructure. Therefore, it is important for an organisation to install up to date facilities. Further forensic systems must also be effective and facilitate the gathering of relevant digital evidences. The majority of the respondents admitted that the use of Mobile Cloud Computing provides universal access to the relevant data that can help in assessing the situation and gathering relevant evidence for investigations. Establishing national crime mapping for cyber-attacks was viewed as a further effective preventative measure. Some participants underlined the importance of systems of partnership and information sharing between law enforcement agents, intelligence community, and national coordination centres as a key preventative measure. This was viewed to create a culture for security between law enforcement, and other stakeholders such as the intelligence community and the national coordination centres and effective coordination of investigations. Participants further emphasised that effective coordination between the security agents and the public would help to curb cyberattacks. Another preventative measure was the adoption or adaptation of voluntary frameworks by organisations to assess the nature and intensity of cyberattacks experienced in different areas of operation. Participants cited the NIST framework as one such which could be adapted to UAE boundaries and comprises five elements of Identify, Protect, Detect, Respond, and Recover.

Prevention measures were further associated with maintenance of time alteration forensic evaluation mechanisms in the cloud and maintenance of periodic inspections of cloud infrastructure. Most organisations were perceived to use cloud computing infrastructures for back-up provisions, and therefore it was considered crucial to conduct frequent maintenance and services to ensure UPS connections to the cloud were in a good condition and UPS monitoring software could be deployed to further enhance alarm reporting, fault finding and overall speed of response. According to the respondents, maintaining and periodic inspection of the cloud infrastructure would help in information retrieval during forensics by the investigators.

5.2.6 Resilience for CPI protection

Participants identified resilience as vital for CPI protection and suggested the following critical factors: readiness and preparedness; speed to evidence volume, acquisition, analysis, and investigation; novelty in responding to CI attack; resources intensity for investigations and recovery purposes; and risk assessments, monitoring and evaluation.

Cyber readiness and preparedness were considered essential involving the process of continuously applying security measures and ensuring that all threats both internally and externally are addressed before an attack occurs. This would ensure a quick response to any form of breach as each and every activity conducted within the networks are monitored hence the problem is easily identified. Readiness and preparedness would help in avoiding large losses or outages.

Participants identified that forensic investigators must follow specific procedures and regulations to ensure that data is not tampered with or mishandled during the process of acquisition, sorting, transfer, and storage and speed of evidence gathering is maintained. During the forensic acquisition stage, evidence is gathered from all the electronic device sources, and mostly involves use of the copy and paste commands to ensure originality of the evidence. It may further involve retrieval of image evidences by physical photo taking and also from storage devices such as hard drives, smartphones, removable disks, CD ROM, and live servers among other devices.

In terms of novelty in responding to CI attack respondents believed that security agents should be actively involved in cybercrime solution seeking. The first response to CI attack is taking inventory of the technological infrastructure available with the company. The inventory taking may involve such activities as frequent system tracking and inspection to ensure security of data. Secondly, the organisation can appoint a team responsible for implementing emergency plans in case there is an attack. The team's responsibility is to contain the situation by offering technical assistance internally before the eventual launching of investigation. Lastly, the company can respond by making contingency plans to secure the situation. This can happen through an emergency address to all the staff members to know the company is under an attack and the situation is being contained.

Resource intensity for investigation and recovery purposes was identified as an essential aspect of cyber security. Certified and highly trained response teams should be ready to apply the necessary response procedures and decisions regarding the situation. The team should collect and analyse all evidence related to the attack. They should ensure that a remediation plan is implemented to ensure that critical mitigation tactics are addressed, and business disruptions are minimal. The most vital and confidential assets should be protected to avoid further loss, and the attack contained to prevent it from spreading a causing additional damage. An investigation report should also be undertaken to ensure that lessons are learnt.

Risk assessment, monitoring, and evaluation of cyber-security were considered essential in determining the effectiveness of controls put in place to understand and control cyber-attacks. Risk assessment was believed to help develop proper risk response. Evaluation and monitoring of cybersecurity could be conducted by establishing and regularly reviewing security metrics, conducting vulnerability assessment and penetration tests to validate security configuration, and completing an internal audit to assess security control operations. Performing risk assessment monitoring and evaluation was identified to reduce long-term costs, avoid data breaches and regulatory issues, and data loss. Respondents further identified the need for legislative reforms to enable law enforcement to have increased powers to access, intercept, and store data efficiently. Specific legislative powers were considered to be critical: increased powers to block cybercrime data stored on cloud platforms (IaaS, SaaS, and PaaS); increased cooperation for sharing regional intelligence on cybercrime; maintenance of up to date information systems for interception and retention of real-time data; and societal engagement and awareness.

5.2.7 Adaptive learning

Finally, the respondents determined that adaptive learning is crucial for the overall policy framework of the UAE and that certain learning should be given priority and even integrated within digital policy frameworks. Participants considered learning from international best practices was key and organisations worldwide can benchmark from other international organisations. Learning from best practices was identified to involve acquiring skills and techniques from different organisations and programmes. Receptivity and openness to learning new technology was further noted as important for positively impacting cyber security in organisations. Another strategy identified was peer to peer learning. Implementation of P2P learning programmes in the organisation was believed to reduce the cost associated with replacing infrastructure in an attack. Finally participants identified learning from failures within the organisation and externally as an important adaptive learning strategy to address cybercrime.

Learning from past experience could help security agents to adapt such strategies as: establishing and maintaining strong crisis management systems and programs, proactively training employees to handle threatening situations, utilising strong encryption and passwords, and frequent system authentication. All the themes in relation to developing digital competencies for law enforcement protection of critical physical infrastructure are summarised in **Error! Reference source not found.**.

5.3 Delphi Phase 2– Semi-structured questionnaire

In phase 2 of the delphi process experts provided quantitative responses to rank and prioritise the key factors and strategies identified in phase 1 as significant for digital competencies of cybersecurity for the protection of critical physical infrastructure. A 6 point likert scale was employed to rank factors from 0 for least important to 5 for most important.

Figure 5-1 shows the results for rating of key factors for balance, type and relevance of digital competency development. Categorisation and prioritisation of training needs and comprehensive 360-degree training were the top two highest rated by the expert panel as the key factor. The bread and depth of digital competency training and digital expertise forum for CIP were the next highest factors. Experts also prioritise the regular updating of digital training plans, trans-border and in-house development as key factors.

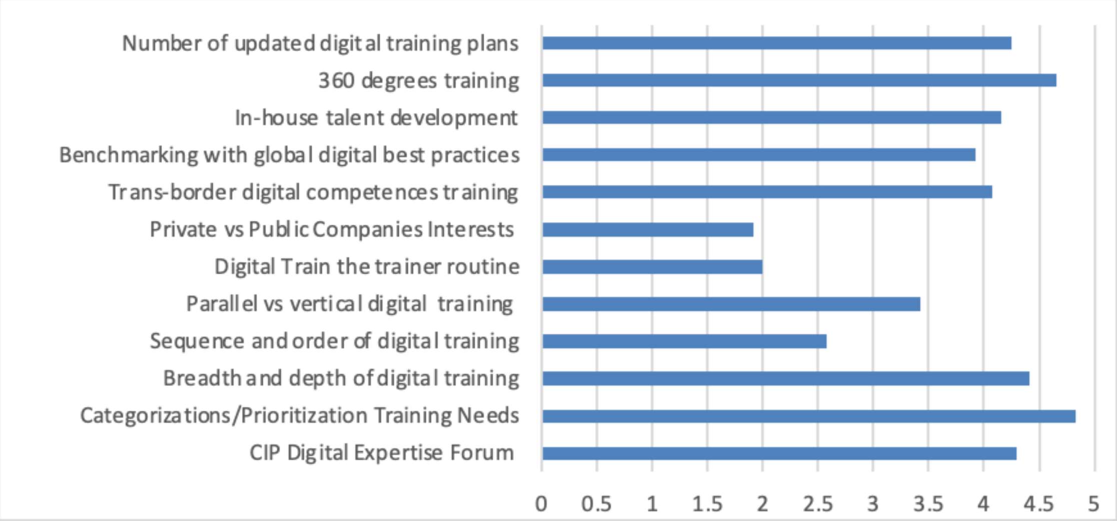


Figure 5-1 Key Factors for Balance, Type, Relevance

Figure 5-2 shows responses for key factors for future technologies. The highest rate factors relevant for digital competency development in terms future technologies was digital micro, mobile e-learning, learning management systems. Digital competencies in relation advanced and industry technologies including gamification were rated moderately as key factors. Figure 5-3 shows the responses for the key factors for digitals skills and knowledge Information security certification was the highest rated factor and followed by digital forensic certifications, guidelines for evaluation where the highest rated factors.

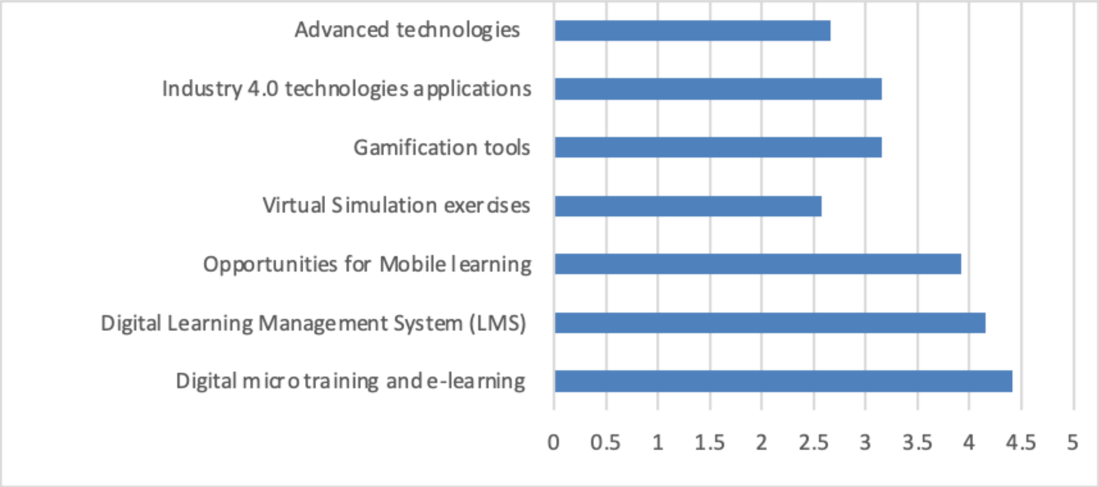


Figure 5-2 Key Factors for Future Technologies

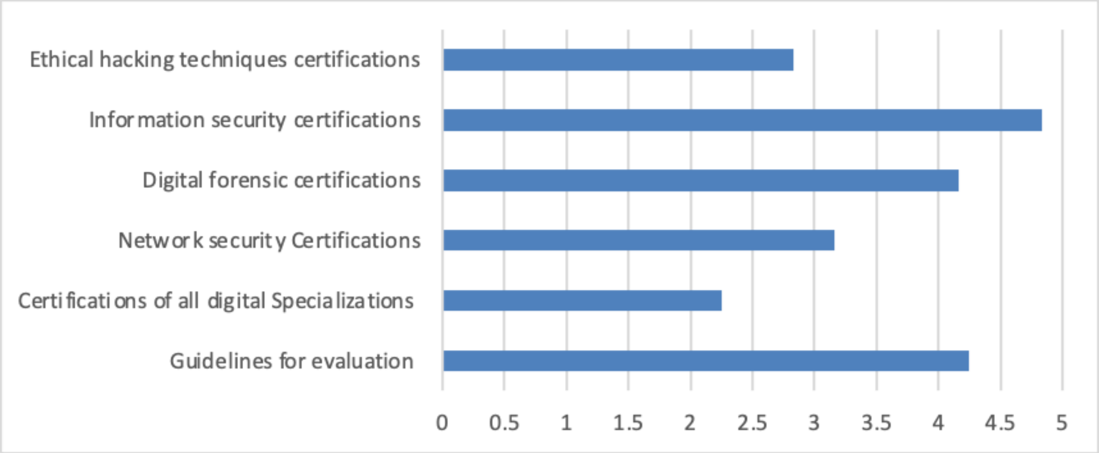


Figure 5-3 Key Factors for Digital Skills and Knowledge

The results for cybersecurity counter measures in Figure 5-4 shows that competencies based on cybercriminal profilin and situation awareness were the highest rated factors for proactive, reactive and preventative measures. The results in Figure 5-5 show the key factors for effective socio-technical system. Development forensic systems was the highest rated factor and then national cybercrime mapping. Further factors key to law enforcement digital competency for CIP was social media analysis and partnerships inter-organisational and with the public and private bodies. The quantitative results also identified critical factors from 37 items across eight dimensions as listed in Appendix 5.

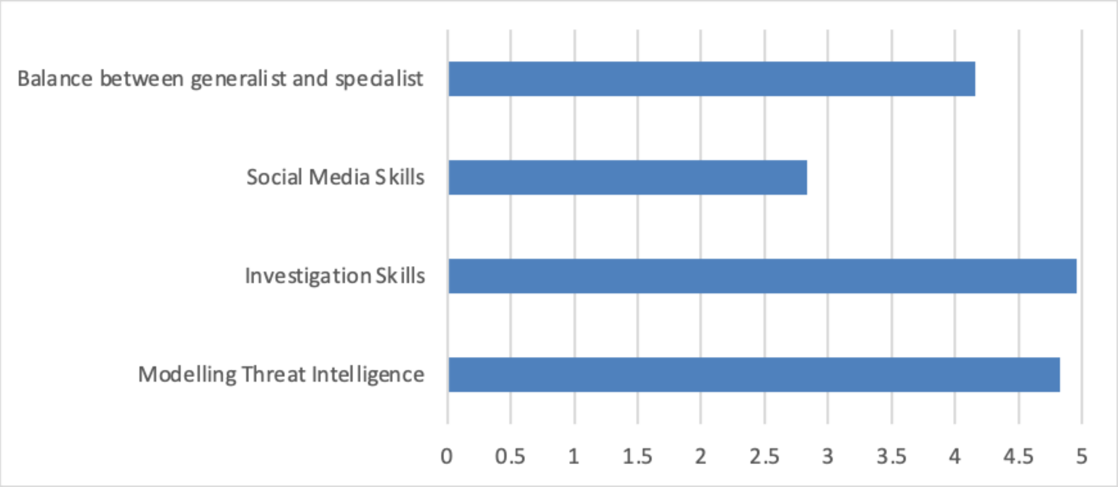


Figure 5-4 Cyberthreat Counter Measures

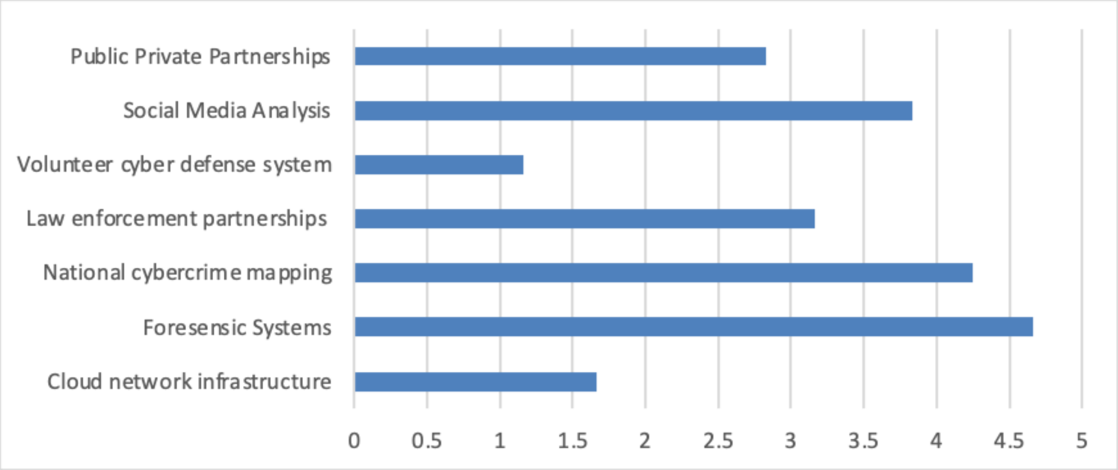


Figure 5-5 Effective Socio-Technical Systems

Error! Reference source not found. provides an overview of critical factors. For digital competence training 3 critical factors were identified: specialized cybercrime policing; critical infrastructure protection; and technological innovation.

Table 5.2 Critical Factors for Digital Competency Development

Dimension	Critical Factors
Digital Competence	• Specialized cybercrime policing such as (*digital forensics, network investigators* • Critical Infrastructure Protection • Technological innovation
CPD	• *Exercises and simulations* • *Frequency*
Skills Areas	• *Investigative Digital Competencies* • *Managerial digital competencies* • *Leadership competencies*
CIP Attack Phases	• *Post-Attack*
CIF	• *Reporting systems* • *Databases, records, & crime mapping*
CIF Effectiveness	• *Speed* • *Co-ordination, Resourcing*
Learning and Feedback	• *Continuous learning from Failure* • *Receptivity to learning* • *CIP global best practices*

For Continuous Professional Development (CPD) exercises and simulations and frequency of development were identified as the critical factors. In terms of skill areas digital competencies three critical areas were identified: investigative; managerial; and leadership competencies. The expert panel identified recording and reporting systems, databases and crime mapping as critical factors for critical infrastructure factors. Experts identified post-attack as most critical phase and speed, co-ordination and resourcing as critical factors for CIF effectiveness. In Terms of learning and feedback experts identified learning from failure; receptivity to learning and CIP global best practices as critical factors.

5.4 Delphi Phase 3– AHP analysis

5.4.1 Prioritisation of Cybersecurity Competence Categories

Participants were requested to prioritise the importance of seven categories of cybersecurity competencies identified in the NICE framework of: Analyse; Collect and Operate; Investigate; Operate and Maintain; Oversee and Govern; Protect and Defend; and Securely Provision. Analysis of the pairwise comparisons shows that the Investigate category was considered the most important by participants with a priority weight of 36%. **Error! Reference source not found.** shows that Analyse indicated the next highest priority of 26.2% followed by Collect and Operate (15.2%) and Protect and Defend (13%). Oversee and Govern (4.5%), Securely Provision (2.8%) and Operate and Maintain (2.4%) were considered the three least important criteria. The consensus responses conformed with the requirements for an acceptable ratio of consistency.

Table 5.3 NICE Competence Categories

NICE Competence Categories	A	CO	I	OM	OG	PD	SP	Priority Vector	Relative Weights %	Consistency Tests
Analyse	0.25	0.36	0.21	0.23	0.24	0.29	0.26	0.262	26.2%	$\lambda_{max=}$ 7.7533 CI= 0.125554 CR=0.095 < 0.10 (consistent)
Collect & Operate	0.08	0.12	0.14	0.18	0.24	0.10	0.21	0.152	15.2%	
Investigate	0.50	0.36	0.42	0.23	0.27	0.48	0.26	0.360	36.0%	
Operate & Maintain	0.03	0.02	0.05	0.03	0.01	0.01	0.03	0.024	2.4%	
Oversee & Govern	0.04	0.02	0.05	0.13	0.03	0.02	0.03	0.045	4.5%	
Protect & Defend	0.08	0.12	0.08	0.18	0.17	0.10	0.18	0.130	13.0%	
Securely Provision	0.03	0.02	0.05	0.03	0.03	0.02	0.03	0.028	2.8%	

5.4.2 Prioritisation of Specialty Areas and Work Roles

5.4.2.1 Investigate Speciality Areas and Work Roles

Based on the NICE competencies framework the Investigate category has two specialty areas of Cyber Investigation and Digital Forensics. As shown in **Error! Reference source not found.** Cyber Investigation ranked the highest specialty area with a weight of 60.5% while Digital Forensics was accorded a lower priority of 39.5%.

Table 5.4 Investigate Specialty Areas

Investigate Specialty Areas	CI	DF	Priority Vector	Relative Weights %	Consistency Tests
Cyber Investigation	0.62	0.64	0.605	60.5%	$\lambda_{max=}$ 3.0756 CI = 0.0378316 CR= 0.065
Digital Forensics	0.31	0.32	0.395	39.5%	

The NICE framework specifies three work roles in relation to Investigate competencies and specialty areas of Cybercrime Investigator, Law Enforcement/Counterintelligence Forensics Analyst and Cyber Defense Forensics Analyst. As **Error! Reference source not found.** shows the highest priority was accorded to Cybercrime Investigator (52.5%) followed by Law Enforcement/Counterintelligence Forensics Analyst (33.4%) with Cyber Defense Forensics Analyst recording the lowest priority with a score of 14.2%.

Table 5.5 Investigate Work Roles

Investigate Work Roles	CI	CFA	CDFA	Priority Vector	Relative Weights %	Consistency Tests
Cybercrime Investigator	0.55	0.60	0.43	0.525	52.5%	λ_{max}= 3.0653 CI=0.032 CR=0.0563
Law Enforcement Counterintelligence Forensics Analyst	0.27	0.30	0.43	0.334	33.4%	
Cyber Defense Forensics Analyst	0.18	0.10	0.14	0.142	14.2%	

5.4.2.2 Analyse Specialty Areas and Work Roles

The Analyse category is associated with five specialty areas of All-Source Analysis, Exploitation Analysis, Language Analysis and Targets Threat Analysis. The consensus responses summarised in **Error! Reference source not found.** indicate that All-Source Analysis and Threat Analysis were considered highest in priority with weightings of 41.6% and 31.3% respectively. Exploitation Analysis was rated third highest in priority (18.5%) while Targets was afforded the lowest priority (3%) overall.

The Analyse category is associated with a total of seven work roles of Threat/Warning Analyst, Exploitation Analyst, All-Source Analyst, Mission Assessment Specialist, Target Developer, Target Network Analyst, and Multi-Disciplined Language Analyst.

Table 5.7 shows that three work roles were most highly prioritised of All-Source Analyst (42.3%), Threat/Warning Analyst (24.2%) and Exploitation Analyst (16.2%). The remaining four work roles were accorded lower priority ranging between 7% for Multi-Disciplined Language Analyst to 2.6% for Mission Assessment Specialist.

Table 5.6 Analyse Specialty Areas

Analyse Specialty Areas	ASA	EA	LA	Ts	TA	Priority Vector	Relative Weights %	Consistency Tests
All-Source Analysis	0.48	0.41	0.34	0.29	0.56	0.416	41.6%	$\lambda_{max=}$ 5.4069 CI=0.101 CR=0.0908
Exploitation Analysis	0.16	0.14	0.25	0.29	0.09	0.185	18.5%	
Language Analysis	0.07	0.03	0.05	0.10	0.04	0.056	5.6%	
Targets	0.05	0.02	0.02	0.03	0.03	0.030	3.0%	
Threat Analysis	0.24	0.41	0.34	0.29	0.28	0.313	31.3%	

Table 5.7 Analyse Work Roles

Analyse Work Roles	T/WA	EA	ASA	MAS	TD	TNA	MDLA	Priority Vector	Relative Weights %	Consistency Tests
Threat/Warning Analyst	0.20	0.31	0.17	0.21	0.27	0.27	0.26	0.242	24.2%	$\lambda_{max=}$7.7883 CI=0.131 CR=0.099
Exploitation Analyst	0.07	0.10	0.10	0.21	0.20	0.20	0.26	0.162	16.2%	
All-Source Analyst	0.60	0.51	0.50	0.27	0.35	0.35	0.36	0.423	42.3%	
Mission Assessment Specialist	0.03	0.01	0.06	0.03	0.02	0.02	0.01	0.026	2.6%	
Target Developer	0.03	0.02	0.06	0.06	0.04	0.04	0.03	0.039	3.9%	
Target Network Analyst	0.03	0.02	0.06	0.06	0.04	0.04	0.03	0.039	3.9%	
Multi-Disciplined Language Analyst	0.04	0.02	0.07	0.15	0.08	0.08	0.05	0.070	7.0%	

5.4.2.3 Collect and Operate Specialty Areas and Work Roles

Of the three speciality areas comprising Collect and Operate competencies Cyber Operations was accorded the highest priority by participants of 57.1%. This was followed by Collection Operations with a weighting of 36.3% as shown in Table 5.8 while Cyber Operational Planning lagged behind in priority with a rating of 6.6%.

Table 5.8 Collect & Operate Specialty Areas

Collect & Operate Specialties	CO	COP	CyOP	Priority Vector	Relative Weights %	Consistency Tests
Collection Operations	0.32	0.47	0.30	0.363	36.3%	$\lambda_{max=}$3.0738 CI=0.036 CR=0.063
Cyber Operational Planning	0.05	0.07	0.09	0.066	6.6%	
Cyber Operations	0.64	0.47	0.61	0.571	57.1%	

The Collect and Operate category is linked to six work roles of All Source-Collection Manager, All Source-Collection Requirements Manager, Cyber Intel Planner, Cyber Ops Planner, Partner Integration Planner and Cyber Operator. Table 5.9 shows that Cyber Operator was accorded the highest priority over the other five work roles of 45.3%. This was followed by All Source-Collection Manager and All Source-Collection Requirements Manager which ranked second and third (19.2% and 18.5%, respectively). The least important work role was Partner Integration Planner with a weighting of 2.6%.

5.4.2.4 Protect and Defend Specialty Areas and Work Roles

Four specialty areas are associated with the Protect and Defend competencies of Cyber Defense Analysis, Cyber Defense Infrastructure Support, Incident Response and Vulnerability Assessment and Management.

Table 5.10 shows the results of the pairwise comparison with Incident Response accorded the highest priority of 51.3%. This was followed by Cyber Defense Analysis with a weighting of 31.7% and Vulnerability Assessment and Management with a priority of 13.1%. Cyber Defense Infrastructure Support ranked last with a weight of 3.9%.

Table 5.9 Collect & Operate Work Roles

Collect & Operate Work Roles	ASCM	ASCRM	CIP	COP	PIP	CO	Priority Vector	Relative Weights %	Consistency Tests
All Source-Collection Manager	0.18	0.15	0.25	0.20	0.21	0.17	0.192	19.2%	$\lambda_{max=}6.5549$
All Source-Collection Requirements Manager	0.18	0.15	0.25	0.20	0.21	0.13	0.185	18.5%	CI=0.110
Cyber Intel Planner	0.04	0.03	0.05	0.03	0.15	0.07	0.061	6.1%	CR=0.089
Cyber Ops Planner	0.06	0.05	0.10	0.07	0.15	0.07	0.082	8.2%	
Partner Integration Planner	0.03	0.02	0.01	0.01	0.03	0.06	0.026	2.6%	
Cyber Operator	0.53	0.60	0.35	0.48	0.26	0.51	0.453	45.3%	

Table 5.10 Protect & Defend Specialty Areas

Protect & Defend Specialty Areas	CDA	CDIS	IR	VAM	Priority Vector	Relative Weights %	Consistency Tests
Cyber Defense Analysis	0.29	0.38	0.28	0.33	0.317	31.7%	$\lambda_{max=}4.1680$
Cyber Defense Infrastructure Support	0.03	0.04	0.06	0.02	0.039	3.9%	CI=0.056
Incident Response	0.58	0.38	0.55	0.54	0.513	51.3%	CR=0.062
Vulnerability Assessment and Management	0.10	0.21	0.11	0.11	0.131	13.1%	

Similarly the priority of four Protect and Defend work roles of Cyber Defense Analyst, Cyber Defense Infrastructure Support Specialist, Cyber Defense Incident Responder and Vulnerability Assessment Analyst was compared. As shown in Table 5.11 Cyber Defense Incident Responder and Cyber Defence Analyst were considered the most important with weightings of 51% and 34.2% respectively. Cyber Defense Infrastructure Support Specialist had the least priority of 4.6%.

5.4.2.5 Oversee and Govern Specialty Areas and Work Roles

Six specialty areas were associated with the Oversee and Govern category of Cybersecurity Management, Executive Cyber Leadership, Legal Advice and Advocacy, Program/Project Management and Acquisition, Strategic Planning and Policy and Training, Education and Awareness. Three specialty areas were accorded the highest priority of Executive Cyber Leadership (46.3%), Cybersecurity Management (25.5%) and Legal Advice and Advocacy (14%) as shown in Table 5.12, while Program/Project Management and Acquisition and Strategic Planning and Policy were considered to be least important with a weighting of 3.4% each.

Table 5.11 Protect & Defend Work Roles

Protect & Defend Work Roles	CDA	CDISS	CDIR	VAA	Priority Vector	Relative Weights %	Consistency Tests
Cyber Defense Analyst	0.30	0.35	0.28	0.44	0.342	34.2%	λ_{max}=4.1411 CI=0.047 CR=0.052
Cyber Defense Infrastructure Support Specialist	0.04	0.05	0.06	0.03	0.046	4.6%	
Cyber Defense Incident Responder	0.60	0.45	0.55	0.44	0.510	51.0%	
Vulnerability Assessment Analyst	0.06	0.15	0.11	0.09	0.102	10.2%	

Table 5.12 Oversee & Govern Specialty Areas

Oversee & Govern Specialty Areas	CM	ECL	LA&A	PPMA	SPP	TEA	Priority Vector	Relative Weights %	Consistency Tests
Cybersecurity Management	0.21	0.17	0.27	0.29	0.26	0.34	0.255	25.5%	λ_{max}=6.5898 CI=0.117 CR=0.095
Executive Cyber Leadership	0.62	0.50	0.27	0.48	0.33	0.48	0.446	44.6%	
Legal Advice & Advocacy Program/Project	0.04	0.10	0.05	0.02	0.07	0.02	0.053	5.3%	
Management & Acquisition	0.07	0.10	0.22	0.10	0.19	0.07	0.122	12.2%	
Strategic Planning & Policy	0.03	0.06	0.03	0.02	0.04	0.02	0.032	3.2%	
Training, Education & Awareness	0.04	0.07	0.16	0.10	0.11	0.07	0.092	9.2%	

A total of fourteen work roles were associated with the Oversee and Govern category as shown in Table 5.13. The respondents considered that in this category the majority of the work roles were of equal importance in comparison to each other however one work role was rated significantly higher than any other of Executive Cyber Leadership with a priority of 19.6%.

The roles of Program Manager, Information Technology (IT) Project Manager, Product Support Manager, IT Investment/Portfolio Manager and IT Program Auditor were each weighted 6.6% while the remaining eight roles of Cyber Legal Advisor, Privacy Officer/Privacy Compliance Manager, Cyber Instructional Curriculum Developer, Cyber Instructor, Information Systems Security Manager, Communications Security Manager, Cyber Workforce Developer and Manager and Cyber Policy and Strategy Planner were prioritised as slightly less important with a rating of 5.9%.

5.4.2.6 Securely Provision Specialty Areas and Work Roles

As shown in Table 5.14 Securely Provision is comprised of seven specialty areas of Risk Management, Software Development, Systems Architecture, Systems Development, Systems Requirements Planning, Technology R&D and Test and Evaluation. Risk Management was considered to be of significantly higher priority than any other area with a weighting of 42.7% while Systems Architecture and Test and Evaluation were both accorded the next highest rating of 16.2%. The remaining specialty areas were all considered of lesser priority equally with a weighting of 6.3%.

In terms of work roles Securely Provision is associated with eleven in total as shown in Table 5.15. Two work roles are considered to be of the highest importance of Security Control Assessor and Security Architect with weightings of 29.2% and 15% respectively. The remaining work roles were accorded much lower and similar prioritisation ranging between 7.9% for System Test and Evaluation Specialist to 5.3% for both Information Systems Security Developer and Systems Developer.

Table 5.13 Oversee & Govern Work Roles

Roles	CLA	PO	CICD	CI	ISSM	CSM	CWDM	CPSP	ECL	PM	ITPM	PSM	IT IPM	IT PA	Priority Vector	Relative Weights %	Consistency Tests
CLA	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	$\lambda_{max=}$14.6798 CI=0.052 CR=0.033
PO	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.02	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
CICD	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
CI	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
ISSM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
CSM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
CWDM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
CPSP	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.03	0.07	0.07	0.07	0.07	0.07	0.059	5.9%	
ECL	0.28	0.32	0.28	0.28	0.28	0.28	0.28	0.28	0.13	0.07	0.07	0.07	0.07	0.07	0.196	19.6%	
PM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.13	0.07	0.07	0.07	0.07	0.07	0.066	6.6%	
ITPM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.13	0.07	0.07	0.07	0.07	0.07	0.066	6.6%	
PSM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.13	0.07	0.07	0.07	0.07	0.07	0.066	6.6%	
IT IPM	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.13	0.07	0.07	0.07	0.07	0.07	0.066	6.6%	
IT PA	0.06	0.05	0.06	0.06	0.06	0.06	0.06	0.06	0.13	0.07	0.07	0.07	0.07	0.07	0.066	6.6%	

Key: CLA=Cyber Legal Advisor; PO=Privacy Officer; CICD=Cyber Instructional Curriculum Developer; CI=Cyber Instructor; ISSM=Information Systems Security Manager; CSM=Communications Security Manager; CWDM=Cyber Workforce Developer and Manager; CPSP=Cyber Policy and Strategy Planner; ECL=Executive Cyber Leadership; PM=Program Manager; ITPM=Information Technology (IT) Project Manager; PSM=Product Support Manager; IT IPM=IT Investment/Portfolio Manager; IT PA= IT Program Auditor

Table 5.14 Securely Provision Specialty Areas

Securely Provision Specialty Areas	RM	SD	SA	SysD	SRP	TR&D	TE	Priority Vector	Relative Weights %	Consistency Tests
Risk Management	0.45	0.33	0.60	0.33	0.33	0.33	0.60	0.427	42.7%	λ_{max}=7.3823
Software Development	0.09	0.07	0.04	0.07	0.07	0.07	0.04	0.063	6.3%	
Systems Architecture	0.09	0.20	0.12	0.20	0.20	0.20	0.12	0.162	16.2%	CI=0.063
Systems Development	0.09	0.07	0.04	0.07	0.07	0.07	0.04	0.063	6.3%	
Systems Requirements Planning	0.09	0.07	0.04	0.07	0.07	0.07	0.04	0.063	6.3%	CR=0.048
Technology R&D	0.09	0.07	0.04	0.07	0.07	0.07	0.04	0.063	6.3%	
Test and Evaluation	0.09	0.20	0.12	0.20	0.20	0.20	0.12	0.162	16.2%	

Table 5.15 Securely Provision Work Roles

Securely Provision Work Roles	AO	SCA	SD	SSA	EA	SA	RDS	SRP	STES	ISSD	SyD	Priority Vector	Relative Weights %	Consistency Tests
Authorising Official	0.08	0.10	0.07	0.07	0.07	0.09	0.05	0.05	0.07	0.05	0.05	0.067	6.7%	λ_{max}=11.8491
Security Control Assessor	0.23	0.31	0.33	0.33	0.33	0.45	0.26	0.26	0.22	0.24	0.24	0.292	29.2%	
Software Developer	0.08	0.06	0.07	0.07	0.07	0.09	0.05	0.05	0.07	0.05	0.05	0.064	6.4%	
Secure Software Assessor	0.08	0.06	0.07	0.07	0.07	0.09	0.05	0.05	0.07	0.05	0.05	0.064	6.4%	CI=0.084
Enterprise Architect	0.08	0.06	0.07	0.07	0.07	0.09	0.05	0.05	0.07	0.05	0.05	0.064	6.4%	
Security Architect	0.08	0.06	0.07	0.07	0.07	0.09	0.26	0.26	0.22	0.24	0.24	0.150	15.0%	
Research and Development Specialist	0.08	0.06	0.07	0.07	0.07	0.02	0.05	0.05	0.07	0.05	0.05	0.057	5.7%	CR=0.055
Systems Requirements Planner	0.08	0.06	0.07	0.07	0.07	0.02	0.05	0.05	0.07	0.05	0.05	0.057	5.7%	
System Test & Evaluation Specialist	0.08	0.10	0.07	0.07	0.07	0.03	0.05	0.05	0.07	0.14	0.14	0.079	7.9%	
Information Systems Security Developer	0.08	0.06	0.07	0.07	0.07	0.02	0.05	0.05	0.02	0.05	0.05	0.053	5.3%	
Systems Developer	0.08	0.06	0.07	0.07	0.07	0.02	0.05	0.05	0.02	0.05	0.05	0.053	5.3%	

5.4.2.7 Operate and Maintain Specialty Areas and Work Roles

Operate and Maintain is associated with six specialty areas related to customer service, administration of data, and administration of systems and networks. Table 5.16 shows that two specialty areas were considered of much higher priority than the remainder of Data Administration (40.6%), and Knowledge Management (30.6%). The lowest priority specialty area was Customer Service and Technical Support with a weighting of 3.2%.

Seven work roles are linked to the Operate and Maintain category. As

Table 5.17 shows three work roles were most prioritised of Data Analyst, Database Administrator and Knowledge Manager with weightings of 39.6%, 26.1% and 17.2% respectively. The lowest priority of 3.6% was accorded to three work roles of Technical Support Specialist, Network Operations Specialist, and System Administrator.

Table 5.16 Operate & Maintain Specialty Areas

Operate & Maintain Specialty Areas	CSTS	DA	KM	NS	SA	SAn	Priority Vector	Relative Weights %	Consistency Tests
Customer Service and Technical Support	0.04	0.08	0.02	0.02	0.02	0.02	0.032	3.2%	$\lambda_{max=}6.6102$ CI=0.122 CR=0.098
Data Administration	0.27	0.55	0.66	0.47	0.47	0.47	0.480	48.0%	
Knowledge Management	0.35	0.18	0.22	0.36	0.36	0.36	0.306	30.6%	
Network Services	0.12	0.06	0.03	0.05	0.05	0.05	0.061	6.1%	
Systems Administration	0.12	0.06	0.03	0.05	0.05	0.05	0.061	6.1%	
Systems Analysis	0.12	0.06	0.03	0.05	0.05	0.05	0.061	6.1%	

Table 5.17 Operate & Maintain Work Roles

Operate & Maintain Work Roles	DA	DAn	KM	TSS	NOS	SA	SSA	Priority Vector	Relative Weights %	Consistency Tests
Database Administrator	0.24	0.22	0.29	0.27	0.27	0.27	0.27	0.261	26.1%	$\lambda_{max=}7.1464$ CI=0.024 CR=0.0184
Data Analyst	0.48	0.43	0.44	0.35	0.35	0.35	0.38	0.396	39.6%	
Knowledge Manager	0.12	0.14	0.15	0.19	0.19	0.19	0.22	0.172	17.2%	
Technical Support Specialist	0.03	0.05	0.03	0.04	0.04	0.04	0.03	0.036	3.6%	
Network Operations Specialist	0.03	0.05	0.03	0.04	0.04	0.04	0.03	0.036	3.6%	
System Administrator	0.03	0.05	0.03	0.04	0.04	0.04	0.03	0.036	3.6%	
Systems Security Analyst	0.05	0.06	0.04	0.08	0.08	0.08	0.05	0.062	6.2%	

5.4.3 Summary of AHP Results

The following section provides a summary of the AHP results for cybersecurity competences, speciality areas and work roles. The expert panel was asked to rank and evaluate the importance of different elements and sub-elements of the NICE Cybersecurity Education Framework. This comprised 7 high-level cybersecurity functions, 33 speciality areas and 52 work roles. The panel completed a total of 14 matrices each of which contained every possible pairing between the items within it. The experts first compared and assessed the importance of the 7 cybersecurity functions to law enforcement for critical physical infrastructure. Judgements were made using a numerical pairwise comparison scale that could indicate increased or decreased priority when one item was compared with another. Experts then evaluated the importance of the specialty areas under each high-level category, with pairwise comparisons conducted that assigned a priority weighting to each specialty area in relation to every other area under that function. Finally pairwise comparisons were made in relation to the work roles associated with each function according to the NICE cybersecurity framework.

The results summarised in the tables below identify the overall or absolute importance of each specialty area and work role in relation to all the others and ranks them, as well as indicating the relative priority of the elements within each category. The absolute weighting was calculated by multiplying the relative weighting of the element with the weighting of the Competence Category to which it belongs. In Table 5.18 the seven Competence categories are ranked in order of the priority accorded to them, showing that the Investigate category is considered most important, followed by Analyse, Collect & Operate and Protect & Defend. With a drop in weighting Oversee and Govern, Securely Provision and Operate & Maintain were considered the three least important criteria. In terms of the absolute prioritisation of the specialty areas across all cybersecurity functions the table shows that Cyber Investigation was the most important specialty area for cybersecurity of CPI by law enforcement. This received nearly-one-fifth of the available weighting. Digital Forensics was the next most prioritised specialty area, followed by All-Source Analysis.

Table 5.18 Summary of AHP Results for Functions and Specialty Areas

Competence Categories	Weight	Specialty Areas	Relative Weight	Absolute Weight	Rank
Investigate	0.360	Cyber Investigation	0.605	0.218	1
		Digital Forensics	0.395	0.142	2
Analyse	0.262	All-Source Analysis	0.416	0.109	3
		Threat Analysis	0.313	0.082	5
		Exploitation Analysis	0.185	0.048	8
		Language Analysis	0.056	0.015	12
		Targets	0.03	0.008	16
Collect & Operate	0.152	Cyber Operations	0.571	0.087	4
		Collection Operations	0.363	0.055	7
		Cyber Operational Planning	0.066	0.010	16
Protect & Defend	0.13	Incident Response	0.513	0.067	6
		Cyber Defense Analysis	0.317	0.041	9
		Vulnerability Assessment and Management	0.131	0.017	11
		Cyber Defense Infrastructure Support	0.039	0.005	19
Oversee & Govern	0.045	Executive Cyber Leadership	0.446	0.020	10
		Cybersecurity Management	0.255	0.011	15
		Program/Project Management & Acquisition	0.122	0.005	18

Competence Categories	Weight	Specialty Areas	Relative Weight	Absolute Weight	Rank
		Training, Education & Awareness	0.092	0.004	21
		Legal Advice & Advocacy Program/Project	0.053	0.002	22
		Strategic Planning & Policy	0.032	0.001	25
Securely Provision	0.028	Risk Management	0.427	0.012	13
		Systems Architecture	0.162	0.005	20
		Test and Evaluation	0.162	0.005	20
		Software Development	0.063	0.002	23
		Systems Development	0.063	0.002	23
		Systems Requirements Planning	0.063	0.002	23
		Technology R&D	0.063	0.002	23
Operate & Maintain	0.024	Data Administration	0.480	0.012	14
		Knowledge Management	0.306	0.007	17
		Network Services	0.061	0.001	24
		Systems Administration	0.061	0.001	24
		Systems Analysis	0.061	0.001	24
		Customer Service and Technical Support	0.032	0.001	26

Similar priorities were next given to Cyber Operations and Threat Analysis, followed by Incident Response, ranked 6th in importance, Collection Operations, Exploitation Analysis and Cyber Defence Analysis. These results are consistent with those for the Competency Categories results, as all of these specialty areas are associated with the top 4 most prioritised categories. Specialty areas from the Oversee and Govern competency category represent the next 3 most prioritised areas of Executive Cyber Leadership, Vulnerability Assessment and Management and Language Analysis. The five least prioritised specialty areas are from the Operate and Maintain domain with Customer Service and Technical Support considered of least importance overall.

In terms of relative weightings, of the two specialty areas in the Investigate category Cyber Investigation scored highest followed by Digital Forensics. For Analyse competencies, All-Source Analysis was the most highly prioritised followed by Threat Analysis and Exploitation Analysis. Targets was the least prioritised in this category. Cyber Operations was the most prioritised specialty area in the Collect & Operate category by some margin over Collection Operations and Cyber Operational Planning with the latter attracting low weightings. In the Protect and Defend category Incident Response achieved the highest rating followed by Cyber Defense Analysis and Vulnerability Assessment and Management. Cyber Defense Infrastructure Support was the least highly prioritised. Of the final three categories, Executive Cyber Leadership was the most important specialty area in the Oversee & Govern function, followed by Cybersecurity Management and Project Management & Acquisition. The least important speciality area was Strategic Planning & Policy. For Securely Provision, Risk Management specialty area was weighted twice as highly as the next two specialty areas of Systems Architecture and Test and Evaluation. For the final category of Operate & Maintain, Data Administration and Knowledge Management were the most highly prioritised while Customer Service and Technical Support was accorded least importance.

Table 5.19 shows the absolute and relative importance for the work roles associated with each cybersecurity Competency Category.

Table 5.19 Summary of Results for Work Roles

Competence Categories	Weight	Work Roles	Relative Weight	Absolute Weight	Rank
Investigate	0.360	Cybercrime Investigator	0.525	0.189	1
		Law Enforcement/ Counterintelligence Forensics Analyst	0.334	0.120	2
		Cyber Defense Forensics Analyst	0.142	0.051	7
Analyse	0.262	All-Source Analyst	0.423	0.111	3
		Threat/Warning Analyst	0.242	0.063	6
		Exploitation Analyst	0.162	0.042	9
		Multi-Disciplined Language Analyst	0.070	0.018	12
		Target Developer	0.039	0.010	15
		Target Network Analyst	0.039	0.010	15
		Mission Assessment Specialist	0.026	0.007	20
Collect & Operate	0.152	Cyber Operator	0.453	0.069	4
		All Source-Collection Manager	0.192	0.029	10
		All Source-Collection Requirements Manager	0.185	0.028	11
		Cyber Ops Planner	0.082	0.012	14
		Cyber Intel Planner	0.061	0.009	17
		Partner Integration Planner	0.026	0.004	25
Protect & Defend	0.13	Cyber Defense Incident Responder	0.510	0.066	5
		Cyber Defense Analyst	0.342	0.044	8
		Vulnerability Assessment Analyst	0.102	0.013	13
		Cyber Defense Infrastructure Support Specialist	0.046	0.006	22
Oversee & Govern	0.045	Executive Cyber Leadership	0.196	0.009	18
		Program Manager	0.066	0.003	26
		Information Technology (IT) Project Manager	0.066	0.003	26
		Product Support Manager	0.066	0.003	26
		IT Investment/Portfolio Manager	0.066	0.003	26

		IT Program Auditor	0.066	0.003	26
		Cyber Legal Advisor	0.059	0.003	27
		Privacy Officer	0.059	0.003	27
		Cyber Instructional Curriculum Developer	0.059	0.003	27
		Cyber Instructor	0.059	0.003	27
		Information Systems Security Manager	0.059	0.003	27
		Communications Security Manager	0.059	0.003	27
		Cyber Workforce Developer and Manager	0.059	0.003	27
		Cyber Policy and Strategy Planner	0.059	0.003	27
Securely Provision	0.028	Security Control Assessor	0.292	0.008	19
		Security Architect	0.150	0.004	23
		System Test & Evaluation Specialist	0.079	0.002	28
		Authorizing Official	0.067	0.002	29
		Software Developer	0.064	0.002	30
		Secure Software Assessor	0.064	0.002	30
		Enterprise Architect	0.064	0.002	30
		Research and Development Specialist	0.057	0.002	31
		Systems Requirements Planner	0.057	0.002	31
		Information Systems Security Developer	0.053	0.001	33
		Systems Developer	0.053	0.001	33
Operate & Maintain	0.024	Data Analyst	0.396	0.010	16
		Database Administrator	0.261	0.006	21
		Knowledge Manager	0.172	0.004	24
		Systems Security Analyst	0.062	0.001	32
		Technical Support Specialist	0.036	0.001	34
		Network Operations Specialist	0.036	0.001	34
		System Administrator	0.036	0.001	34

This identifies that overall the role of Cybercrime Investigator was considered the most important across the categories. This is highly consistent with the results for specialty areas and the categories themselves. In terms of the remaining work roles, the table shows that the highest overall priorities were distributed among a further 16 work roles before dropping to less than 1% of the absolute weighting. The next two roles in importance were Law Enforcement/Counterintelligence Forensics Analyst and All-Source Analyst while more moderate significance was given to the roles of Cyber Operator, Cyber Defense Incident Responder, Threat/Warning Analyst, Cyber Defense Forensics Analyst, Cyber Defense Analyst and Exploitation Analyst. All of these roles are associated with the top four competence categories identified earlier. Data Analyst, ranked 16th in importance, is the first work role from another category namely Operate & Maintain. Following these top nine work roles, All Source-Collection Manager and All Source-Collection Requirements Manager are ranked the next highest in importance. The competency category of Oversee & Govern has multiple job roles that all receive a similar modest weighting including Program Manager, Information Systems Security Manager, and Cyber Policy and Strategy Planner. Securely Provision work roles related to systems development and Operate & Maintain roles related to technical support, network operations and system administration ranked the least highest in importance.

In terms of the relative importance of the work roles within each category, Table 5.19 shows that Cybercrime Investigator was considered most important in the Investigate category by a moderate margin over the second most prioritised of Law Enforcement Counterintelligence Forensics Analyst. The least weighted role was that of Cyber Defense Forensics Analyst. For the Analyse category the most important roles were All-Source Analyst, Threat Analyst and Exploitation Analyst while Mission Assessment Specialist received the lowest priority. Cyber Operator was accorded the highest importance in the Collect & Operate category with some margin over all other job roles. All Source-Collection Manager and All Source-Collection Requirements Manager were found to be next highest in priority. The least important were planner roles with Partner Integration Planner accorded the lowest weighting. In the Protect & Defend category, the most highly prioritised job roles were Cyber Defense Incident

Responder and Cyber Defense Analyst while Cyber Defense Infrastructure Support Specialist was least prioritised. Of the 14 work roles in the Oversee & Govern category, priority weightings were fairly evenly balanced among all of them except for the role of Executive Cyber Leadership which attracted a much higher weighting. Securely Provision is associated with 11 work roles of which Security Control Assessor and Security Architect are considered the most important, and Systems Developer the least. Lastly in the Operate and Maintain category work roles in relation to data analysis and data administration as well as knowledge management attracted higher weightings than the remaining roles, with technical support roles recording the lowest weightings.

In the NICE framework knowledge, skills, and ability competencies as well as task competencies are defined under the categories and associated with each work role for that function. Table 5.20 maps the knowledge, skills, abilities and tasks (KSATs) for the top 15 work roles identified in the AHP analysis of the 52 work roles in the framework. The table shows that for the top 5 most prioritised work roles the framework specifies over 430 digital competencies in terms of knowledge, skills, abilities and tasks. In the AHP analysis the top three most important work roles were Cyber Investigator, Law Enforcement/ Counterintelligence Forensics Analyst and All-Source Analyst. This provides an indication of the most prioritised KSATs. The Cyber Investigator role is the most prioritised, and is associated with 2 ability competencies, 4 skills competencies, 25 knowledge competencies, and 24 tasks including:

- Knowledge of dark web (A0174)
- Investigation abilities across different operating system platforms (A0175)
- Evidence preservation skills (S0047)
- Maintaining evidence integrity across processes (S0068)
- Intrusion detection skills (K0046)
- Cybercrime tactics, techniques, and procedures (K0110)

Law Enforcement/ Counterintelligence Forensics Analyst is the second most prioritised work role and is associated with 2 ability competencies, 19 skill competencies, 42 knowledge competencies, and 33 tasks including:

- Decryption skills (A0005)
- Information extraction skills (S0062)

- Use of forensic tool suites (e.g., EnCase, Sleuthkit, FTK) (S0071)
- Knowledge of hacking methodologies (K0119)
- Digital forensics data types (K0133)

All-Source Analyst is associated in the framework with 18 ability competencies, 18 skill competencies, 56 knowledge competencies, and 42 tasks including:

- Ability to accurately and completely source all data used in intelligence, assessment and/or planning products (A0066)
- Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes (A0072)
- Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships (S0256)
- Skill in evaluating information for reliability, validity, and relevance (S0218)
- Knowledge of network traffic analysis methods (K0058)
- Knowledge of cyber intelligence/information collection capabilities and repositories (K0409)

The weightings assigned to the work roles suggest that the three most prioritised are concerned predominantly with investigative functions in terms of investigating cybercrimes and identifying, collecting, examining and preserving digital evidence and establishing intelligence. As shown in Table 5.20 the next most prioritised work roles of Cyber Operator and Cyber Defense Incident Responder are mainly operationally focused and involve locating targets and responding to cyber incidents. The next three work roles of Cyber Defense Forensics Analyst, Threat/Warning Analyst, and Cyber Defense Analyst centre on environmental and situational awareness emphasising analysis of trends and patterns that can help mitigate threats and vulnerabilities. The roles of All Source-Collection Manager, All Source-Collection Requirements Manager and Exploitation Analyst are broadly concerned with the collection of relevant data and information that can assist investigation and mitigation efforts. The final four roles of Data Analyst, Executive Cyber Leadership, Security Control Assessor and Database Administrator focus more generally on how data and information is managed and controlled.

Table 5.20 Knowledge, Skills and Abilities for Work Roles

Rank	Work Roles	Role	Competencies			
			Knowledge	Skills	Abilities	Tasks
1	**CYBERCRIME INVESTIGATOR** - Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques		K0001-6; K0046; K0070; K0107; K0110; K0114; K0118; K0124; K0125; K0128; K0144; K0155-56; K0168; K0209; K0231; K0244; K0251; K0351; K0624	S0047;S0068; S0072;S0086	A0174-75	T0031; T0059; T0096; T0103-104; T0110; T0112-14;T0120; T0193; T0225; T0241; T0342; T0346; T0360; T0386; T0423; T0430; T0433; T0353; T0471; T0479; T0523
2	**Law Enforcement/ Counterintelligence Forensics Analyst** Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.		K0001-6; K0017; K0021; K0042; K0060; K0070; K0077-8; K0107; K0109; K0117-9; K0122-3; K0125; K0128; K0131-4; K0145; K0155-6; K0167-8; K0179; K0182-9; K0305; K0624	S0032; S0046-7; S0062; S0065; S0067-9; S0071; S007-5; S0087; S0088-93;	A0005; A0175;	T0027; T0036; T0048; T0075; T0087; T0103; T0113; T0120; T0165; T0167-8; T0172; T0173; T0179; T0182; T0190; T0193; T0212; T0216; T0238; T0240-1; T0246; T0253; T0285-9; T0432; T0439; T0471; T0532;
3	**All-Source Analyst** Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.		K0001-6; K0036; K0058; K0108-9; K0177; K0221; K0349; K0357; K0362; K0377; K0392; K0395; K0405; K0409-10; K0427; K0431; K0436-7; K0440; K0444-6; K0449; K0457-8; K0460; K0464-5; K0469; K0471; K0480; K0507; K0511; K0516; K0533; K0542; K0549; K0551; K0556; K0560; K0561; K0565; K0577; K0598; K0603-4; K0610; K0612; K0614;	S0189; S0194; S0203; S0211; S0218; S0227; S0229; S0249; S0254; S0256; S0278; S0285; S0288-9; S0296-7; S0303; S0360;	A0013; A0066; A0072; A0080; A0082-5; A0087-9; A0091; A0101-2; A0106-9;	T0167; T0172; T0569; T0582-6; T0589; T0593; T0597; T0615; T0617; T0642; T0660; T0678; T0685-7; T0707-8; T0710; T0713; T0718; T0748-9; T0751-2; T0758; T0761; T0771; T0782-3; T0785-6; T0788-9; T0792; T0797; T0800; T0805; T0834;
4	**Cyber Operator** Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.		K0001-6; K0009; K0021; K0051; K0109; K0142; K0224; K0363; K0372-3; K0375; K0379; K0403; K0406; K0420; K0423; K0427-30; K0433; K0438; K0440; K0452; K0468; K0480-1; K0485-6; K0516; K0528; K0530-1; K0536; K0560; K0565; K0573; K0608-	S0062; S0182-3; S0190; S0192; S0202; S0206; S0221; S0236; S0242-3; S0252; S0255; S0257; S0266-7; S0270;	A0095; A0097; A0099-100;	T0566-7; T0598; T0609-10; T0612; T0616; T0618-20; T0623; T0643-4; T0664; T0677; T0696-7; T0724; T0740; T0756; T0768; T0774; T0796; T0804; T0828-9;

		9;	S0275-6; S0281-2; S0293; S0295; S0298-9; S0363;		
5	**Cyber Defense Incident Responder** Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	K0001-6; K0021; K0026; K00334; K0041-2; K0046; K0058; K0062; K0070; K0106; K0157; K0161-2; K0167; K0177; K0179; K0221; K0230; K0259; K0287; K0332; K0565; K0624;	S0003; S0047; S0077-80; S0173; S0365;	A0121; A0128;	T0041; T0047; T0161; T0163-4; T0170; T0175; T0214; T0233; T0246; T0262; T0278-9; T0312; T0395; T0503; T0510;
6	**Cyber Defense Forensics Analyst** Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	K0001-6; K0018; K0021; K0042; K0060; K0070; K0077-8; K0109; K0117-9; K0122-3; K0125; K0128; K0131-4; K0145; K0155-6; K0167-8; K0179; K0182-9; K0224; K0254-5; K0301; K0304; K0347; K0624;	S0032; S0047; S0062; S0065; S0067-9; S0071; S0073-5; S0087-93; S0131-3; S0156;	A0005; A0043;	T0027; T0036; T0048-9; T0075; T0087; T0103; T0113; T0165; T0167-8; T0173; T0175; T0179; T0182; T0190; T0212; T0216; T0238; T0240-1; T0253; T0279; T0285-9; T0312; T0396-401; T0432; T0532; T0546;
7	**Threat/Warning Analyst** Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.	K0001-6; K0036; K0058; K0108-9; K0177; K0349; K0362; K0377; K0392; K0395; K0405; K0409; K0415; K0417; K0427; K0431; K0436-7; K0440; K0445-6; K0449; K0458; K0460; K0464; K0469; K0471; K0480; K0499; K0511; K0516; K0556; K0560-1; K0565; K0603-4; K0610; K0612; K0614	S0194; S0196; S0203; S0211; S0218; S0227; S0228-9; S0249; S0256; S0278; S0285; S0288-9; S0296-7; S0303;	A0013; A0066; A0072; A0080; A0082-4; A0087-9; A0091; A0101-2; A0106; A0107; A0109;	T0569; T0583-6; T0589; T0593; T0597; T0615; T0617; T0660; T0685; T0687; T0707-8; T0718; T0748-9; T0751-2; T0758; T0761; T0783; T0785-6; T0792; T0800; T0805; T0834;
8	**Cyber Defense Analyst** Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	K0001-7; K0013; K0015; K0018-9; K0024; K0033; K0040; K0042; K0044; K0046; K0049; K0056; K0058-61; K0065; K0070; K0074; K0075; K0093; K0098; K0104; K0106-7; K0110-3; K0116; K0139; K014-3; K0157; K0160-2; K0167-8; K0177; K0179-80; K0190-2; K0203; K0221-2; K0260-2; K0290; K0297; K0300-1; K0303;	S0020; S0025; S0027; S0036; S0054; S0057; S0063; S0078; S0096; S0147; S0156; S0167; S0169; S0367; S0370;	A0010; A0015; A0066; A0123; A0128; A0159;	T0020; T0023; T0043; T0088; T0155; T0164; T0166; T0178; T0187; T0198; T0214; T0258-60; T0290-310; T0332; T0469-70; T0475; T0503; T0504; T0526; T0545; T0548;

		K0318; K0322; K0324; K0332; K0339; K0342; K0624;			
9	**All Source-Collection Manager** Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.	K0001-6; K0036; K0058; K0109; K0177; K0353; K0361; K0364; K0380; K0382-3; K0386-7; K0390; K0392; K0395; K0401; K0404-5; K0412; K0417; K0419; K0425; K0427; K0431; K0435; K0440; K0444-6; K0448-9; K0453-4; K0467; K0471; K0474-5; K0477; K0480; K0482; K0492; K0495-6; K0498; K0503; K0505; K0513; K0516; K0521-2; K0526-7; K0552-4; K0558; K0560-3; K0565; K0569-70; K0579-81; K0583-4; K0587-8; K0596; K0601; K0605; K0610; K0612-3;	S0238; S0304-5; S0311; S0313; S0316-7; S0324-5; S0327-8; S0330; S0332; S0334-6; S0339; S0342; S0344; S0347; S0351; S0352; S0362;	A0069-70; A0076; A0078-9;	T0562; T0564; T0568; T0573; T0578; T0604; T0605; T0625; T0626; T0631; T0632; T0634; T0645-6; T0647; T0649; T0651; T0657; T0662; T0674; T0681; T0683; T0698; T0702; T0714; T0716; T0721; T0723; T0725; T0734; T0737; T0750; T0753; T0755; T0757; T0773; T0779; T0806; T0809; T0810-2; T0814; T0820-1; T0827;
10	**All Source-Collection Requirements Manager** Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.	K0001-6; K0036; K0058; K0109; K0177; K0353; K0361; K0364; K0380; K0382-4; K0386; K0387; K0390; K0395; K0401; K0404; K0412; K0417; K0419; K0421; K0425; K0427; K0431; K0435; K0444-6; K0448; K0453; K0454; K0467; K0474; K0475; K0477; K0480; K0482; K0492; K0495-6; K0498; K0505; K0513; K0516; K0521; K0526-7; K0552; K0554; K0558; K0560-1; K0562-3; K0565; K0568-70; K0579-81; K0584; K0587-8; K0596; K0605; K0610; K0612;	S0304-5; S0316-7; S0327; S0329-30; S0334-7; S0339; S0344; S0346-8; S0352-3; S0362;	A0069-70; A0078;	T0564-5; T0568; T0577-8; T0580; T0596; T0602; T0605; T0613; T0651; T0668; T0673; T0675; T0682; T0689; T0693-4; T0714; T0725; T0730; T0734; T0746; T0780; T0809; T0810-1; T0819; T0822; T0830-3;
11	**Exploitation Analyst** Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized	K0001-6; K0009; K0108-9; K0131; K0142-3; K0177; K0224; K0349; K0351; K0354; K0362; K0368; K0371; K0376; K0379; K0388; K0393-4;	S0066; S0184; S0199; S0200-1; S0204; S0207; S0214; S0223;	A0013; A0066; A0074; A0080; A0084; A0086; A0092-3; A0104;	T0028; T0266; T0570; T0572; T0574; T0591; T0600; T0603; T0608; T0614; T0641; T0695; T0701; T0720; T0727; T0736; T0738; T0754; T0775; T0777;

	resources and analytic techniques to penetrate targeted networks.	K0397; K0417-8; K0430; K0443-4; K0447; K0451; K0470-1; K0473; K0484; K0487; K0489; K0509-10; K0523; K0529; K0535; K0544; K0557; K0559-60; K0608;	S0236-7; S0239-40; S0245; S0247; S0258; S0260; S0264; S0269; S0279; S0286; S0290; S0294; S0300;		
12	**Data Analyst** Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.	K0001-6; K0015-6; K0020; K0022-3; K0025; K0031; K0051-2; K0056; K0060; K0065; K0068-9; K0083; K0095; K0129; K0139-40; K0193; K0197; K0229; K0236; K0238; K0325; K0420;	S0013; S0017; S0028; S0029; S0037; S0060; S0088-9; S0094-5; S0103; S0106; S0109; S0113-4; S0118-9; S0123; S0125-7; S0129-30; S0160; S0202; S0369;	A0029; A0035; A0036; A0041; A0066;	T0007-8; T0068; T0146; T0195; T0210; T0342; T0347; T0349; T0351; T0353; T0361; T0366; T0381-3; T0385; T0392; T0402-5; T0460;
13	**Executive Cyber Leadership** Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.	K0001-6; K0009; K0070; K0106; K0147; K0296; K0314; K0624; K0628;	S0018; S0356-9;	A0033; A0070; A0085; A0094; A0105-6; A0116-9; A0129-30;	T0001-2; T0004; T0006; T0025; T0066; T0130; T0134; T0135; T0148; T0151; T0227; T0229; T0248; T0254; T0263; T0264; T0282; T0337; T0356; T0429; T0445; T0509; T0763; T0871-2; T0927-8;
14	**Security Control Assessor** Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	K0001-11; K0013; K0018-9; K0021; K0024; K0026-9; K0037; K0038; K0040; K0044; K0048-9; K0054; K0056; K0059; K0070; K0084; K0089; K0098; K0100-1; K0126; K0146; K0168-70; K0179; K0199; K0203; K0260-2; K0267; K0287; K0322; K0342; K0622; K0624;	S0001; S0006; S0027; S0034; S0038; S0073; S0078; S0097; S0100-12; S0115; S0120; S0124; S0128; S0134-8; S0141; S0145; S0147; S0171-7; S0184; S0232-44;	A0001; A0011-6; A0018-9; A0023; A0026; A0030; A0035-6; A0040; A0056; A0069; A0070; A0082-96; A0098; A0101; A0106; A0108-9; A0111-2; A0114-9;	T0145; T0177-8; T0181; T0184; T0205; T0221; T0243-4; T0251; T0255; T0264-5; T0268; T0272; T0275; T0277; T0309; T0344; T0371; T0495;

			S0248-52; S0254; S0271; S0273; S0278-81; S0296; S0304-7; S0325; S0329; S0332; S0367; S0370; S0374;	A0123; A0170;	
15	**Database Administrator** Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.	K0001-6; K0020-3; K0025; K0031; K0056; K0060; K0065; K0069; K0083; K0097; K0197; K0260-2; K0277-8; K0287; K0420;	S0002; S0013; S0037; S0042; S0045;	A0176;	T0008; T0137; T0139; T0140; T0146; T0152; T0162; T0210; T0305; T0306; T0330; T0422; T0459; T0490;

5.5 Delphi Phase 4 –Group Model Building

The final phase of the Delphi involved group model building to propose an initial framework or seed model for the development of law enforcement digital competencies for the protection of critical physical infrastructure. The qualitative analysis has revealed 8 elements to be utilised for developing effective CPI protection in the UAE. The findings were grouped along the qualitative themes that emerged from thematic analysis namely 1) Balance, Type, & Relevance of Training; 2) Futuristic Training & Unconventional techniques; 3) Mandatory certifications; Digital knowledge and skills; 4) Non-Technical Digital Competences; 5) Proactive, Reactive, Preventative Measures; 6) Socio-Technical System (Cloud, Public, & Volunteer Defenders); 7) Resilience, and 8) Adaptive Learning. The results of the group model building stage shows that a diverse range of ideas were identified including training, systems, legislations, and learning. These themes/parameters have been set against the policy levers namely digital policing policy, digital governance policy, digital regulations policy, and digital collaborations policy.

Figure 5-6 shows the initial framework for CPI protection in the UAE that emerged from the group model building stage. This shows several key inputs to critical infrastructure protection of socio-technical systems, resilience, strategic organisational training and learning from best practice examples each with multiple characteristics important for the effectiveness of each input.

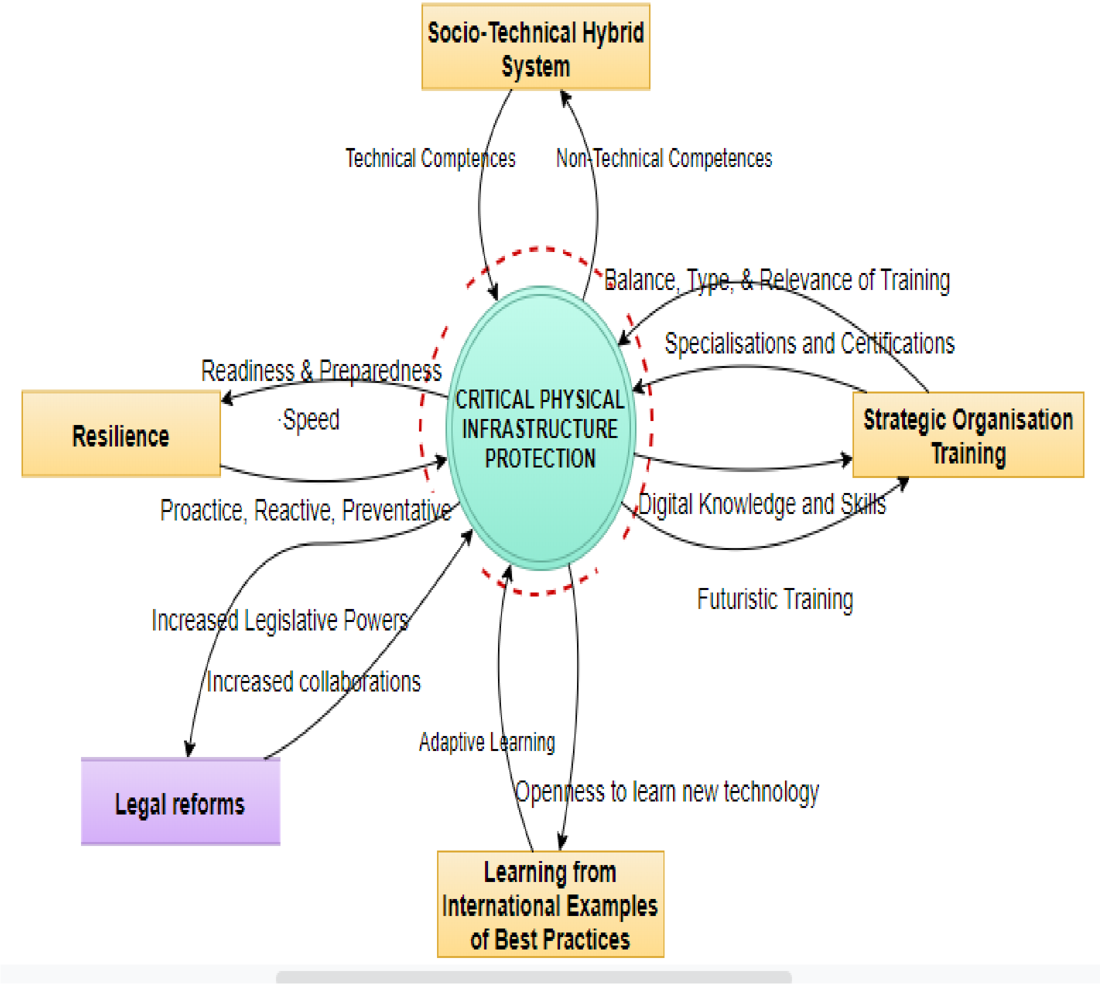

Socio-Technical Hybrid System
Technical Comptences
Non-Technical Competences
Balance, Type, & Relevance of Training
Specialisations and Certifications
Strategic Organisation Training
Digital Knowledge and Skills
Futuristic Training
Readiness & Preparedness
Speed
Resilience
Proactice, Reactive, Preventative
CRITICAL PHYSICAL INFRASTRUCTURE PROTECTION
Increased Legislative Powers
Increased collaborations
Legal reforms
Adaptive Learning
Openness to learn new technology
Learning from International Examples of Best Practices

Figure 5-6 Initial Framework /Seed Model for CPI Protection in the UAE

(Author's Diagram)

The above model is developed from the integration of the findings of the literature review as well as the findings of each round of the Delphi process. Factors identified in both the literature review and the data analysis are incorporated in the initial framework/seed model and which constitute the key factors/approaches believed to be effective in the CPI protection from both expert consensus and the literature.

The model for CPI protection in the UAE could be implemented within an organisational setting such as a law enforcement agency based on the five key inputs identified. In terms of strategic organisation training a thorough skills gap assessment at individual and organisational level could be conducted that reveals areas for improvement in terms of digital skills and knowledge, balance, type and relevance of training, futuristic training and specialisation. As part of the skills gap analysis at individual level the organisation may need to determine all the digital skills relevant to different job roles. Learning from international best practice could link to benchmarking exercises to ascertain and compare the current state of digital skills and competency training with other organisations internationally. The emphasis can be placed not just on performance assessment but also on improvement and innovation. Therefore implementation of this aspect should include promotion of opportunities for collaboration and knowledge exchange in relation to best practices. Implementation could also encompass undertaking analysis of the legal structure for cybersecurity that identifies problems of enforcement and legal obstructions which expose the UAE's critical infrastructure to harm. Analysis could also focus on legal reform that enhances the capacity of the state to identify, prosecute and punish cybercriminals acting against the public interest. Implementation of resilience could rest on measures that promote cyber readiness and preparedness involving a process of continuous application of security monitoring and measures and ensuring a rapid or even pre-emptive response to security threats. Readiness and preparedness would help in avoiding large losses or outages. Finally application of a socio-technical hybrid system could comprise assessment of socio-technical gaps within organisational information and cybersecurity practices and implementation of remedies and that bring about a shared emphasis on both the social and technical factors impacting security practices. This could involve development of a specific socio-technical systems cybersecurity framework that may be applied to any new or existing information and cybersecurity solutions in the organisation.

5.6 Conclusion

This chapter presented the qualitative and quantitative results gather across the different phases of the Delphi process. Qualitative data generated from the open-ended questionnaire from Phase 1 was thematically analysed identifying key themes emerging from the initial phase of group model building. The second section of this chapter presented the results from a semi-structure questionnaire and the quantitative ranking of the key factors identified in Phase 1. The results from these two phases contributed knowledge on the key factors and issues relating to the design and implementation of a digital competency framework for law enforcement for enhancing cybersecurity of CPI. The initial model of these factors emerging from the focus group in Delphi Phase 4 is presented. This chapter also presented the results from Phase 3 of the Delphi process which focused on defining and prioritisation of cybersecurity digital competencies based on Cybersecurity Educational Framework. This identified and prioritised the cybersecurity functions, specialty areas and roles in terms of importance and relevance as digital competencies for law enforcement and CIP. In the next chapter these findings are discussed in relation to the literature.

Chapter 6 Discussion of Findings

6.1 Introduction

Until this study the notion of a digital competency framework for cybersecurity that is specific to the context of law enforcement in protecting critical infrastructure has yet to be addressed in either theory or practice. This study has highlighted the threat of cybercrime to the security of critical infrastructures and the stability and security of society and the role of law enforcement. The digitisation of CPI and the evolving and increasing online digital threat and attacks underlines the significance of digital competencies in the area of law enforcement. Yet the capacity of law enforcement to mount effective preventative and reactive measures responses is severely undermined globally and in the UAE by major skills gaps and a lack of digital competencies. The goal of this study is to develop a digital competency framework for UAE law enforcement agencies to combat cyber security threats facing the UAE's critical physical infrastructure. To fulfil this aim the research is directed towards three research objectives:

1. To investigate the key function and roles of law enforcement in cyber security for CPI

2. To define and validate the key dimensions and elements of digital competency for cyber security law enforcement to perform its role in protecting CPI

3. To develop a framework to guide policy and the development of law enforcement in the UAE and enhance its capability to perform its role effectively in a digital environment.

In relation to these objectives, this chapter provides a discussion of the findings arising from a Delphi process that engaged a sample of 24 experts to develop a digital competency framework. Firstly, the design and implementation context and factors of digital competency in the context of law enforcement and CPI are discussed. The second part of this discussion focuses on the prioritisation of specific digital competency categories, specialty areas, work roles, knowledge, skills, abilities and tasks that are necessary for law enforcement in this field.

6.2 Design and Implementation Factors

Phase 1 and phase 2 of the Delphi generated both qualitative and quantitative data on the design and implementation context of the digital competency framework for law enforcement. There was a convergence by the expert panel on themes that were viewed as critical for the design and effective implementation of digital competency framework.

These findings provided context-specific identification and understanding of critical design strategies and processes for implementing a digital competency framework. Framing of digital competency development was an overarching foundational theme where experts underlined the significance of a balanced approach to ensure a diverse range of competencies could be developed to address the broad range of digital competency training and topics. Experts perceived a risk of specialisation in one area or specific divisions of law enforcement. A comprehensive programme that addresses a range of domains across all areas and levels of law enforcement that was in turn relevant to roles and operations was identified as a key success factor. Failure to achieve an optimal balance means that either digital competencies are highly generalised and lack focus, depth or relevance to certain roles; or on the other hand are highly specialised and concentrated in a small number of personnel and divisions. The literature has shown that specialisation has been one of the key issues affecting the ability of law enforcement to respond to cybercrime. Cybersecurity capabilities are concentrated in specialist teams, while a large percentage of law enforcement personnel lack basic digital competencies to counter the cyber threat. This is consistent with the challenges described by Willits and Nowacki (2016) and Williams et al., (2013) and the tensions between specialists and non-specialist cybercrime divisions and the lack of recognition of digital and cybersecurity competencies as an organisation-wide requirement.

Emphasis was placed on a diverse range of development mechanisms and modes of training to address different learning styles and work contexts to maximise access to development programmes. This requirement has been underlined by several studies that identified gaps in law enforcement development programmes and point to the need for diverse and flexible learning approaches and the prioritisation of digital competency (ENISA, 2019; Broadhead, 2018; Kraemer-Mbula et al., 2013).

Future proofing of the digital competency was linked to formation of Learning Management System (LMS) and incorporation of emergent learning technologies such as gamification, simulations software or virtual or augmented reality. Experts viewed LMS as critical for systematically assessing and monitoring digital competencies and promoting continuous professional development linked to new technological opportunities for learning. The significance of formal and structured learning management systems has been underlined as critical to development planning and development of skills necessary for law enforcement to maintain pace with new technologies and evolving threats (Nowacki, and Willits, 2019; Europol, 2018; Schreuders et al., 2018). Validation of development outcomes through certification of competencies for law enforcement across different areas of cybersecurity was identified as a critical factor.

Digital competency was discussed in relation to the approaches and focus of overall capability. There was convergence on the view that law enforcement capabilities should address reactive, proactive and preventative competencies. Reactive competencies were associated with law enforcement capacity to respond effectively to cyber incidents on CPI with implications for reporting and initiating investigation, digital evidence gathering and forensic analysis. Proactive measures were associated with digital competencies that for law enforcement enabled high level of situational awareness, profiling, monitoring and identification of trends and threats, intelligence gathering, modelling and profiling and inter-organisational co-operation and sharing of information systems across boundaries. Preventative measures were associated with the capacity of law enforcement to support organisations managing CPI in enhancing cybersecurity. Digital competencies are necessary in this area for accessing information systems, monitoring threats, vulnerabilities and disseminating alerts, briefings and guidance to the sector. The literature underscores the role of proactive and preventative strategies to strengthen the resilience of CPI and enhance readiness (Au-Yong et al., 2014; Al-Najjar and Wang, 2001).

A key theme that emerged was the importance of co-ordinated and collaborative effort between agencies and CPI to promote information and knowledge sharing that increased the resilience of CPI. This implied digital competencies for law enforcement to operate in digital space and utilise ICT and advanced technologies to promote intelligence gathering, information exchange and communication between key actors at any stage. This has implications for development of information and knowledge management drive competencies. This is consistent with studies that have underlined cognitive dimensions of digital competency and the ability to assimilate, analyse and share knowledge (Xiong, 2016; Osterman, 2013; Davies, 2011; Van Es and Schafer, 2017; Reedy and Goodfellow., 2012) and to operate inter-organisational and across borders. The latter underlines the digital competencies to access and query databases and sources across different technological and administrative environments (Ala-Mutka, 2011; Ferrari et al., 2012).

These factors were underscored as critical for enhancing the resilience of CPI technically and socially. Cyber-readiness and preparedness was associated with development of digital competencies that enhanced proactive, reactive and preventative approaches to law enforcement. Readiness and response of law enforcement was addressed from a resource perspective underlining the importance of the availability of skills and resources. Emphasis was placed on allocation of human and technical resources to enable law enforcement to enhance digital competencies. Against the significant challenges and serious resource constraints faced by the public and law enforcement accurate assessment of needs and prioritisation of cybersecurity skills was identified as a critical factor to maximise efficiency and effectiveness of law enforcement. This finding is supported by multiple studies that have described organisational, leadership, managerial, and resource constraints that hinder development of cybercrime capabilities (Skogan and Hartnett, 2005; Weisburd and Lum, 2005; Boin and McConnell, 2007).

A further theme was the broader external context identifying social, technical, and legal dimensions of cybersecurity protection of critical infrastructures. Awareness and engagement with different stakeholders was identified as a key factor to support preventative and reactive approaches. Experts emphasised fostering a culture of information sharing and co-ordination that would support strengthening of critical infrastructures and increased awareness of the socio-technical systems particularly cloud. Experts pointed to voluntary initiatives in the industry that allow for higher levels of mapping CPI and sharing of security information and guidance between law enforcement agencies, data providers and critical infrastructure industry. An overarching dimension of this socio-technical system was the legislative and regulatory measures that would allow for data sharing with cloud infrastructure providers and other technology providers to enhance preventative and reactive measures to counter threats. This has implications for legislative framework which as the expert panel in the UAE have found, requires reforms of powers to increase access, intercept, and store data and increased powers to block cybercrime data stored on cloud platforms (IaaS, SaaS, and PaaS). These findings are consistent with the emphasis placed in the literature on safeguarding regulations and regulations to require CIP to implement security measures and regulations to promote information sharing and increase access to data from intermediaries.

This situates cybersecurity of CPI and the role of law enforcement within a complex socio-technical system. The evolving nature of critical infrastructures has resulted in a distributed interconnected network of systems and data across multiple organisations, regional and national boundaries. This has implications for digital competencies of law enforcement in possessing both the technical and legal capabilities to effectively navigate the system. At a preventative level there is requirement to have a level of awareness of the threats to infrastructures and counter-measures that depends on understanding the socio-technical environment in terms of the different stakeholders involved and responsibility for CPI. At a reactive level, law enforcement requires both the capabilities and powers to access this socio-technical environment when responding to cyberattacks to investigate and gather evidence.

6.3 Cybersecurity Competence Categories, Specialty Areas and Work Roles

The third round of the Delphi process involved the completion of Analytical Hierarchy Process (AHP) matrices to determine the relative importance for the protection of critical infrastructure by law enforcement agencies of cybersecurity competence categories, specialty areas and work roles presented in the NICE framework. The AHP analysis provided a systematic and numerical decision technique that supported identification and prioritisation of the competency categories and specialty areas and work roles associated with each category. The weightings from the AHP analysis were aggregated to produce results based on the average scores. The following sections discuss the results of these evaluations in the context of the literature and the implications for police training and development.

6.3.1 Cybersecurity Competence Categories

The findings resulted in the ranking of the seven categories of cybersecurity competencies in the NICE framework in terms of their importance for critical infrastructure protection by law enforcement. Four categories of Investigate, Analyse, Collect and Operate and Protect and Defend were assigned higher importance by experts. The AHP priority weightings for these four categories ranged considerably between the highest and lowest weightings suggesting that there were clear priorities for categories of competencies and unambiguously establishing their relative importance for law enforcement.

6.3.1.1 Investigate

Investigate was the most highly ranked competency category overall with a high prioritisation over the other three top ranked categories. Investigate refers to the investigation of cybersecurity events or crimes related to IT systems, networks and digital evidence (NICE, 2021). This result emphasises the investigation function of police in relation to critical infrastructure protection over and above its three other functions of enforcing the law, prevention, and detection (UN, 2011). This could suggest an expert view that the role of law enforcement in protecting critical infrastructure is primarily reactive with functions and competencies focused on response following the occurrence of a cybercrime. On the other hand proactive investigations of cybercrime involve effective targeting, profiling, criminal intelligence, surveillance and analysis of data (Cross, 2019; Carrier and Spafford, 2003). The NICE framework itself appears to encapsulate a broader view of investigation competencies by incorporating prevention and detection competencies such as surveillance and evidence gathering for network vulnerability mitigation in the Investigation category.

The literature shows this has implications for training and development in the process of digital forensics and the identification, preservation, collection, examination, and analysis of digital evidence (Kent et al., 2006; Palmer, 2001). The development of competencies would focus on enabling evidence to be collected through the recording of physical and digital crime scenes using standardised procedures and techniques and approved methodologies, software and hardware (UNODC, 2019). Enacting covert surveillance requires a unique set of competencies to monitor and analyse patterns of activity across systems and may involve interception of digital communications, analysis of video records, use of online information, monitoring discussion groups, or nurturing informants online (Cross, 2019; Carrier and Spafford, 2003).

6.3.1.2 Analyse

Results showed that Analyse ranked as the next highest competency category with a weighting that was balanced between the top-ranked category and the next two categories. Analyse is defined in the NICE framework as the performance of highly specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence (NICE, 2021). Key specialty areas in this category include threat analysis and all-source analysis which produce findings to help initialise or support law enforcement and counterintelligence investigations or activities (NICE, 2021). The high rating given to this competency category might suggest that experts consider that proactive competencies in terms of monitoring and detection are important for law enforcement to protect critical infrastructure. The literature shows that monitoring and analysing cybercrime trends as well as alert and advise on cybercrime risks and crimes is a major role for law enforcement in cybersecurity (Pedley et al., 2018). The finding aligns with approaches that prioritise the development of analytical competence which could be used to assess vulnerabilities and conduct risk analysis for remediation and mitigation for infrastructure protection over a unique set of intelligence collection methods or unique integrated intelligence functions (Radvanovsky and McDougal, 2010). Therefore adopting this strategy would have implications for the design and development of digital competence training that prioritises analytical competences over intelligence collection and sharing. The consequences for training and development are shown in the literature, which points to competencies for the Analyse category such as monitoring and identifying cyber threats and cyber-crimes and analysis and profiling of cyber-crime activity.

6.3.1.3 Collect and Operate

The findings showed that Collect and Operate was ranked third highest in importance for cybersecurity competence categories. This category refers to the collection of cybersecurity information that may be used to develop intelligence as well as to provide specialised denial and deception operations (NICE, 2021). Collecting information involves knowledge and deployment of appropriate collection strategies following established priorities and the gathering of evidence on possible or real-time threats from criminal sources (NICE, 2021). While the Collect and Operate function is separate to that of Investigation in the NICE framework, collection is frequently cited as a specific part of the investigation and digital forensics process in other cybersecurity frameworks (UNODC, 2019; Martini and Choo, 2012; Kent et al., 2006; Palmer, 2001). The literature shows that there are implications for the development of competencies in information and intelligence gathering (Radvanovsky and McDougal, 2010). Yeboah-Boateng and Akwa-Bonsu (2018) propose that cyber-security intelligence gathering is closely linked to knowledge management and knowledge sharing to prevent, detect and respond to threats. This points to the potential need to develop competencies in knowledge sharing among appropriate agencies and units. Core competencies and skills for data collection and examination are identified in the Cyber Intelligence Tradecraft Project (CITP) as involving research methodologies and applications and quantitative and qualitative collection strategies as well as competencies in collection management and open source data (Chabinsky. 2010). Again there is recognition of the requirement for abilities in knowledge management for planning and organising information collection and for applying tools to gather and support complex data and information analysis (Chabinsky. 2010).

6.3.1.4 Protect and Defend

The results show that the competence category of Protect and Defend was ranked closely behind Collect and Operate suggesting that these two categories were considered more or less equal in importance. These competencies are related to the identification, analysis and mitigation of threats to IT systems and/or networks (NICE, 2021). Protection relates to competencies such as cyber defense analysis and vulnerability assessment and management while Defend relates to competencies of immediate incident response to cybersecurity breaches and crises (NICE, 2021). Some literature suggests that important competencies for law enforcement agents responding to a breach in CPI cybersecurity include contingency planning and situational information assessment (Boin and McConnell, 2007). Literature also points to a range of non-technical competencies such as public–private collaboration with owners, and promoting the adaptive behaviour of citizens to foster greater resilience, including the abilities to engage in joint preparation, joint training, continuity planning, and working with communities and private owners (Boin and McConnell, 2007).

6.3.1.5 Oversee and Govern, Securely Provision and Operate and Maintain

The three remaining competency categories of Oversee and Govern, Securely Provision and Operate and Maintain were considered the least important cybersecurity competence categories for law enforcement protection of CPI. This was reflected in their low weightings which were much reduced compared to the four top criteria. This result is logical as these competency categories are associated either with higher leadership levels of the law enforcement agency rather than the front-line police officer or with the internal situation of the organisation under attack. Oversee and Govern is related to the provision of leadership, management, development and advocacy so that the organisation may effectively undertake cybersecurity work (NICE, 2021). This aligns with literature which underlines the essential importance of police leadership to respond effectively to a cybersecurity crisis and manage complex cybercrime enquiries (Bednar et al., 2008; Boin and McConnell, 2007), to develop effective cybercrime solutions (Willits and Nowacki, 2016) and to collaborate with external entities to solve cybersecurity problems (Bednar et al., 2008). This places emphasis on several leadership and management competencies such as crisis management, relationship management, collaboration skills, and cognitive competencies to foster goal achievement among teams undertaking task-related problems and developmental leadership (Santos et al., 2015; Rafferty and Griffin, 2006; Boin and McConnell, 2007; Dutta and McCrohan, 2002).

Securely Provision and Operate and Maintain competence categories have similar low weightings showing that both have lesser importance for law enforcement. Securely Provision encompasses the conceptualisation, design, procurement and/or building of secure IT systems, while Operate and Maintain is about providing the support, administration and maintenance necessary to ensure effective and efficient performance and security in IT systems (NICE, 2021). Neither of these competence categories fall within the remit of law enforcement for protecting critical infrastructure, as the scope lies predominantly with the critical infrastructure organisation itself.

6.3.2 Cybersecurity Specialty Areas and Work Roles

A second objective of this study is to identify key domains and elements of digital competency for cyber security critical for law enforcement to perform its role in protecting CPI. This was achieved by gathering the perspectives of police practitioners to identify how they prioritise and weight the specialty areas and work roles associated with each of the competence categories in the NICE framework for cybersecurity.

6.3.2.1 Overall Rankings

The findings indicate the overall ranking of specialty areas and work roles across all the competence categories based on calculation of the absolute weightings for each of these elements derived from their relative weightings and weighting of their competence category. The specialty areas and work roles that have the highest importance arise from the Investigate category. Cyber Investigation and Cyber Investigator received the highest overall weightings for specialty areas and work roles while Digital Forensics and Law Enforcement/Counterintelligence Forensics Analyst ranking second in priority. This is not an unsurprising result given the law enforcement context of this research which emphasises an investigative, reactive approach to attacks on critical physical infrastructure. The absolute priorities for specialty areas and work roles show that the Analyse category has some of the most prioritised elements. In particular All-Source Analysis and All-Source Analyst are the third most prioritised across all categories while Threat Analysis is the fifth most prioritised Specialty Area and Threat/Warning Analyst the seventh most prioritised work role. From the Collect and Operate category Cyber Operations was the fourth highest specialty area and Cyber Operator the fourth highest work role across all of the categories. These results are consistent with those for the Competency Categories results, as all of these specialty areas are associated with the top 4 most prioritised categories. The findings underline the importance of consideration of specialty areas and work roles within the Investigate, Analyse, Collect & Operate and Protect & Defend categories and provide a guide in terms of the most important knowledge, skills and abilities that should be incorporated within training and development for law enforcement to protect critical physical infrastructure.

6.3.2.2 Investigate Specialty Areas and Work Roles

In terms of the relative importance of the two specialty areas associated with the Investigate competency category findings show that Cyber Investigation was prioritised more highly and with a moderate margin over Digital Forensics. This result is not surprising as Cyber Investigation is a broader area than Digital Forensics that includes techniques, procedures and tactics for a wide variety of investigative processes and tools including non-digital competencies such as interview and interrogation techniques as well as digital skills including surveillance and intelligence gathering. Digital Forensics on the other hand focuses predominantly on the collection, processing, preservation, analysis, and presentation of digital evidence to support law enforcement investigations or network vulnerability mitigation. This result aligns with the literature which shows that digital forensics is a phase of the overall cyber investigation which is initiated in an identification phase focused on recognising and characterising cybercrime incidents through processes such as monitoring and analysis or profile detection (UNODC, 2019; Carrier and Spafford, 2003). Shavers and Bair (2016) suggest that the role of cybercrime investigator is a broad one that still involves traditional investigative methods and good skills in researching information and following leads.

Three work roles are associated with the Investigate competence category with findings showing that each work role is significantly prioritised over the other. Cybercrime Investigator achieved the highest priority followed by Law Enforcement/Counterintelligence Forensics Analyst and Cyber Defense Forensics Analyst. This is consistent with the results for specialty areas in prioritising broader investigative roles over more specific. A defensive investigative role is viewed to be least important for law enforcement to protect critical infrastructure.

In the NICE framework every work role is associated with specific technical and non-technical knowledge, skills and abilities (KSAs) required to carry out the role effectively. These have implications for the development of law enforcement competencies for cybersecurity protection of critical infrastructure. Some of these KSAs are overlapping and applied across a number of different roles. For the cybercrime investigator role KSAs are a broad set of predominantly technical competencies focused on understanding of security threats, evidence-gathering techniques and evidence preservation (NICE, 2021). Of the 25 knowledge items specified cyber investigators need to know about aspects such as the dark web, intrusion detection, and cyber threats and vulnerabilities (NICE, 2021). Skills relate to preserving and maintaining the integrity of digital evidence. The Law Enforcement/Counterintelligence Forensics Analyst work role is similarly technically focused with a more concentrated set of KSAs. These include decryption skills and investigative abilities across a wide range of operating system platforms. Knowledge of digital forensic processes and data backup and recovery are included among the 42 knowledge items for this role. Skills include forensic data extraction in different digital environments. The Cyber Defense Forensics Analyst role includes many overlapping

KSAs but also includes items such as skill in malware analysis and carrying out bit-level analysis.

6.3.2.3 Analyse Specialty Areas and Work Roles

The Analyse competency category is associated with five specialty areas of which the relative findings show three were most prioritised: All-Source Analysis, Threat Analysis and Exploitation Analysis. While these received the highest weightings there was a moderate margin of difference between each of them. The remaining two areas of Language Analysis and Targets were considered to be of much lower priority reflected in their weightings. The results for this category appear to reflect a determination among the experts that the broadest specialty areas have higher priority than narrower and more specific areas. All-Source Analysis was accorded the highest priority and involves the analysis of threat information from multiple sources, disciplines, and agencies across the intelligence community and its synthesis in context to generate insights about the possible implications (NICE, 2021). The emphasis placed on this area is consistent with cybercrime practices in Europol that ascribe significant importance to collecting and analysing information from a broad array of public, private and open sources (Europol, 2021). Threat Analysis, the next prioritised specialty area, is more limited in scope focusing on identifying and assessing the capacities and conduct of cyber criminals and producing findings to facilitate commencement and operation of police investigations. Some literature supports the emphasis placed on this specialty identifying it as a key stage in the threat intelligence lifecycle that allows information to be converted into intelligence that can inform decision-making (Cascavilla et al., 2021). Exploitation Analysis, the third most prioritised area, is concerned only with the analysis of data gathered to detect any weaknesses and the possibilities for exploitation (NICE, 2021). The lowest prioritised areas of Language Analysis and Targets involve the application of the individual’s current expertise and knowledge in terms of language, cultural, and technical knowledge to support information collection, analysis, and the development of targets.

In terms of the seven work roles associated with the Analyse category the results showed that rankings reflected the same pattern of broad to more narrow roles. All-

Source Analyst, Threat/Warning Analyst and Exploitation Analyst were the most highly prioritised in that order with moderate differences in weightings between each of them. The remaining four roles were assigned a similar and much lower rating: Multi-Disciplined Language Analyst; Target Network Analyst; Target Developer; and Mission Assessment Specialist. The least prioritised role of Mission Assessment Specialist is linked to the All-Source Analysis specialty area, however focuses on assessing the performance of responses to cyber events. It is likely that experts considered this role to be outside of normal expectations for the functions of a front-line police officer.

For the top three work roles the NICE framework includes a number of overlapping KSAs. These encompass communication skills for conveying complex information, knowledge of computer networking and cyber security methods and protocols, and ability to evaluate information in terms of its validity and reliability (NICE, 2021). The role of All-Source Analyst is associated with 18 abilities, 56 knowledge items, and 18 skills, representing a mix of technical and non-technical KSAs. These include ability to source intelligence data, knowledge of how to analyse network traffic, and skill in utilising different analytic tools and techniques (NICE, 2021). The NICE framework for the Threat/Warning Analyst role identifies a slightly lower number of KSAs that includes the ability to utilise different sources of intelligence, knowledge of cyber attack stages and skill in identifying cyber threats (NICE, 2021). The Exploitation Analyst work role is associated with KSAs such as target analysis abilities, knowledge of attack approaches and methods and skill in analysing traffic and distinguishing network devices.

6.3.2.4 Collect and Operate Specialty Areas and Work Roles

The findings showed that pairwise comparison of the three specialty areas for Collect and Operate showed that there was significant difference in importance between them. Cyber Operations was assigned a significantly higher level of importance than Collection Operations which in turn was prioritised much more highly than Cyber Operational Planning. This result reflects the context for law enforcement in which being able to collect evidence on criminal or foreign intelligence actors to mitigate potential or actual threats (Cyber Operations) may be prioritised more highly than the more general competency of collection of cybersecurity information using appropriate strategies and collection management priorities (Collection Operations) (NICE, 2021). While much of the literature associates the term cyber operations with national offensive and defensive capabilities (Stinissen and Geers, 2015; Lin, 2010) some literature points to the importance of threat-informed cyber operations and the critical role of actionable threat intelligence in cyber defense (Skorupka and Boiney, 2015). Cyber Operational Planning appears to be beyond the scope of most front-line police officers who generally would not get involved in conducting strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations. This would account for the low priority this specialty area is accorded by the experts.

Six work roles were associated with the Collect and Operate category of related to all-source collection, cyber planning, and cyber operations. By far the most prioritised is that of Cyber Operator, aligning with the finding for specialty areas priorities, and the most broad and general role available in terms of the collection of information. A cyber operator is involved in system geolocation in order to locate, track or exploit targets of interest (NICE, 2021). Much lower in priority are managerial roles associated with all-source collection and incorporating priority information requirements into collection management and evaluating collection operations (NICE, 2021). These are more generalised roles that focus on execution, and were preferred over the least prioritised roles planning roles. These roles focus on developing detailed operational plans in collaboration with other planners, and on advancing cooperation across organisational or national borders which experts may have considered were too specialist for a front-line officer.

The Cyber Operator work role is associated with a broad range of predominantly technical KSAs many of which are unique to this job role. This includes monitoring and responding to events and trends, knowledge of current defense software and methodologies, and skill in information extraction (NICE, 2021). For the All-Source Collection managerial roles non-technical abilities are desired that include collaboration abilities, critical thinking skills, and coordination abilities across all levels of the organisation. The planning work roles require a broad and comprehensive range of knowledge, abilities and skills that include many non-technical KSA’s focusing on communication and administration competencies.

6.3.2.5 Protect and Defend Specialty Areas and Work Roles

The relative importance of four specialty areas were compared for the Protect and Defend competence category. Findings showed that two specialty areas of Incident Response followed by Cyber Defense Analysis were most prioritised by a significant margin over the remaining two areas of Vulnerability Assessment and Management and Cyber Defense Infrastructure Support. This finding shows that the ability to respond to cybersecurity crises or urgent situations to mitigate threats to property or people is a highly emphasised competency for law enforcement in the context of critical infrastructure protection. The priority accorded to this area is strongly consistent with the literature which shows that cybersecurity for incident response is studies and discussed in a range of different organisational contexts and industry sectors (e.g. Naseer et al., 2021; Papastergiou et al., 2019; Catota et al., 2018; Steinke et al., 2015). Some literature has focused specifically on incident response for critical infrastructure cybersecurity (Lekota and Coetzee, 2019; Settanni et al., 2017; Jaatun et al., 2009) while research also shows that numerous governments and sectors are addressing incident response to breaches of critical infrastructure cybersecurity through specific agencies, organisations and teams (CISA, 2021; CGCCI, 2021; ENISA, 2021). The weighting accorded to Cyber Defense Analysis also shows that a defensive approach that uses information gathered from diverse sources to detect, evaluate, and inform on events and threats that take place or may happen is also considered important. The low rating given to the specialty area of Cyber Defense Infrastructure Support indicates that testing, deployment, maintenance and review of infrastructure hardware and software is not considered to be a part of the complement of cybersecurity competencies a frontline officer is expected to have.

Four work roles are associated with the Protect and Defend competence category. The priority assigned to these roles follows a similar pattern and weighting as the specialty areas, with Cyber Defense Incident Responder and Cyber Defense Analyst being considered of higher importance than Vulnerability Assessment Analyst and Cyber Defense Infrastructure Support Specialist. The incident response and cyber defense roles are comprised of mainly technical KSAs integrating abilities such as incident response for cloud and intrusion detection abilities, and malware neutralisation skills.

6.3.2.6 Specialty Areas and Work Roles for Oversee and Govern, Securely Provision and Operate and Maintain

The specialty areas and work roles for these three competency categories provide an indication of the reason why these categories were considered of least relevance for the context of law enforcement front-line protection of critical infrastructure. This is because many of the specialty areas and work roles are irrelevant in the law enforcement and front-line context. Oversee and Govern has six speciality areas with leadership and management areas receiving the highest ratings while strategic planning, legal advocacy and training and education were prioritised much less highly. Securely Provision has seven specialty areas of which systems and software competencies were weighted least while risk management received the highest weighting by significant margin over the rest. Finally Operate and Maintain has six specialty areas in which data administration and knowledge management are the only areas to have received significant weightings.

6.4 Summary of Findings and Contribution

The findings of this study provide the basis for a holistic approach to developing key digital competencies within law enforcement for cybersecurity of critical physical infrastructure. As Table 6.1 shows findings identify critical digital competencies, specialty areas and work roles to inform a digital competencies framework for law enforcement in this context. In addition findings point to how this framework can be implemented effectively within law enforcement, identifying critical design and implementation factors for the development of digital competencies for cybersecurity of critical physical infrastructure.

Table 6.1 Summary of Findings and Contribution

Area of Findings	**Finding**	**Unique Contribution**
Design and Implementation Factors	Eight key factors are qualitatively identified for implementing a digital competencies framework for law enforcement for CPI: • Balance, type, & relevance of training • Futuristic training • Mandatory certifications, digital knowledge and skills • Skills development and resources • Proactive, reactive, preventative measures • Socio-technical system • Resilience • Adaptive learning The importance of multiple implementation subfactors is quantitatively identified for each critical factor	Identification of critical implementation factors for effecting a digital competencies framework for law enforcement to protect critical physical infrastructure.
Key Categories of Competence	Identification of four key categories of digital competencies relevant to law enforcement for protecting critical physical infrastructure: • Investigate • Analyse • Collect and Operate • Protect and Defend	Empirical analysis prioritising categories of critical competencies for CPI cybersecurity protection by law enforcement
Specialty Areas of Digital Competence	Findings identified three critical areas of specialty relevant to law enforcement for cybersecurity of critical physical infrastructure: • Cyber Investigation	Empirical analysis prioritising areas of specialty for CPI cybersecurity protection by law enforcement

	• Digital Forensics • All-Source Analysis and the relative importance of multiple specialty areas for each of the categories of digital competence	
Digital Competence Work Roles	Findings identified three key work roles critical to law enforcement for cybersecurity of critical physical infrastructure: • Cyber Investigator • Law Enforcement/Counterintelligence Forensics Analyst • All-Source Analyst and the relative importance of multiple work roles for each of the categories of digital competence	Empirical analysis prioritising the importance of different digital competence work roles for CPI cybersecurity protection by law enforcement

6.5 Conclusion

This chapter presented a discussion of findings generated from a mixed method research process that employed a Delphi method, AHP analysis and group model building process focused on conceptualising a digital competencies framework for law enforcement cybersecurity protection of critical physical infrastructure. Three sources of qualitative and quantitative data were evaluated and discussed in relation to the research goal of this thesis. The findings contributed novel insights into the planning and implementation context for development of digital competency. These results underlined the broader digital competency context which is influenced by the evolving external context that continuously influences the requirements for digital competencies. Evolving critical infrastructures, technologies and cybercrime context underline the need for a dynamic digital competency framework. The regulatory and institutional context similarly has implications for development of digital competency influencing requirements and resourcing. The findings further identify broad dimensions of digital competency and key dimensions of cybersecurity competencies that are critical for law enforcement and protection of CPI. Finally, these findings supported the development of a holistic and dynamic eco-system for development of digital competency in the context of law enforcement and critical infrastructures protection. The next chapter concludes this research, discussing the contribution to knowledge in relation to the research and the theoretical and practical implications and the limitations and future research opportunities emerging from this study.

Chapter 7 Conclusions

7.1 Introduction

An overarching goal of this study was to address how digital competency for law enforcement in enhancing cybersecurity for critical physical infrastructures (CPI) can be conceptualised and implemented. CPI are vital to the social and economic functioning and development of nations.

The evolving technological context and increasingly digitised and interconnected nature of CPI coincides with increasing threat and risk of cybercrimes. Yet this study has underlined the limitation in the capacity of law enforcement around the globe to counter the severe threat posed by cyberattacks in respect of the digital capabilities that are necessary to maintain pace with technologies and respond effectively in a digital environment. In theory and practice, the notion of digital competency in the context of law enforcement and critical infrastructure protection (CIP) has received little attention. This thesis has revealed digital competency as a multifaceted concept informed by multiple disciplines that emphasises different dimensions of competency: internet skills, information and knowledge processing, technology, media, socialisation, communication as well as attitudinal, cognitive and critical thinking competencies. The scope of this research focuses on cybersecurity related digital competencies that are to varying degrees underpinned by broader digital competencies.

In practice the absence of a comprehensive common framework has resulted in a fragmented and concentrated approach to the development of digital capabilities in law enforcement as a whole. This issue is more acute in respect of sector-specific contexts such as CPI. Further, this study identified digital competencies, in regards to knowledge, skills, abilities and attitudes, as an integral dimension for law enforcement that underpinned all aspects of law enforcement functions and roles and ultimately its ability to counter cyberattacks. It underpins its capacity to operate in a digital environment and perform preventative, proactive or reactive functions. Against this context, the research goal is focused on three key objectives:

i) To investigate the key function and roles of law enforcement in cyber security for CPI

ii) To define and validate the key dimensions and elements of digital competency for cyber security law enforcement to perform its role in protecting CPI

iii) To develop a framework to guide policy and the development of law enforcement in the UAE and enhance its capability to perform its role effectively in a digital environment.

7.2 Summary of Key Findings

The findings of this research address comprehensively the concept of digital competency in relation to both the planning and implementation context and the dimensions critical to enhancing law enforcement cybersecurity for protection of CPI. This study conceptualises the development of digital competency as an interplay of multiple interconnected dimensions.

The enhancement of law enforcement cybersecurity is contingent on strategic factors and framing of digital competency development which emerged as an overarching foundational theme. Experts underlined the significance of a balanced approach to ensure a diverse range of competencies could be developed to address the broad range of digital competency training and topics. There is a requirement to define the scope of digital competency development and foster appropriate organisational and learning conditions. The study finds that cybersecurity for CIP requires a holistic socio-technical approach and evaluation of digital competency requirements in line with the different functions and roles of law enforcement. This establishes digital competency as a core organisation-wide multilevel competency with varying levels and types of digital competency. A digital competency framework advanced in this study emphasises multiple planning factors that are critical to establish an effective and efficient implementation context. Balance, type and relevance of training is critical for defining development requirements for different areas of law enforcement and ensuring relevance. A digital competency framework is underpinned by diverse learning mechanisms, technologies and platforms to address learning styles and access to development. Future proofing digital competency is a key factor that is based on a process of feedback loops linked with the external environment in relation to cybercrime development and trends and technological advances.

This study further identified areas of digital competency development to address broad law enforcement functions. Digital competencies can be defined in terms of preventative, reactive and proactive competencies. At another level digital competency can be assessed in respect of organisational, managerial and leadership competencies. Finally, this study evaluated the importance and relevance of specific cybersecurity competencies based on the Cybersecurity Educational Framework. The expert panel assessed through a pairwise comparison process using AHP ranking each of 7 high-level cybersecurity functions, the 33 speciality areas and the 52 work roles in terms of their relevance and significance to law enforcement for the protection of CPI.

This study showed that of the seven categories of cybersecurity, Investigate competencies were the most significant dimension of digital competency for law enforcement composed of two specialty areas of Cyber Investigation and Digital Forensics. Cyber Investigation was ranked the highest specialty by a significantly higher margin than Digital Forensics specialty area. Investigate was associated with ability to investigate cybersecurity incidents or crimes related to information technology (IT) systems, networks and digital evidence. The NICE framework specifies three work roles in relation to Investigate competencies. Cybercrime Investigator was the highest rated by a significant margin, followed by Law Enforcement/Counterintelligence Forensics Analyst. Cyber Defence Forensics Analyst received the lowest rating in terms of relevance and significance.

Analyse competencies was the second most significant dimension of digital competency for law enforcement. This category was associated with competencies related to performance of highly specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. The third highest rated top-level cybersecurity category was Collect & Operate. Collect & Operate competencies were characterised by providing specialised denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. Protect & Defend was ranked the fourth highest top-level cybersecurity function in terms of its relevance and importance to law enforcement and CIP. This function addresses abilities to identify, analyse and mitigate threats to internal IT systems and or networks. Three cybersecurity functions of Oversee & Govern, Securely Provision and Operate & Maintain were ranked as least important or relevant to law enforcement by a significant margin. There was a significant difference in the relative weighting between these three functions and the top four highest rated functions. This finding was supported by qualitative findings from the expert panel converging on the view that these functions were more relevant to cybersecurity personnel at critical infrastructure organisations than for law enforcement.

Quantitative evaluation using AHP for the sub-components of the highest rated cybersecurity functions identified the most relevant and significant speciality areas and work roles. In the NICE framework each speciality area and work role is associated with a specific set of knowledge, skills and abilities (KSA). Investigate category has two specialty areas of Cyber Investigation and Digital Forensics, of which the former attracted the highest priority over the latter. Analyse category is associated with five specialty areas. Digital cybersecurity competencies for All-Source Analysis and Threat Analysis rated highest in priority weightings. Exploitation Analysis was rated third highest in priority and Targets was afforded the lowest priority. In terms of the three work roles associated with the top level Investigate category Cybercrime Investigator and Law Enforcement Counterintelligence Forensics Analyst were prioritised much more highly than Cyber Defense Forensics Analyst. For the Analyse category three were most highly prioritised: All-Source Analyst was by a significant margin the highest rated role; followed by Threat/Warning Analyst and Exploitation Analyst. Target Network Analyst and Mission Assessment Specialist were the least significant roles.

The third highest rated cybersecurity category (Collect and Operate) consisted of three speciality areas. Cyber Operations attracted the highest priority by a significant margin followed then by Collection Operations. Cyber Operational Planning was the least important and relevant by a significant margin. In terms of work roles Collect and Operate category is linked to six work roles. Cyber Operator ranked highest priority over the other five work roles by a significant margin. All Source-Collection Manager and All Source-Collection Requirements Manager ranked second and third. The least important work role was Partner Integration Planner.

Protect and Defend was the fourth highest ranked cybersecurity function. Four specialty areas are associated with the Protect and Defend competencies. Incident Response was the highest rated speciality area by a significant margin and Cyber Defence Analysis was the second highest rated. Vulnerability Assessment and Management and Cyber Defence Infrastructure Support were the least relevant and significant speciality areas compared to the top two highest ranked. In terms of work roles for Protect and Defend the NICE Cybersecurity Educational Framework defines four work roles. Considered the most important Cyber Defence Incident Responder was the highest rated role, followed by Cyber Defence Analyst. Cyber Defence Infrastructure Support Specialist was ranked the least priority by a significant margin.

Finally the analysis indicated the overall ranking of specialty areas and work roles across all seven competence categories based on calculation of the absolute weightings. The specialty areas and work roles with the highest overall importance are associated with the

Investigate category. Cyber Investigation and Cyber Investigator were the highest ranked specialty area and work role of all while Digital Forensics and Law Enforcement Counterintelligence Forensics Analyst ranked second in priority. All-Source Analysis and All-Source Analyst from the Analysis category are the third most prioritised specialty and work role across all the categories with Cyber Operations the fourth highest specialty area and Cyber Operator the fourth highest work role, arising from the Collect & Operate category. The findings underline the importance of consideration of specialty areas and work roles within the Investigate, Analyse, Collect & Operate and Protect & Defend categories and provide a guide in terms of the most important knowledge, skills and abilities that can be incorporated within training and development for law enforcement to protect critical physical infrastructure. In the NICE framework knowledge, skills, and ability competencies as well as relevant tasks are defined under the categories and associated with each work role for that function. For the top 5 most prioritised work roles the framework specifies over 430 digital competencies in terms of knowledge, skills, abilities and tasks (KSATs). The overarching priority given to investigative work roles in this study provides an indication of the most important KSATs for law enforcement in its role to protect the cybersecurity of critical physical infrastructure.

7.3 Theoretical and Practical Implications

7.3.1 Theoretical Implications

This study makes a novel contribution to theory of digital competency conceptualising a context-specific digital competency framework for law enforcement. Firstly, these findings identify and characterise key factors, processes and inputs that underpin effective design and implementation of digital competency development. This conceptualises constituent elements of planning and organisational processes that impact on design and implementation including future proofing, framing, resourcing and feedback processes. In the area of law enforcement this study advances new requirements of digital competency and the different functions of policing. Further, it underlines digital competency as a key determinant for enhancing cybersecurity and law enforcement response to cyberthreats and protection of CPI. This study further makes a methodological contribution to theory in the application of AHP to digital competency in law enforcement. This establishes a foundation for exploration of this method in future studies and provides insights into empirical techniques to define digital competency requirements. Another major contribution of this study is the identification of key categories of competences and speciality areas of digital competency of cybersecurity necessary for law enforcement to effectively protect CPI. Under each of the identified dimensions the study identifies key knowledge, skills and abilities (KSA) in the area of law enforcement for enhancing security of CPI.

7.3.2 Practical Implications

Cybercrime and cybersecurity threats represent an evolving context that has implications for the development of digital competencies for law enforcement to maintain pace with such developments. The findings from this study give rise to a number of implications for practice. Firstly, the findings place emphasis on fostering appropriate organisational and learning environment that promotes the development of digital competencies. Practitioners should at a planning level define the scope of digital competency requirements across all the roles. A key factor is balancing between general or common digital competencies and specialised digital competencies. This has implications for developing digital competency requirements for different divisions, teams and roles. This framework provides a comprehensive tool that prioritises the key categories, speciality areas and associated KSAs. Practitioners need to conduct a review and evaluate the relevance of these competencies for specific contexts. Further, the evolving cybercrime context and significance of future proofing further posits digital competency development as a dynamic process. This critically depends on a continuous monitoring and evaluation of the requirements to ensure that digital competencies and the cybersecurity capabilities of law enforcement are responsive to emergent technologies, methods and threats. From a resource perspective, there are implications for the formation of platforms and environment that allows for flexible and diverse learning and development including systematic processes for development planning and monitoring.

7.4 Research Novelty

This study makes novel contributions to knowledge in a number of different ways. Firstly this research is novel in terms of the methodology and is the first in this field to employ a Delphi method to systematically develop a framework of law enforcement digital competences for the protection of critical physical infrastructure. This approach allowed for structuring of group mutual communications over several phases to facilitate an iterative and inclusive process of identification, development and validation of a commonly agreed framework for critical physical infrastructure. There is further novelty in the inclusion of an objective and systematic AHP process within the Delphi implementation and its application to empirically determine the importance of specific digital competencies for protecting critical physical infrastructure by law enforcement.

Secondly this research is novel in terms of the research sample and inclusion of an extensive set of 24 experts and practitioners from key areas in this field. The sample was specifically selected to ensure that data was collected from a diverse range of perspectives from different law enforcement organisations and from different roles and different levels of the organisation. This supported the goal to provide a holistic and inclusive account of digital competencies for critical infrastructure protection that could inform a comprehensive framework for law enforcement. Experts were drawn from all seven Emirates and from a cross-section of policing agencies at federal and local levels that have key responsibilities for cybersecurity and critical infrastructure protection.

A unique contribution is also to be found in the findings of this study that is the only research to investigate digital competencies in relation to law enforcement. While some literature has explored digital competencies for cybersecurity (Cybok.org, 2020; JCNSS, 2018; Libicki, 2007), the focus of previous research has not been on law enforcement. This research identifies and prioritises categories of digital competencies and associated specialties and work roles critical for law enforcement to perform its role in protecting critical physical infrastructure. In addition this research is the only study to have applied the NICE framework and evaluated that framework in the context of law enforcement digital competencies.

The originality of this research further extends to the focus on critical physical infrastructure and the relevance of digital competencies for the role of law enforcement in protecting them. Empirical analysis presented in this research identifies and prioritises the specific digital competencies, speciality areas and work roles for law enforcement that are significant for protection of critical physical infrastructure. The resulting framework addresses a knowledge gap in understanding and mapping digital competencies that are required for different law enforcement roles in terms of cybersecurity of CPI. This uniquely points to a comprehensive reference of the set of knowledge, skills, and abilities necessary for law enforcement that defines structured pathways for understanding and developing them.

A novel contribution to both theory and practice is made by expanding knowledge on critical infrastructure protection and digital competencies in law enforcement. At a theoretical level this research contributes a novel digital competency framework for cybersecurity skills specific to law enforcement protection of CPI. A holistic and practical framework is applied that integrates the theories of cybercrime linked to CPI protection. The proposed framework takes into consideration organisational, leadership, managerial, and resource driven digital competences. Moreover a unique contribution emerges in terms of identification of key implementation factors for a digital competencies framework for law enforcement in the context of cybersecurity for CPI. This helps to address the planning and implementation context by identifying multiple planning factors that are critical to establish an effective and efficient design and implementation for a digital competency framework.

Finally this research is novel in extending understanding in the context of an Arab and developing country, and specifically in the context of the UAE. Despite the significance of developing digital competences of enforcement agencies, there is limited analysis or empirical evidence in this area within the UAE context. While traditionally UAE law enforcement has focused on preventing failures in CPI caused by accidents or natural disasters a rapid and widespread increase in digitisation underlines an urgent need for additional research in safeguarding CPI within UAE against growing threats of cyberattacks. This study is unique in addressing the need to identify the organisational, technical and development interventions required by UAE law enforcement to enhance cyber security.

7.5 Limitations

There are a number of limitations that should be acknowledged in respect of the methodology and findings. While the findings were based on a large expert sample (N=24) with diverse and extensive experts, the study employed a single case study design which as a result places emphasis on a highly contextual setting. The sample of experts in the Delphi panel are embedded in the UAE and therefore their perspectives and expertise are indicative of this setting.

The findings relating to the implementation context reflecting organisational and learning factors are viewed relevant to the specific case of the UAE and law enforcement in the UAE. Further, the empirically based prioritisation and comparison of digital competencies is influenced by this context. In respect of the Delphi method, each of the phases of the Delphi was limited to 2 rounds to provide initial responses and a second round to review and provide revisions or additional insights. Due to COVID face-face group model modelling was restricted to online email and video-conferencing.

Thirdly, the evaluation of the cybersecurity skills and the associated digital competencies was based on the Cybersecurity Educational Framework by the National Initiative Cybersecurity Education (NICE). The NICE is the most comprehensive cybersecurity skills and education framework consisting of 7 top level cybersecurity functions; 33 speciality areas reflecting distinct areas of cybersecurity; 52 work roles and more than 1,000 specific knowledge, skills, and abilities (KSAs) that are necessary for these work roles. Due to the constraint in conducting an Analytical Hierarchy Process (AHP) for the entire framework, the study limited the AHP cybersecurity functions, speciality areas and work roles. The KSAs associated with these components were not assessed in terms of their relative importance. Further, the prioritisation of these dimensions was focused on the relevance to law enforcement in the area of cybersecurity for CPI. The study findings do not classify the competencies between basic, intermediate or advanced level competencies. Further research may classify, these competencies in relation to those relevant for all law enforcement personnel, competencies for all law enforcement cybersecurity roles, and competencies for specific law enforcement work roles. This scope of this study is limited to cybersecurity and CIP related digital competencies and in doing so excludes other dimensions of digital competency such as information, media, technology, cognitive or attitudinal related competencies, which underpin or support cybersecurity competencies.

7.6 Future Research

It is important to validate this framework that has been developed as the contribution of this thesis. The design and implementation factors should be evaluated. This study underlined the requirement for a comprehensive view of digital competency beyond a specialist perspective. However, further research is required to define and map digital competencies to specific functions of law enforcement and the roles of law enforcement that would promote a precise alignment of digital competencies that address cybersecurity for CPI. Generic digital competencies should be defined in relation to those common to all law enforcement in the area of cybersecurity CPI. At another level further research can explore mapping of digital competencies to identify sets of KSAs that are relevant to specific roles.

References

Adeyemon, E. (2009). Integrating digital literacies into outreach services for underserved youth populations. *The reference librarian*, 50(1), pp.85-98.

AGIMO, (2011). *Cloud computing strategic direction paper: opportunities and applicability for use by the Australian government*. Canberra: Commonwealth of Australia.

Akkermans, H. A., Bogerd, P., Yucesan, E., & van Wassenhove, L. N. (2003). The impact of ERP on supply chain management: Exploratory findings from a European Delphi study. *European Journal of Operational Research*, 146(2), 284-301.

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, 4(1), 290-301.

Ala-Mutka, K. (2011). Mapping digital competence: Towards a conceptual understanding. *Sevilla: Institute for Prospective Technological Studies*, 7-60.

Al-Najjar, B., & Wang, W. (2001). A conceptual model for fault detection and decision making for rolling element bearings in paper mills. *Journal of Quality in Maintenance Engineering*, 7,192–206.

Alneaimi, A. (2015). A framework for effectiveness of cyber security defences, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 4(1), 290-301.

Al-shihri, F.S. (2016). Impacts of large-scale residential projects on urban sustainability in Dammam Metropolitan Area, Saudi Arabia. *Habitat International*, 56, 201-211.

Ananiadou, K., & Claro, M. (2009). 21st century skills and competences for new millennium learners in OECD countries. *OECD Education Working Papers*, No. 41. OECD Publishing (NJ1).

Andersen, D. F., & Richardson, G. P. (1997). Scripts for group model building. *System Dynamics Review: The Journal of the System Dynamics Society*, 13(2), 107-129.

Anderson, A. R., & Warren, L. (2011). The entrepreneur as hero and jester: Enacting the entrepreneurial discourse. *International Small Business Journal*, 29(6), 589-609.

Annetta, L. A., Cheng, M. T., & Holmes, S. (2010). Assessing twenty-first century skills through a teacher created video game for high school biology students. *Research in Science & Technological Education*, 28(2), 101-114.

Asaba, S., & Lieberman, M. B. (2008). Business imitation. In *21st Century Management: A Reference Handbook*. London: Sage.

Atak, M., & Ertugut, R. (2010). An empirical analysis on the relation between learning organization and organizational commitment. *Procedia Social and Behavioural Sciences*, 2, 3472-3476

Au-Yong, C.P., Ali, A.S., & Ahmad, F. (2014). Preventive maintenance characteristics towards optimal maintenance performance: A case study of office buildings. *World Journal of Engineering and Technology*, 2, 1-6.

Barnett, B. G. (1995). Developing reflection and expertise: can mentors make the difference?. *Journal of Educational Administration*. 33(5), 45-59.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. *Digital Investigation*.

Bass, B. (1985). *Leadership and performance beyond expectations*. New York: Free Press.

Bate, L. (2017, May 17). *The cyber workforce gap: A national security liability?* https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/

Battistoni, R., Di Pietro, R., & Lombardi, F. (2016). CURE—Towards enforcing a reliable timeline for cloud forensics: Model, architecture, and experiments. *Computer Communications*, 91–92, 29–43.

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel (Eds.)*, Digital literacies*, 17- 32. New York, NY: Peter Lang.

Bednar, P.M., Katos, V., & Hennell, C. (2008). Cyber-crime investigations: Complex collaborative decision making. *Third International Annual Workshop on Digital Forensics and Incident Analysis*, Malaga, 2008, 3-11.

Belmont Report (1979*). Ethical principles and guidelines for the protection of human subjects of research*. Washington D.C.: US Gov., Department of Health & Human Services.

Berkow, J. (2011, June 24). Canadian 'lawful access' laws come at too high a price, critics argue. *Financial Post*, https://financialpost.com/technology/canadian-lawful-access-laws-come-at-too-high-a-price-critics-argue

Birk, D., & Wegener, C. (2011). Technical issues of forensic investigations in cloud computing environments. In: *6th International workshop on systematic approaches to digital forensic engineering–IEEE/SADFE 2011*, Oakland, CA, USA, 1–10.

Boe, O., & Holth, T. (2015). The relationship between developmental leadership, the results of leadership and personality factors. *Procedia Economics and Finance*, 26, 849-858.

Bogdanoski, M., Trajchevski, N., Bogatinov, D., Serafimova, N., & Stevanoski, G. (2019). *European network of Cyber-security centers and competence Hub for Innovation and Operations (ECHO)-Research and Inovation Action*. https://eprints.ugd.edu.mk/28316/

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of contingencies and crisis management*, 15(1), 50-59.

Bolden, R., & Gosling, J. (2006). Leadership competencies: time to change the tune?. *Leadership*, 2(2), 147-163.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: an international journal of police strategies & management.*

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Brenner, S. W. (2007). Private-public sector cooperation in combating cybercrime: In search of a model. *J. Int'l Com. L. & Tech.*, 2, 58.

Brenner, S.W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, 46(4), 189-206.

Brewer, J., & Hunter, A. (1989). *Multimethod research: A synthesis of style*. Newbury Park, CA: Sage

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review,* 34(6), 1180-1196.

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces*, 36(6), 530-544.

Bryman, A., & Bell, E. (2007). *Business research methods*. 2nd ed. Oxford: Oxford University Press.

Bryson, J. M. (2018). *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement.* London: John Wiley & Sons.

Bryson, J. M., & Finn, C. B. (1995). Creating the future together: Developing and using shared strategy maps. In A. Halachmi and G. Bopuckaert (Eds.). *The enduring challenges of public management,* 247-280. San Francisco, CA: Jossey-Bass.

Burrell, G., & Morgan, G. (2017). *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life*. London: Routledge.

Calam, M. (2017). *Policing–a vision for 2025.* https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/Policing%20a%20vision%20for%202025/Policing-A-vision-for-2025.pdf

Campbell, B. (1990). What is literacy? Acquiring and using literacy skills. *Australasian Public Libraries and Information Services,* 3(3), 149-152.

Campion, M. A., Fink, A. A., Ruggeberg, B. J., Carr, L., Phillips, G. M., & Odman, R. B. (2011). Doing competencies well: Best practices in competency modeling. *Personnel psychology,* 64(1), 225-262.

Carrier, Brian D. and Eugene H. Spafford. (2003). *Getting physical with the digital investigation process.* International Journal of Digital Evidence, Vol. 2(2), p. 6.

Carson, D., Gilmore, A., Perry, C. and Gronhaug, K., 2001. Focus group interviewing. Qualitative marketing research. Thousand Oaks, CA: Sage Publications.

Cascavilla, G., Tamburri, D.A. and Van Den Heuvel, W.J., 2021. Cybercrime Threat Intelligence: a Systematic Multi-Vocal Literature Review. *Computers & Security,* p.102258.

Catota, F.E., Morgan, M.G. and Sicker, D.C., 2018. Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity, 4*(1), p.tyy002.

Cavelty, M.D., Mauer, V., and Krishna-Hensel, S.F. (2016). *Power and security in the information age: Investigating the role of the state in cyberspace.* London: Routledge.

CGCCI (2021). *Coordination group for cybersecurity and critical infrastructure.* https://www.energy-community.org/aboutus/institutions/CyberCG.html

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *J. Nat'l Sec. L. & Pol'y,* 4, 27.

Chang, S,E., & Ho, B.C. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106 (3), 345-36.

Check, J., & Schutt, R.K. (2012). *Survey research. Research methods in education*. London: Routledge.

Cheetham, G., & Chivers, G. E. (2005). *Professions, competence and informal learning.* Edward Elgar Publishing.

Choo, K.K.R. (2010). Cloud computing: Challenges and future directions. *Trends and Issues in Crime and Criminal justice,* 400, 1-6.

CISA (2021, March 15). *Cyber incident response*. https://www.cisa.gov/cyber-incident-response

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C., & Trevorrow, P. (2018). Police cybercrime training: Perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice,* 12(4), 1-19.

College of Policing (2018, September 13). *Competency and values framework for policing: Overview of framework* https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2017/09/Competency-and-Values-Framework-for-Policing_4.11.16.pdf

Collis, J., & Hussey, R. (2003). *Business Research: A practical Guide for Undergraduate and Postgraduate Students*. (2nd Ed). Hampshire: Palgrave Macmillan Ltd.

Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: what constitutes a theoretical contribution?. *Academy of management review*, 36(1), 12-32.

Craiger, J. P., Pollitt, M., & Swauger, J. (2005). Law enforcement and digital evidence. In H. Bidgoli (Ed), *Handbook of information security,* (2nd Ed), pp. 739-777). Hoboken, NJ: Wiley

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. (2nd Ed). London: Sage Publications Ltd.

Cross, C., 2019. Cybercrime and the policing of politics in Tanzania. In *Social media and politics in Africa: Democracy, censorship and security*, p.195.

CSI & FBI (2004, June 11). *Computer crime and security survey*. https://www.crime-research.org/news/11.06.2004/423/.

CSIS (2021). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs. *Computer law & security review*, 28(1), 62-68.

CyberX Report (2018). *An executive guide to network and information security directive*. https://cyberx-labs.com/en/nisd/#download-report

Cybok,org (2020). *The cyber security body of knowledge*. https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

Davies, R. S. (2011). Understanding technology literacy: A framework for evaluating educational technology integration. *TechTrends*, 55, 45-52.

De Felice, F., & Petrillo, A. (2014). Proposal of a structured methodology for the measure of intangible criteria and for decision making. *International Journal of Simulation and Process Modelling*, 9(3), 157-166.

De Laine, M. (2000). *Field work participation and practice: Ethics and dilemmas in qualitative research*. London: Sage Publications

Defence Signals Directorate (2011). *Cloud computing security considerations.* Canberra: Commonwealth of Australia.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), 15-32.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, 43(1), 3-24.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global internet filtering* (p. 472). Cambridge, MA: MIT Press

Delfino, M., & Persico, D. (2011). Unfolding the potential of ICT for SRL Development. In *Self-Regulated Learning in Technology Enhanced Learning Environments* (pp. 51-74). Brill Sense.

Densten, I, L. (2003). Senior police leadership: Does rank matter? *Policing An International Journal of Policies and Strategies*, 26(3), 400-418

DeRue, D. S., & Wellman, N. (2009). Developing leaders via experience: the role of developmental challenge, learning orientation, and feedback availability. *Journal of applied psychology*, 94(4), 859.

Dexter, A. S., Janson, M. A., Kiudorf, E., & Laast-Lass, J. (1993). Key information technology issues in Estonia. *Journal of Strategic Information Systems*, 12(2), 139-152.

Dick, G., & Metcalfe, B. (2001). Managerial factors and organisational commitment-A comparative study of police officers and civilian staff. International journal of public sector management.

Diener, E., & Crandall, R. (1978). *Ethics in social and behavioral research*. U Chicago Press.

Digital14 (2021, May 3). *UAE threat landscape 2021.* https://www.digital14.com/docs/default-source/reports/digital-14-cyber-threat-report-may-2021.pdf

Drodge, E. N., & Murphy, S. A. (2002). Interrogating emotions in police leadership. *Human Resource Development Review*, 1(4), 420-438.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.

Dutton, W. H., & Peltu, M. (2007). The emerging Internet governance mosaic: connecting the pieces. *Information polity*, 12(1-2), 63-81.

Dykstra, J., & Sherman, A.T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, 90–98.

ECSO (2018). *Energy networks and smart grids cyber security for the energy sector*. https://ecs-org.eu/documents/publications/5fdb2673903c6.pdf

Eisenhardt, K. M. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25-32.

ENISA (2019). *Cybersecurity skills development in the EU.* https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

Eriksson, P., & Kovalainen, A. (2008). *Qualitative methods in business research*. London: Sage

European Parliament (2006, December 18). *Recommendation of the European parliament and of the council of 18 December 2006 on key competences for lifelong learning.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:394:0010:0018:en:PDF

European Police Office (EPO) 2014. *The internet organised crime threat assessment 2014*. The Hague.

European Union (EU) (2020). *Communication from the commission on the EU security union strategy*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=ES

European Union (EU) (2021, April 14). *Communication from the commission to the European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on the EU Strategy to tackle Organised Crime 2021-2025.* https://op.europa.eu/en/publication-detail/-/publication/94c1d470-9e13-11eb-b85c-01aa75ed71a1

European Union Agency for Network and Information Security (ENISA) (2014). *An evaluation framework for cyber security strategies*. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nationalcyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1;

Europol (2015). *Exploring tomorrow's organised crime*. Europol.

Europol (2017). *Crime in the age of technology*. https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

Europol (2018). *EC3 European Cybercrime Centre. Internet Organised Crime Threat Assessment*. https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Europol (2019, October 19). *Cybercrime is becoming bolder with data at the centre of the crime scene*. https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene

Europol (2021, December 7). *Cyber intelligence*. https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence

Fahsing, I. A., Glomseth, R., & Gottschalk, P. (2008). Characteristics of effective SIOs: a content analysis for management in police investigations. International *Journal of Management and Enterprise Development*, 5(6), 708-722.

Fatih, T., & Bekir, C. (2015). Police use of technology to fight against crime. *European scientific journal*, 11(10).

Fearn-Banks, K. (2007). *Crisis communications: A casebook approach*. 3rd Ed. New Jersey: Lawrence Erlbaum Associates

Ferrari, A., Punie, Y., & Redecker, C. (2012, September). Understanding digital competence in the 21st century: An analysis of current frameworks. In *European Conference on Technology Enhanced Learning* (pp. 79-92). Springer, Berlin, Heidelberg.

Fields, D. (2008). Leadership styles: Developing a leadership style to fit the 21st century challenge. In *21st Century Management: A Reference Handbook*. Eds Charles Wankel. San Francisco, CA: Jossey-Bass.

FireEye (2018, December 17): *Attackers deploy new ICS attack framework 'TRITON' and cause operational disruption to critical infrastructure.*. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Foddy, W., & Foddy, W. H. (1994). *Constructing questions for interviews and questionnaires: Theory and practice in social research*. Cambridge university press.

Forouzan, H., Jahankhani, H., & McCarthy, J. (2018). An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the Metropolitan Police Service. *Cyber Criminology*, 307-323.

Fox, K.E, & Granda, S.E. (2008). Emotions in organisations. In *21st Century Management: A Reference Handbook* Eds Charles Wankel. San Francisco, CA: Jossey-Bass.

Frevel, B. (2014). Collaboration in Crime Prevention Partnerships: Research with a Multilevel Mixed Design. In *Researching the Police in the 21st Century* (pp. 117-140). London: Palgrave Macmillan.

Frydenberg, M., & Lorenz, B. (2020). Lizards in the street! Introducing cybersecurity awareness in a digital literacy context. *Information Systems Education Journal*, 18(4), 33-45.

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5-10.

Gálik, S., & Tolnaiová, S. G. (2020). Cyberspace as a new existential dimension of man. *Cyberspace*, 13.

Garfinkel, S. L. (2010). Digital forensics research: the next 10 years. *Digital Investigation*, 7, 64–73.

Gercke, M. (2009) *Understanding cybercrime: A guide for developing countries.* www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Gerdsri, N., & Kocaoglu, D. F. (2007). Applying the Analytic Hierarchy Process (AHP) to build a strategic framework for technology roadmapping. *Mathematical and computer modelling*, 46(7-8), 1071-1080.

Gjesvik, L., 2019. *Comparing cyber security. Critical infrastructure protection in Norway, the UK and Finland.* NUPI Report.

Global Cybersecurity Index (2018). *Global cybersecurity index, 2018* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Global Cybersecurity Index (2021). *Global Cybersecurity Index, 2021* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Gluschke, G., & Cain, M. H. (2018). *Cyber security policies and critical infrastructure protection*. Institute for Security and Safety Press.

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Doubleday.

Gompf, K., Traverso, M., & Hetterich, J. (2021). Using analytical hierarchy process (AHP) to introduce weights to social life cycle assessment of mobility services. *Sustainability,* 13(3), 1258.

Goodman, C.M. (1987). The Delphi technique: a critique. *Journal of advanced nursing*, *12*(6), 729-734.

Greenberg, A. (2018). Stealthy, destructive malware infects half a million routers. *Wired Magazine*.

Groves, K.S. (2007). Integrating leadership development and succession planning best practices. *Journal of management development*.

Guba, E.G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Ectj*, 29(2), 75-91.

Guest, G., Macqueen, K. M., & Namey, E. E. (2014). *Applied thematic analysis*. Thousand Oaks: SAGE Publications Ltd.

Hague, C., & Williamson, B. (2009). *Digital participation, digital literacy, and school subjects: A review of the policies, literature and evidence*. Futurelab.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, 19(6), 519-536.

Hartfield, C. (2008). The organization of 'organized crime policing' and its international context. *Criminology & Criminal Justice*, 8(4), 483-507

Harvey, D. (1999). Theorizing the transition…flexible accumulation – solid transformation or temporary fix? In *The Economic geography reader*. ed. Bryson, J., Henry, N., Keeble, D., & Martin, R., New York: John Wiley and Sons Limited

Hasson F., Keeney S. & McKenna H. (2000) Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing* 32(4), 1008–1015,

Haugli, M., Ridola, N., Roald,H., & Gansmo, A. (2019, February 8). *Avinor: Dataproblemene er løst*. https://www.nrk.no/ostlandssendingen/avinor_-dataproblemene-er-lost-1.14420969.

Heal, C. S., Cowper, T., & Olligschlaeger, A. (2006). Law enforcement technology. *Working Group,* 2(1), 29-38.

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management*. 27(3), 341-357.

Hitchcock, A., Holmes, R., & Sundorph, E. (2017). *Bobbies on the net: a police workforce for the digital age*. London, UK: Reform. https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/nonsecure/b/o/b/bobbies-on-the-net-police-workforce-for-the-digital-age-17.pdf

Hogue, M. C., Black, T., & Sigler, R. T. (1994). The differential use of screening techniques in the recruitment of police officers. *American Journal of Police*, 13, 113.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

Home Affairs Committee (2018). *Policing for the future: tenth report of Session 2017–19*. London: House of Commons.

Homeland Security (2018, September 7). *Protecting critical infrastructure*. https://www.dhs.gov/topic/protecting-critical-infrastructure

Hooper, C., Martini, B., & Choo, K,R. (2013). Cloud Computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, (29), 152-163.

Hovmand, P., Rouwette, E.A.J.A., Andersen, D., Richardson, G., Calhoun, A., Rux, K., & Hower, T. (2011). *Scriptapedia: a handbook of scripts for developing structured group model building session*s.
https://repository.ubn.ru.nl/bitstream/handle/2066/95406/95406.pdf

Hsu, C.C., & Sandford, B.A. (2010) Delphi technique. In N.J Salkind (ed.), *Encyclopedia of research design*. Thousand Oaks, CA: Sage.

Hunton, P. (2012) Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. *Public Money & Management*, 32 (3), 225-232,

Ilomäki, L., Kantosalo, A., & Lakkala, M. (2011). *What is digital competence?*. https://helda.helsinki.fi/bitstream/handle/10138/154423/Ilom_ki_etal_2011_What_is_digital_competence.pdf

Ilomäki, L., Paavola, S., Lakkala, M., & Kantosalo, A. (2016). Digital competence–an emergent boundary concept for policy and educational research. *Education and information technologies*, 21(3), 655-679.

ISC2 (2021, March 17). *Cybersecurity workforce study 2021*. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2), 26-37.

Jackson, B. A., Vermeer, M. J., Leuschner, K. J., Woods, D., Hollywood, J. S., Banks, D., & Shelton, S. R. (2020, February 15). *Fostering innovation across the US criminal justice system.*
https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4242/RAND_RR4242.pdf

Jacobs, B.A. (1996). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology*, 34(3), 409-431.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In: Akhgar, B., Staniforth, A., & Bosco, F. (Eds.). (2014). *Cyber crime and cyber terrorism investigator's handbook*. London: Sage.

Jamil, M., Ahmad, F., & Jeon, Y.J. (2016). Renewable energy technologies adopted by the UAE: Prospects and challenges – A comprehensive overview. *Renewable and Sustainable Energy Reviews*, (55), 1181-1194.

Janssen, J., Stoyanov, S., Ferrari, A., Punie, Y., Pannekeet, K., & Sloep, P. (2013). Experts' views on digital competence: Commonalities and differences. *Computers & Education*, 68, 473-481.

Jenkins, H., Clinton, K., Purushotma, R., & Weigel, M. (2006). *Confronting the challenges of participatory culture: Media education for the 21st Century*. Cambridge, MA: MIT Press.

Johnson, C.W. (2014). Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures. *Ergonomics*, *57*(3), 419-433.

Joint Committee on the National Security Strategy (JCNSS) (2018). *Cyber security skills and the UK's critical national infrastructure.* Second Report of Session 2017–19, HL Paper 172. London: House of Lords and House of Commons.

Jones, B., & Flannigan, S. L. (2008). Connecting the digital dots: Literacy of the 21st century. *Educause Quarterly*, 29(2), 8-10.

Joshi, P. (2015, October 16). Cyber-crime on the increase in the UK. *International Business Times,* http://www.ibtimes.co.uk/uk-cyber-crime-increase-1524219

Kamat, P., & Gautam, A.S. (2018). Recent trends in the era of cybercrime and the measures to control them. In *Handbook of e-business security* (pp. 243-258). Auerbach Publications.

Kent, K., Chevalier, S., & Grance, T. (2006). Guide to integrating forensic techniques into incident. *Tech. Rep*. 800-86.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2016). *Guide to integrating forensic techniques into incident response. SP800–86*. Gaithersburg: U.S. Department of Commerce

Kitzinger, J. (1995). The methodology of focus groups: the importance of interaction between research participants. *Sociology of health & illness*, *16*(1), 103-121.

Kohnke, A., Shoemaker, D., & Sigler, K.E. (2019). *The complete guide to cybersecurity risks and controls*. Auerbach Publications.

Koksal, T. (2009). *The effect of police organization on computer crime* (Doctoral dissertation).

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows?. *Technological Forecasting and Social Change,* 80(3), 541-555.

Krumsvik, R.J. (2008). Situated learning and teachers' digital competence. *Education and information technologies*, 13(4), 279-290.

Labaka, L., Hernantes, J., & Sarriegi, J. (2016). A holistic framework for building critical infrastructure resilience. *Technological Forecasting and Social Change* 103, 21–31.

Lancaster, G. A., Dodd, S., & Williamson, P. R. (2004). Design and analysis of pilot studies: recommendations for good practice. *Journal of evaluation in clinical practice*, 10(2), 307-312.

Law, N., Woo, D., & Wong, G. (2018). *A global framework of reference on digital literacy skills for indicator 4.4. 2* (No. 51, p. 146). UNESCO.

Lee, J.R., Holt, T.J., Burruss, G.W. & Bossler, A.M. (2019). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review.*

Lehto, M., & Neittaanmäki, P. (Eds.). (2018). *Cyber Security: Power and Technology* (Vol. 93). Springer.

Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-saharan African aviation industry. In *International Conference on Cyber Warfare and Security* (pp. 536-XII). Academic Conferences International Limited.

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 18(2), 157-175.

Leu, D. J., Kinzer, C. K., Coiro, J., Castek, J., & Henry, L. A. (2018). New literacies: A dual-level theory of the changing nature of literacy, instruction, and assessment. In *Theoretical models and processes of literacy* (pp. 319-346). Routledge.

Li, C., & Bernoff, J. (2008). *Groundswell: Winning in a world transformed by social technologies*. Boston: Harvard Business Press.

Li, Y-F., Sansavini, G., Zio, E. (2013). Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. *Reliability Engineering and System Safety*, (111), 195-205.

Libicki, M.C. (2007). *Conquest in cyberspace: national security and information warfare.* Cambridge: Cambridge University Press.

Lilja, K., Laakso, K., & Palomaki, J. (2011). Using the Delphi method. In *Proceedings of PICMET '11.*

Lin, H. (2016). Attribution of malicious cyber incidents. Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper*, (1607), 56.

Lincoln, Y.S., & Guba, E.G. (1985). *Naturalistic inquiry*. London: Sage.

Linstone, H. A., & Turoff, M. (2011). Delphi: A brief look backward and forward. *Technological forecasting and social change*, 78(9), 1712-1719.

Lovet, G. (2009, September 19). *Fighting cybercrime: Technical, juridical and ethical challenges.* http://www.fortiguard.com/papers/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf

Ludwig, B. (1997). Predicting the future: Have you considered using the Delphi methodology?. *Journal of extension*, 35(5), 1-4.

Manning, M., Ransley, J., Smith, C., Mazerolle, L., & Cook, A. (2013). Policing methamphetamine problems: a framework for synthesising expert opinion and evaluating alternative policy options. *Journal of Public Policy*, 33(3), 371-396.

Marios-Panagiotis, E. (2016). Cyber-security in smart cities: The case of Dubai, *Journal of Innovation and Entrepreneurship*, 5 (11), 1-16

Martin, A., & Grudziecki, J. (2006). DigEuLit: Concepts and tools for digital literacy development. *Innovation in teaching and learning in information and computer sciences,* 5(4), 249-267.

Martin, R., & Sunley, P. (2007). Complexity thinking and evolutionary economic geography. *Journal of Economic Geography,* 7(5), 573-601

Martini, B., & Choo, K.R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9, 71-80.

Mäses, S., Randmann, L., Maennel, O., & Lorenz, B. (2018, July). Stenmap: framework for evaluating cybersecurity-related skills based on computer simulations. In *International Conference on Learning and Collaboration Technologies* (pp. 492-504). Springer, Cham.

May, A. (1999). Developing management competencies for fast changing organisations. *Career Development International*, 4(6), 336-339.

McGrath, J. E. (1962). *Leadership behavior: Some requirements for leadership training.* Washington, DC: US Civil Service Commission Office of Career Development.

McGuire, M. (2018). *Into the web of profit: Understanding the growth of the cybercrime economy*. Bromium Report.

McKemmish, R. (1999). *What is forensic computing?* (pp. 1-6). Canberra: Australian Institute of Criminology.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. U.S. Department of Commerce.

Merriam, S. B. (1998). *Qualitative research and case study applications in education. Revised and expanded from case study research in education*. Jossey-Bass Publishers.

Merrick, N. (1997). Strong HRM of the Law. *People Management*, 3(14), 32-5.

Moore, M. H., & Stephens, D.W. (1991). *Beyond command and control: The strategic management of police departments.* https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=137138

Morgan, S. (2020, November 13). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015.

Murphy, D. (2020, June 12). *Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says.* https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html

Nadiri, H., & Tanova, C. (2010). An investigation of the role of justice in turnover intentions, job satisfaction, and organizational citizenship behaviour in hospitality industry, *International Journal of Hospitality Management*, (29), 33-41.

Naseer, H., Maynard, S.B., & Desouza, K.C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication*, 800(2017), 181.

NICE (2021). *Workforce Framework for Cybersecurity* (NICE Framework). https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

NIST (2020). *Cloud computing*. https://csrc.nist.gov/Projects/Cloud-Computing

Nowacki, J., & Willits, D. (2019). An organizational approach to understanding police response to cybercrime. *Policing: An International Journal*.

Nuth, M. S. (2008). Taking advantage of new technologies: For and against crime. *Computer Law & Security Review, 24*(5), 437-446.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & management*, 42(1), 15-29.

Osterman, M.D. (2013). *Digital literacy: Definition, theoretical framework, and competencies.* https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1213&context=sferc

Owaida, A. (2020, March 12). *European power grid organization hit by cyberattack.* https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

Ozdemir, M.S. (2005). Validity and inconsistency in the analytic hierarchy process. *Applied Mathematics and Computation*, *161*(3), 707-720.

Ozkaya, E., & Islam, R. (2019). *Inside the dark web*. CRC Press.

Pallant. J. (2005). *SPSS survival manual: A step by step guide to data analysis using SPSS Version 12.* New York: McGraw Hill Education

Palmer, G. (2001). dfrws technical report: a road map for digital forensic research. *Digital Forensic Research Workshop*. Utica, New York. p. 24

Palmiotto, M. J., Birzer, M. L., & Unnithan, N. P. (2000). Training in community policing: A suggested curriculum. Policing: An International Journal of Police Strategies & Management.

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2019, May). Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane). In *International Conference on Engineering Applications of Neural Networks* (pp. 476-487). Springer, Cham.

Parker, P., Hall, D.T., & Kram, K.E. (2008). Peer Coaching: A Relational Process for Accelerating Career Learning. *Academy of Management Learning & Education*, 7 (4), 487–503.

Patton, M. (2002). *Qualitative evaluation and research methods*. London: Sage.

Peachy, P. (2014, December 8). Police 'failing to train key staff to fight growing threat of cybercrime.' *Independent. http://www.independent.co.uk/news/uk/crime/police-failing-to-trainkey-staff-to-fight-growing-threat-of-cyber-crime-9909334.html*

Pedley, D., McHenry, D., Motha, H., & Shah, J. (2018). *Understanding the UK cyber security skills labour market.* UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework).* (No. NIST Special Publication (SP) 800-181 Rev. 1 (Draft)). National Institute of Standards and Technology.

Phaal, R., Farrukh, C. J., & Probert, D. R. (2001, July). Characterisation of technology roadmaps: purpose and format. In *PICMET'01. Portland International Conference on Management of Engineering and Technology. Proceedings Vol. 1: Book of Summaries (IEEE Cat. No. 01CH37199)* (pp. 367-374). IEEE.

Pickhard, J. (1995). Blue thunder. *People Management*, 1(5), 26-8.

Piersarskas, E. (2020). *Cybersecurity skills framework*. SPARTA. https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

Platt, J. (2007). Case study. In *Sage Handbook of Science and Methodology*, eds Outhwaite, W., Turner, S. P. London: Sage Publications

Pöyhönen, J., Rajamäki, J., Ruoslahti, H., & Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection. *Annals of Disaster Risk Sciences: ADRS,* 3(1), 0-0.

Probert, D. R., Farrukh, C. J. P., & Phaal, R. (2003). Technology roadmapping—developing a practical approach for linking resources to strategic goals. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture,* 217(9), 1183-1195.

Punie, Y. (2007). Learning Spaces: an ICT-enabled model of future learning in the Knowledge-based Society. *European journal of education*, 42(2), 185-199.

Putnam, T. L., & Elliott, D. D. (2001). International Responses to cyber crime. *Transnational Dimension of Cyber Crime and Terrorism*, 35-66.

Quille, M. (2009). *Keynote address. Current threats and future challenges posed by cybercrime*. Octopus Conference, CoE.

Radvanovsky, R., & McDougall, A. (2018). *Critical infrastructure: homeland security and emergency preparedness.* CRC PRESS.

Rafferty, A. E., & Griffin, M. A. (2004). Dimensions of transformational leadership: Conceptual and empirical extensions. *Leadership Quarterly*, 15(3), 329–354.

Rafferty, A.E., * Griffin, M.A. (2006). Refining individualised consideration: Distinguishing developmental leadership and supportive leadership. *Journal of Occupational and Organisational Psychology*, 79, 37-61

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017, June). UAE cybercrime law and cybercrimes—An analysis. In *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)* (pp. 1-6). IEEE.

Rana, E. (1999). Police urged to find right blend of personnel skills. *People Management*. 5(18), 18-20.

Reedy, K., & Goodfellow, R. (2012). *Digital and information literacy framework.* Open University.

Rees, D. (2021, June 18). *Cyber attacks in healthcare: the position across Europe.* https://www.pinsentmasons.com/out-law/analysis/cyber-attacks-healthcare-europe

Richardson, G. P., & Andersen, D. F. (1995). Teamwork in group model building. *System Dynamics Review*, 11(2), 113-137.

Richey, J. M., & Grinnell, M. (2004). Evolution of roadmapping at Motorola. *Research-Technology Management*, 47(2), 37-41.

Robertson, J.G. (2019). *The impact of the digital society on police recruit training in Canada* (Doctoral dissertation).

Robson, C. (2002). *Real world research: A resource for social scientists and practitioner researchers*. 2nd Edn. Oxford: Blackwell Publishing

Rouleau, L., & Balogun, J. (2011). Middle managers, strategic sensemaking, and discursive competence. *Journal of Management studies*, 48(5), 953-983.

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence*, 26(3), 453-481.

Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field Methods*, 15(1), 85–109.

Saaty, T. L. (1980). *The analytic hierarchy process*. McGraw-Hill, New York.

Saaty, T.L. (1978). Modeling unstructured decision problems—the theory of analytical hierarchies. *Mathematics and computers in simulation*, 20(3), 147-158.

Saaty, T.L. (1990). How to make a decision: the analytic hierarchy process. *European journal of operational research*, 48(1), 9-26.

Sanders, C. B., & Hannem, S. (2012). Policing "the risky": Technology and surveillance in everyday patrol work. *Canadian Review of Sociology/Revue canadienne de sociologie*, 49(4), 389-410.

Santos, J. P., Caetano, A., & Tavares, S. M. (2015). Is training leaders in functional leadership a useful tool for improving the performance of leadership functions and team effectiveness?. *The Leadership Quarterly*, 26(3), 470-484.

Sapkota, P. (2014). *Application of analytic hierarchy process for strategic planning and implementation at Nepalese universities and colleges.* http://www.isahp.org/uploads/p730266.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students*. 4th eds. London: Pearson Education Ltd.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students*. England: Pearson Education Limited

Savona, E. U., & Mignone, M. (2004). The fox and the hunters: How IC technologies change the crime race. *European Journal on Criminal Policy and Research,* 10(1), 3-26.

Schafer, J. A., & Boyd, S. (2020). The future of education and training for policing. *Exploring the Future of Crime, Communities, and Policing*, 372.

Scheider, M.B., Chapman, R., & Schapiro, A. (2009). Towards the unification of policing innovations under community policing. *Int'l J. Police Strat.& Mgmt*, 32 (4), 694-718.

Schreuders, Z. C., Cockcroft, T. W., Butterfield, E. M., Elliott, J. R., & Soobhany, A. R. (2018). *Needs assessment of cybercrime and digital evidence in a UK police force.* Leeds Beckett University. https://eprints.leedsbeckett.ac.uk/id/eprint/5076/1/Needs

Schwandt, D. R., & Gorman, M. (2004). Foresight or foreseeing? A social action explanation of complex collective knowing. *Managing the future: Foresight in the knowledge economy*, 77-97.

Sefton-Green, J., Nixon, H., & Erstad, O. (2009). Reviewing approaches and perspectives on "digital literacy". *Pedagogies: An International Journal*, 4(2), 107-125.

Sekaran, U., & Bougie, R. (2010). *Research methods for business: a skill building approach* (5th Ed). New Jersey: John Wiley and Sons.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., Boettinger, K., Gall, M., Brost, G., Ponchel, C. & Haustein, M. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, 166-182.

Sharma, R., Fantin, A.R., Prabhu, N., Guan, C., & Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. *Telecommunications Policy*, 40(7), 628-643.

Shavers, B., & Bair, J. (2016). *Hiding behind the keyboard: uncovering covert communication methods with forensic analysis*. Syngress.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. New York: The Penguin Press.

Skogan, W. G., & Hartnett, S. M. (2005). The diffusion of information technology in policing. *Police Practice and Research*, 6, 401–417.

Skorupka, C. & Boiney, L. (2015). *Cyber Operations Rapid Assessment (CORA): A guide to best practices for threat-informed cyber security operations*. Mitre Corp Mclean Va Mclean.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, 6(1), 1-21.

Smith, G. (2018). The intelligent solution: automation, the skills shortage and cyber-security. *Computer Fraud & Security, 2018*(8), 6-9.

Smithson, J. (2000). Using and analysing focus groups: limitations and possibilities. *International journal of social research methodology, 3*(2), 103-119.

Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security: The transnational dimension. *The transnational dimension of cyber crime and terrorism,* 1-34.

Sommer, M., Njå, O., & Lussand, K. (2017). Police officers' learning in relation to emergency management: A case study. *International journal of disaster risk reduction*, 21, 70-84.

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security,* 2004(1), 8-12.

Staber, U. (1997). An ecological perspective on entrepreneurship in industrial districts. *Entrepreneurship & Regional Development*, 9(1), 45-64.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A.J., Repchick, K.M., Zaccaro, S.J., Dalal, R.S., & Tetrick, L.E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy*, *13*(4), 20-29.

Stinissen, J., & Geers, K. (2015). A legal framework for cyber operations in Ukraine. *Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn*, 123-134.

Stoetzer, O., & Robertson, J. (2019). *Upfront and digital: training and educating for digital literacy.* http://www.cape-educators.ca/wp-content/uploads/2020/01/Stoetzer-and-Robertson-presentation.pdf

Stokes, T. R. (2010). Gone the renaissance cop: Will specialized police officers be the staffing models of the future? *Journal of California Law Enforcement*, 4.

Tashakkori, A., & Teddlie, C. (2009). Integrating qualitative and quantitative approaches to research. *The SAGE handbook of applied social research methods*, 2, 283-317.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, 2011(3), 4-10.

The Organisation for Economic Co-operation and Development (OECD) (2005). *The definition and selection of key competencies*. *Executive summary.* The DeSeCo Project. http://www.oecd.org/dataoecd/47/61/35070367.pdf.

Thorpe, S., & Ray, I. (2012). Detecting Temporal Inconsistency in Virtual Machine Activity Timelines. *Journal of Information Assurance & Security*, 7(1).

Timpf, J. L. (2014). *Training police officers to meet the demands of public expectations* [White paper]. https://shsu-ir.tdl.org/handle/20.500.11875 /1924

Tobey, D. H., Reiter-Palmon, R., & Callens, A. (2012). Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance. *OST Working Group Report. National Board of Information Security Examiners, Idaho Falls, ID.*

Tolbert, P. S., & Zucker, L. G. (1983). Institutional sources of change in the formal structure of organizations: The diffusion of civil service reform, 1880–1935. *Administrative Science Quarterly*, (28), 22–39.

Tropina, T. (2017). Cyber-policing: the role of the police in fighting cybercrime. *Special Issue 2 Eur. Police Sci. & Res. Bull.,* 287.

Trottier, D., & Lyon, D. (2013). Key features of social media surveillance. In *Internet and Surveillance* (pp. 89-105). Routledge.

Turner, J.C. (1991). *Social influence*. Pacific Grove, CA: Brooks/Cole Publishing Company

Turner, S.P. (2007). *Introduction: Evaluation, engagement, and collaborative research*. In *The Sage Handbook of Science and Methodology*, eds Outhwaite, W., Turner, S. P. London: Sage Publications.

Turoff, M., Bañuls, V. A., Plotnick, L., & Hiltz, S. R. (2014). Development of a dynamic scenario model for the interaction of critical infrastructures. In *ISCRAM 2014,* Penn State College (US), 2014.

UAE Gov (2019). *National cybersecurity strategy*. https://www.tra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf

UAE Gov (2021, November 16). *Bridging digital divide*. https://u.ae/en/about-the-uae/digital-uae/bridging-digital-divide

Udrea, C. (2014). Pedagogical strategies for continuous training in the police system. *Procedia-Social and Behavioral Sciences, 142*, 597-602.

UK Gov (2018). *Initial national cyber security skills strategy: Increasing the UK's cyber security capability*. HMSO

UN (2011). *Handbook on police accountability, oversight and integrity*. https://www.unodc.org/pdf/criminal_justice/Handbook_on_police_Accountability_Oversight_and_Integrity.pdf

UN (2015). *Crime Congress 2015: A focus on Cybercrime.* https://www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html

United Nations Office on Drugs and Crime (UNODC) (2013). *Comprehensive Study on cybercrime*. Geneva: United Nations.

United Nations Office on Drugs and Crime (UNODC) (2019). *Cybercrime investigations. https://www.unodc.org/e4j/en/cybercrime/module-5/index.html*

Van Deursen, A.J.A.M., Courtois, C., & Van Dijk, J. (2010). *Internet skills. Vital assets in an information society.* Enschede, the Netherlands: University of Twente.

Van Es, K., & Schäfer, M.T. (2017). *The datafied society. Studying culture through data*. Amsterdam University Press.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, 4(2), 32-46.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity.

Wall, D.S. (1998). Catching cybercriminals: policing the Internet. *International Review of Law, Computers & Technology*, 12(2), 201-218.

Wall, D.S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*, 2(2).

Wall, D.S., & Williams, M. eds., (2017). *Policing cybercrime: Networked and social media technologies and the challenges for policing*. London: Routledge.

Wall, D.S., & Williams, M.L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. *Policing & Society*, 23 (4).

Walsh, J. P., & Ungson, G. R. (1991). Organisational memory. *Academy of Management: Academy of Management Review*, 16(1), 57-91

Weed, S. A. (2019). *US policy response to cyber attack on SCADA Systems supporting critical national infrastructure*. Air Force Research Institute.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research*, (6), 419–434.

Wexler, C. (2012, December 12). *How are innovations in technology transforming policing*. https://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf

White, M. D., & Escobar, G. (2008). Making good cops in the twenty-first century: Emerging issues for the effective recruitment, selection and training of police in the United States and abroad. *International Review of Law, Computers & Technology*, 22(1-2), 119-134.

Wiedeman, R. (2018, February 19). Gray hat. *New York Magazine*, http://nymag.com/intelligencer/2018/03/marcus-hutchins-hacker.html

Williams, C. B., Fedorowicz, J., Kavanaugh, A., Mentzer, K., Thatcher, J. B., & Xu, J. (2018). Leveraging social media to achieve a community policing agenda. *Government Information Quarterly*, *35*(2), 210-222.

Williams, M, L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J., & Sloan, L. (2013) Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and Society*, 23 (4), 461-481.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: an organizational analysis. *Criminal Justice Studies*, 29 (2), 105-124.

Willyard, C.H., & McClees, C.W. (1987). Motorola's technology roadmap process. *Research management*, 30(5), 13-19.

Wilson, J. (2010). *Essentials of business research: A guide to doing your research project.* SAGE Publications, p.7

Wolf, J. W. (2013). *The training curriculum at Pennsylvania municipal police academies: Perceptions of effective training* (Doctoral dissertation).

World Economic Forum (2020). *The global risks report 2020*. 15th Ed. Cologny, Switzerland: World Economic Forum.

World Economic Forum (WEF) (2020). *Global risks report 2020*. https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

Xiong, J. (2016, December). Information ability evaluation based on AHP for students in police college. In *Proceedings of the 2016 International Seminar on Education Innovation and Economic Management (SEIEM 2016).* Chongqing, China: Atlantis Press.

Yar M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology,* 2(4, 407-27.

Yar, M. (2006). *Cybercrime and society.* London: Sage.

Yeboah-Boateng, E. O., & Akwa-Bonsu, E. (2018). Cyber-security intelligence gathering: Issues with knowledge management. In *Evaluating Media Richness in Organizational Learning* (pp. 203-231). IGI Global.

Yin, R.K. (2003). Design and methods. *Case study research*, 3(9.2).

Yin, R.K. (2009). *Case study research: Design and methods.* 4th Ed. London: Sage Limited.

ZAWYA (2021, October 17). *GITEX 2021: ICS Computers in UAE subject to increased cyber threats when compared to worldwide.* https://www.zawya.com/mena/en/press-releases/story/GITEX_2021_ICS_Computers_in_UAE_subject_to_increased_cyber_threats_when_compared_to_worldwide-ZAWYA20211017090503/

Zedner, L. (2007). Pre-Crime and Post-Criminology? *Theoretical Criminology* 11(2), 261–81.

Zhang, C., & Ramirez-Marquez, J.E. (2013). Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information. *IIE Transactions*,45(3), 244-258.

Appendix 1: NICE Cybersecurity Skills Framework

The full details of the NICE Cybersecurity Workforce Framework are available at https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

Table A1: Cybersecurity Categories, Specialisms and Work Roles

CyberSecurity Categories		CyberSecurity Specialisms	Cybersecurity WorkRoles
Analyze	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	All-Source Analysis	All-Source Analyst
			Mission Assessment Specialist
		Exploitation Analysis	Exploitation Analyst
		Language Analysis	Multi-disciplined Language Analyst
		Targets	Target Developer
			Target Network Analysts
		Threat Analysis	Threat/Warning Analyst
Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	Collection Operations	All Source-Collection Manager
			All Source-Collection Requirements Manager
		Cyber Operational Planning	Cyber Intel Planner
			Cyber Ops Planner
			Partner Integration Planner
		Cyber Operations	Cyber Operator
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Cyber Investigation	Cyber Crime Investigator
		Digital Forensics	Cyber Defense Forensics Analyst
			LawEnforcement/Counterintelligence Forensics Analyst
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security	Customer Service and Technical Support	Technical Support Specialist
		Data Administration	Data Analyst
			Database Administrator
		Knowledge Management	Knowledge Manager
		Network Services	Network Operations Specialist
		Systems Administration	System Administrator
		Systems Analysis	Systems Security Analyst
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	Cybersecurity Management	Communications Security (COMSEC) Manager
			Information Systems Security Manager
		Executive Cyber Leadership	Executive Cyber Leadership
		Legal Advice and Advocacy	Cyber Legal Advisor
			Privacy Officer/Privacy Compliance Manager

		Program/Project Management and Acquisition	IT Investment/Portfolio Manager
			IT Program Auditor
			IT Project Manager
			Product Support Manager
			Program Manager
		Strategic Planning and Policy	Cyber Policy and Strategy Planner
			Cyber Workforce Developer and Manager
		Training, Education, and Awareness	Cyber Instructional Curriculum Developer
			Cyber Instructor
Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Cyber Defense Analysis	Cyber Defense Analyst
		Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist
		Incident Response	Cyber Defense Incident Responder
		Vulnerability Assessment and Management	Vulnerability Assessment Analyst
Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	Risk Management	Authorizing Official/Designating Representative
			Security Control Assessor
		Software Development	Secure Software Assessor
			Software Developer
		Systems Architecture	Enterprise Architect
			Security Architect
		Systems Development	Information Systems Security Developer
			Systems Developer
		Systems Requirements Planning	Systems Requirements Planner
		Technology R&D	Research & Development Specialist
		Test and Evaluation	System Testing and Evaluation Specialist

Table A2: Speciality Areas

Categories	Specialty Areas	Specialty Area Descriptions
Securely Provision (SP)	Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
	Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
	Systems Architecture (ARC)	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
	Technology R&D (TRD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning (SRP)	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
	Test and Evaluation (TST)	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
	Systems Development (SYS)	Works on the development phases of the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
	Knowledge Management (KMG)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

	Customer Service and Technical Support (STS)	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.
	Network Services (NET)	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
	Systems Administration (ADM)	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis (ANA)	Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
	Training, Education, and Awareness (TEA)	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management (MGT)	Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
	Strategic Planning and Policy (SPP)	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
	Executive Cyber Leadership (EXL)	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
	Program/Project Management (PMA) and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information

Categories	Specialty Areas	Specialty Area Descriptions
		exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
	Cyber Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
Analyze (AN)	Threat Analysis (TWA)	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
	Exploitation Analysis (EXP)	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis (ASA)	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
	Targets (TGT)	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis (LNG)	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

Categories	Specialty Areas	Specialty Area Descriptions
Collect and Operate (CO)	Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process.
	Cyber Operational Planning (OPL)	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
	Cyber Operations (OPS)	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate (IN)	Cyber Investigation (INV)	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
	Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Appendix 2: Open Ended Questionnaire

Round 1

This questionnaire is part a PhD research undertaken to ‘***Develop a Digital Competences Framework for UAE Law Enforcement Agencies to enable them enhance Cyber security of Critical Infrastructure’.***

Please read and answer the questions below. This is an open ended questionnaire (which means there is no fixed limit to your answers). You have the flexibility to either provide your responses in a written form in the spaces provided below or alternatively send a recorded audio transcript to the following email: *[XXXXXXX]*

Digital Competences Training Plan

1a. What factors of digital competences training plan do you perceive to be critical for Critical Infrastructure Protection? Why do you think these factors are important to improve digital competences?

....
....
....
....
....

1b. What strategies do you think are important to apply in order to attain best practice and why?

....
....
....
....
....

Digital Competences Continues Professional Development & Training

2a. What factors of digital competences ‘continues professional development training’ (CPD) do you believe to be important for continuous developing digital competences? Please explain why.

………………………………………………………………………………………………
………………………………………………………………………………………………
……………………………………………………………………………….....................................
....

....

2b. What strategies do you think are important to apply in order to achieve best practice and why?

....
....
....
....
....

Digital Training Evaluation & Monitoring

3a. What factors or elements of training and evaluation are critical for improving for developing digital competences and Why?

………………………………………………………………………………………………...………
………………………………………………………………………………………………………
………………………………………………………………………………………..
....
....

3b**.** What strategies do you think are important to apply in order to achieve best practice and why?

....
....
....
....
....

Digital Competency Skills Development & Resources

4a. What factors or elements of digital competences skills & resources are significant to enhancing Critical Infrastructure Protection and Why are they important?

……………………………………………………………………………………………….........
....
....
....
....

4b. What organisational, managerial, & leadership approaches as well as resources needs can improve Critical Infrastructure Protection and Why?

……………………………………………………………………………………………………
……………………………………………………………………………………………………
………………………………………………………………………………….............................
....
....

4c. What strategies do you think are important to apply and achieve best practice and Why?

....
....
....
....
....

Critical Infrastructure Protection Phases of Attack

5a.What factors or processes of do you perceive to be critical for protecting Critical Infrastructure on different phases of the attack (pre; aftermath; and recovery)? and Why do you think these factors are important?

……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………

……………………………………………………………………

5b. What strategies do you think are important to apply and achieve best practice?

……
……
…………………………………………………………………………………….

……

……

Critical Infrastructure & Cyber Defence Systems

6a. What factors of critical infrastructure & cyber defence systemsdo you believe are important for improving Critical Infrastructure Protection? and Why do you think these factors are critical?

……
……
……………………………………………………………………………………

……

……

6b. What strategies do you think are important to apply in order to achieve best practice and why?

……
……
……………………………………………………………………………………

....

……

Critical Infrastructure Protection Effectiveness

7a. What factorsdo you perceive to be critical for effective critical infrastructure protection and Why?

……………………………………………………………………………………………………
……………………………………………………………………………………………………
………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

7b. What strategies do you think are important to apply in order to achieve best practice and why?

……………………………………………………………………………………………………
……………………………………………………………………………………………………
………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

Legislative Reform Public Engagement

8a. In your view is increased legislative powers through reform and public engagement important for critical infrastructure protection? What elements of legislative reformare significant for improving critical infrastructure governance and cooperation?

....
....
....

....

....

8b. What strategies do you think are important to apply in order to achieve best practice and why?

………………………………………………………………………………………………………
………………………………………………………………………………………………………
…………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

Learning & Feedback: Continuous Development of National Digital Competences for UAE Critical Infrastructure Protection

9a. What factors of learning and feedback do you perceive to be vital towards continuous development of national digital competences for critical infrastructure protection? Please explain why do you think these factors are important?

....

....
....

....

....

9b. What strategies do you think are important to apply in order to achieve best practice and why?

....

....
....

....

....

Appendix 3 Analytical Hierarchy Process Guide

Developing a Framework for UAE law enforcement Agents to Enhance Digital Competences for Critical Infrastructure Protection

In this phase (3) of the Delphi process the purpose is to evaluate the relevance/applicability of components of Workforce Framework for Cyber security (NICE Framework). This document contains the research instrument for ranking and evaluating the importance of different elements and sub-elements of the NICE Cybersecurity Education Framework. The NICE framework consists of 7 high-level cybersecurity functions; 33 speciality areas; 52 workroles and underlying specific knowledge, skills, and abilities (KSAs). The scope of this evaluation is focused on on the 7 high-level cybersecurity functions; 33 speciality areas; 52 workroles.

Key Questions

The evaluation is concerned with the following key questions:

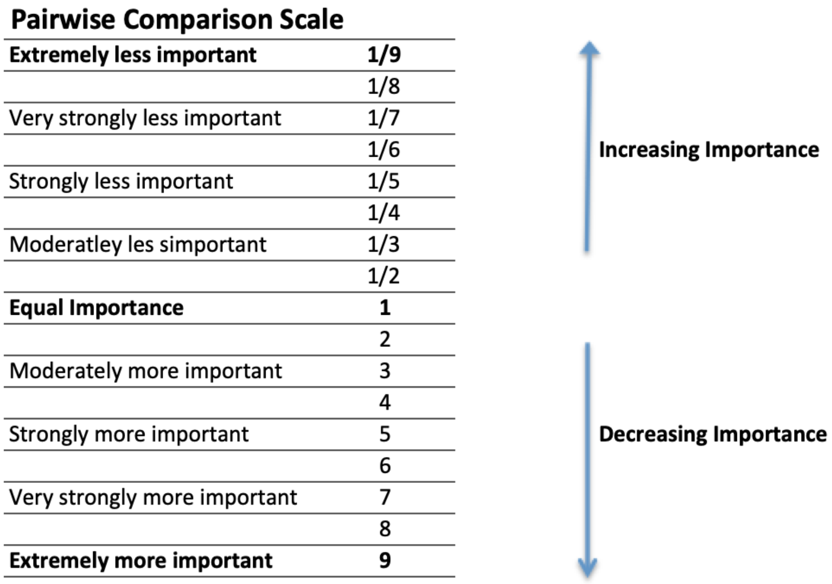
1. Which of the 7 categories are relevant for digital competence of law enforcement in the area of CPI?
2. Please review the 33 specialty areas of cybersecurity under the 7 categories. The speciality areas are listed under under of the top level categories. Which are of the speciality are relevant/applicable to the role of law enforcement for CPI.
3. Which of cybersecurity work roles are relevant or applicable to digital competence of law enforcement in the area of CPI?

The evaluation will be conducted using Analytical Hierarchy Process (AHP) which is a quantitative technique to rank/prioritise elements of the NICE Framework. A spreadsheet is supplied consisting of a matrix form consisting of the elements of the CyberSecurity Framework that will be ranked that will ranked/prioritised based on the following comparison scale.

There are 14 matrices. Each matrix contains every possible combination of pairing between all the items. On average each matrix should take only a few minutes to complete.

How to use the Priority Scale

Please examine each matrix. And for every pair of items decide on the relative importance of the two items using the comparison scale in the table below.



Pairwise Comparison Scale

Extremely less important	**1/9**
	1/8
Very strongly less important	1/7
	1/6
Strongly less important	1/5
	1/4
Moderatley les simportant	1/3
	1/2
Equal Importance	**1**
	2
Moderately more important	3
	4
Strongly more important	5
	6
Very strongly more important	7
	8
Extremely more important	**9**

Increasing Importance
Decreasing Importance

For example in the categories sheet you will compare and evaluate the importance of the 7 cybersecurity functions to law enforcement for CPI. In the yellow cells enter your rating. If you think 'Analyze' is equal importance to 'Collect & Operate' then using the scale below enter 1. If ' you decide ‘Analyze' is extremely more important, then enter 9. If Extremely less important then enter 1/9.

Example AHP Matrix 1 – Pairwise Comparison on Cyber Functions

	Analyze	Collect & Operate	Investigate	Operate & Maintain	Oversee & Govern	Protect & Defend	Securely Provision
Analyze	1	Enter Rating	Enter Rating	Enter Rating	Enter Rating	Enter Rating	Enter Rating
Collect & Operate	1	1	Enter Rating	Enter Rating	Enter Rating	Enter Rating	Enter Rating
Investigate	1	1	1	Enter Rating	Enter Rating	Enter Rating	Enter Rating
Operate & Maintain	1	1	1	1	Enter Rating	Enter Rating	Enter Rating
Oversee & Govern	1	1	1		1	Enter Rating	Enter Rating
Protect & Defend	1	1	1	1	1	1	1
Securely Provision	1	1	1	1	1	1	1

Appendix 4: Semi-structured Questionnaire

Developing a Framework for UAE law enforcement Agents to Enhance Digital Competences for Critical Infrastructure Protection

THE QUESTIONNAIRE

This research survey is made by ***Mohammed Butti i***n regards to developing digital competences of UAE police to enable them combat cybercrime. All information provided by you will be held in confidence and will be used for the sole purpose of this research without reference to your name or person. You also reserve the right to withdraw at any time should you chose to.

ORGANISATION:	
DEPARTMENT	
POSITION	

1. How long (Years) have you worked in the UAE police force? [*please tick the applicable one*]

0 – 5 years		**16 – 20 years**	
6 – 10 years		**20 – 25 years**	
11 – 15 years		**Over 25 years**	

2. Please tick on a scale of 0 to 5, with 5 being the highest indicate how often do you attend training on cybercrime policing strategies.

0 (None)	**1**	**2**	**3**	**4**	**5 (Highest)**

3. Please identify and rank by ticking which are the highest Key factors to be considered for effective '**Balance, Type, & Relevance**'?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Formation of Critical Infrastructure Protection digital expertise group/forum						
Categorizations and prioritization of digital skills training needs						
Breadth and depth of digital training						
Sequence and order of digital training						
Parallel vs vertical digital training						
Digital Train the trainer routine						
Balancing Private vs public companies interests						
Trans-border digital competences training						
Benchmarking with global digital best practices						

Digital Training for in-house talent development						
360 degrees training (in all areas of digital policing)						
Number of updated digital training plans						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

4. Please identify and rank by ticking which are the highest Key factors to be considered towards effective **<u>‘Futuristic Training using unconventional methods</u>**’?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Provision of accessible digital micro training and e-learning						
Utilising a Digital Learning Management System (LMS) platforms						
Providing opportunities for Mobile learning						
Utilising Virtual Simulation exercises						

Utilizing Gamification tools						
Providing opportunities for using Industry 4.0 technologies applications such as Internet of Things (IoT) etc						
Applying range of advanced technologies like Virtual Reality (VR), Augmented Reality (AR), Artificial Intelligence (AI) and Robotics						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

5. Please identify and rank by ticking which are the highest Key factors of specialisations to be considered for effective '**<u>Digital Knowledge and Skills Developement</u>**'?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Provision of clearer Guidelines for evaluation						

Certifications of all digital Specializations						
Network security Certifications						
Digital forensic certifications						
Information security certifications						
Ethical hacking techniques certifications						
Information security certifications						
Information system security certifications						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

6. Please identify and rank by ticking which are the highest Key factors of '**Digital Knowledge andSkills Development**' required for effective counteracting of cyber threats of Critical Infrastructure?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Developing skills for Modeling and testing of threat intelligence						
Developing expertise in all domains like digital forensics, network investigation, and technical inquirer						
Achieving Balance of knowledge vs. skills						
Developing skills of detecting, investigating, and putting together cyber-crime evidences						
Developing skills for social media policing (covert and overt)						
Achieving balance between Generalist vs specialist skills routes						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

7. Please identify and rank by ticking which are the highest Key factors to be considered at different phases of attack (pre, after, recovery) for effective ‘**<u>Proactive, Reactive, & Preventative Measure’</u>**?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Joint preparation and training						
Working closely with communities						
Undercover social media policing						
Contingency planning						
Situational information assessment						
Cybercriminal profiling						
Volume of evidence						

Preventative measures						
Provision of Resources for inter-jurisdictional investigation						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

8. Please identify and rank by ticking which are the highest Key factors of defence systems to be considered for effective ‘**Socio-Technical Systems**’?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Strengthened cloud network infrastructure & forensic systems						
Establish National crime mapping for cyber-attack on CI system						
Develop Systems of Partnership between law enforcement agents, intelligence community, and national coordination						

centers						
Develop volunteer cyber defense system						
Develop Systems of lateral surveillance on social media using pseudonyms						
Maintenance of time alteration forensic evaluations mechanisms on cloud						
Development of Public Private Partnership arrangements systems						
Maintenance of periodic inspections of cloud infrastructure						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

9. Please identify and rank by ticking which are the highest Key factors to be considered for effective '**Resilience**'?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Readiness & Preparedness						
Speed to seizure, acquisition, analysis, and investigation of evidences						
Novelty in responding to Critical Infrastructure attack						
Resources intensity for investigations and recovery purposes						
Risk assessments, monitoring and evaluation						
Common vision						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

10. Please identify and rank by ticking which are the highest Key factors to be considered for effective '**Increase in Legislative Powers**' required for improved critical infrastructure protection?

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Increased powers to intercept cybercrime data stored on cloud platforms						
Increased cooperation for sharing regional intelligence on cybercrime						
Maintenance of up to date information system on interception and retention of real time data						
Societal engagement and awareness						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

11. Please identify and rank by ticking which are the highest Key factors to be considered for effective ‘**Adaptive Learning** ’ required for improved policies linked to critical infrastructure protection.

	0 **(None)**	**1**	**2**	**3**	**4**	**5** **(Highest)**
Learning from international best practices						
Receptivity and openness to learning new technology						
Peer to Peer Learning						
Learning from failure						
Reflecting on the current cyber threats, skills gap, and resources within the UAE law enforcement agencies, elaborates on key influential factors ranked above.						

8 Appendix 5: Table of Critical Factors

Section 5. Digital Competence Training Plan

		Critical	**Non-critical**
	We receive training on dealing with digital service providers from private and public sectors		
	We receive training based on specialized cybercrime policing such as *Domain experts, digital forensics, network investigators, Technical enquirer, network security and architecture*		
	We receive training on degree of preparedness for critical infrastructure attacks (*Reactive, Proactive, Preventative)*		
	We receive training on protection of *Critical Physical Infrastructure & Critical Information Infrastructure, computer networks, software, cloud etc*		
	We receive training on social media policing for critical infrastructure protection *Facebook, Twitter, Instagram*		
	We receive training on new technological Innovations to refel critical infrastructure attack *Online neighbourhood monitoring etc*		

Section 6: Digital Competences Continues Professional Development & Training

Do you agree with the following?

	We frequency attend training on digitally competences	Critical	Non-critical
	We follow our National Guidelines for the future development of our digital competences		
	We receive training using exercises such as Drills and simulations programmes		
	We receive certifications for digital Skills acquired		

Section 7: Digital Competency Skills Development

Do you agree with the following?

		Critical	Non-critical
Organisational Digital Competences	*We received training for improved organisational loyalty, commitment, & motivation*		
Managerial Digital Competences	*We received training for improved Decision, communication, and coordination*		
Leadership Digital Competences	*We received training for improved skills in Developmental leadership & Crisis leadership*		
Investment in key Technical and investigative Competence capacities	*Our unit invests in developing strengthening our Technical and technological infrastructure*		

	Our unit invests in developing or Human Resources		
	Our provides needed Financial Resources		

Section 8: Critical Infrastructure Protection Phases of Attack

Do you agree with the following?

		Critical	Non-critical
	We have been trained in preparation for Pre cyber-attack:		
	We have been trained in preparation for Aftermath of cyber Attack		
	We have been trained in preparation for Recovery from cyber Attack:		

Section 9: Critical Infrastructure & Cyber Defence Systems

Do you agree with the following?

		Critical	Non-critical
	We keep well-developed Data bases, records, & crime mapping		
	We engage Volunteer cyber defenders to enhance our critical infrastructure protection		
	We ensure Compliance to		

	International Security Directives		
	We engage in the practice of Public Private Partnerships (cooperation's) for enhanced critical infrastructure protection		
	We engage in a fruitful Partnership between law enforcement agencies, intelligence community, and national coordination centres.		
	We have a well-developed and efficient reporting systems crimes committed online		
	State plays a key role towards the governance of cyberspace in the UAE		

Section 10: Critical Infrastructure Protection Effectiveness

Do you agree with the following?

		Critical	Non-critical
	We respond to critical infrastructure attack with Speed and Novelty		
	We respond to critical infrastructure attack with Coordination & Resilience		
	We respond to critical infrastructure attack with Unified Direction (common Vision)		
	We respond to critical infrastructure attack with resources intensity		

Section 11: Legislative Reform Public Engagement

Do you agree with the following?

		Critical	Non-critical
	Our laws allows law enforcement agents to engage in Interception and retention of cybercrime data in real time		
	Our law allows law enforcement agents to engage in sharing cybercrime data for intelligence purposes regionally		
	Our laws allows law enforcement agents to engage in interception of cybercrime data stored on cloud platforms *(*Saas, Paas, Iaas) – seizure, acquisition and analysis		
	We are allowed a lawful access and disclosure of digital data among the law enforcement		

Section 12: Learning & Feedback: Continuous Development of National Digital Competences for CIP protection

		Critical	Non-critical
	We engage in continues Learning from our previous failures,		
	We are very receptive to learning,		
	We engage in learning from best practices of critical infrastructure protection from around the world		

9 Appendix 7: Summarised Table of New Emergent Themes from Thematic Analysis

Critical Factors	**Key Elements**			**Summary of Emergent Themes from the Questionnaire**
Digital Competence Training Plan				
	Nature of ownership (private vs public)			
	Nature of specialisation *specialized cybercrime policing units *Domain experts, digital forensics, network investigators, Technical enquirer, network security and architecture*			Balance, Type, & Relevance of Training
	Degree of preparedness *Reactive, Proactive, Preventative*			
	Nature of Infrastructure *Critical Physical Infrastructure & Critical Information Infrastructure, computer networks, software, cloud etc*			
	Nature of social media handles			

	Facebook, Twitter, Instagram			
	Technological Innovation *Online neighbourhood monitoring, tension, volunteers*			
Digital Competences Continues Professional Development & Training	*Frequency of training & recruitment of digitally competent law enforcement agents*			Futuristic Training & Unconventional techniques
	National Guidelines for the future			
	Continues testing, evaluations using exercises Drills and simulations programmes			
Digital Training Evaluation & Monitoring	*Content, Skills Certifications & Capacity building*			Mandatory specialisations and Certifications Digital knowledge and skills
Digital Competency Skills Development & Resources				
Organisational Digital Competences	*Loyalty, commitment, & motivation*			
Managerial Digital Competences	*Decision, communication, and coordination*			Non-Technical Digital Competences

Leadership Digital Competences	*Developmental leadership & Crisis leadership*			
Investment in key Technical and investigative Competence capacities	*Technical and technological infrastructure*			
	Human Resources			
	Financial Resources			
Critical Infrastructure Protection Phases of Attack				
	Pre cyber-attack:			Proactive, Reactive, Preventative Measures
	Aftermath of cyber Attack			
	Recovery from cyber Attack:			
Critical Infrastructure & Cyber Defence Systems				
	Data bases, records, & crime mapping			Socio-Technical System (Cloud, Public, & Volunteer Defenders)

	Volunteer cyber defenders			
	Compliance to International Security Directives			
	Public Private Partnerships (cooperation’s)			
	Partnership between law enforcement agencies, intelligence community, and national coordination centres.			
	Efficient reporting systems			
	Role of State and cyber governance			
Critical Infrastructure Protection Effectiveness				
	Speed and Novelty			
	Coordination & Resilience			
	Unified Direction (common Vision)			
	Recovery & resources intensity			
Legislative Reform Public	*Interception and retention of data in real time*			Increased Legislative Powers

Engagement	*sharing of cybercrime data for intelligence purposes regionally*			
	interception of cybercrime data stored on cloud platforms *(*Saas, Paas, Iaas) – seizure, acquisition and analysis			
	Lawful access and disclosure of digital data among the law enforcement			Adaptive Learning
Learning & Feedback: Continuous Development of National Digital Competences for CIP protection	Learning from failures, receptivity to learning, & learning from best practices			