A Cyber Counterintelligence Competence Framework

Thenjiwe Sithole and Jaco Du Toit
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
thenjiwes@icloud.com
jacodt@uj.ac.za

Abstract: The increased use of cyberspace and technological advancement are fundamentally changing the cyber threat landscape. Cyberattacks are becoming more sophisticated, frequent, and destructive. Internationally, there is a growing acceptance that Cyber Counterintelligence (CCI) is essential to counter cyber-attacks optimally. Therefore, in addition to government intelligence and security agencies, more companies are incorporating a CCI approach as a critical element of their posture for engaging cyber threats. However, the successful adoption of a CCI approach depends on the availability of skilled CCI professionals equipped with the requisite competences. The creation of such CCI professionals, in turn, requires a framework for developing the necessary CCI competences. At least in as far as reviewed academic literature is concerned, there is no existing postulation on a framework to develop the CCI competences, specifically for developing countries. Given the complexity and multi-disciplinary nature of the emerging CCI field, such a framework needs to provide two distinctive skillsets linked to CCI's two distinct areas of expertise, namely cyber (security) and counterintelligence. The paper presents a high-level Cyber Counterintelligence Competence Framework (CCIC Framework) that outlines dimensions of CCI, functional areas, job roles and requisite competences (knowledge, skills, and abilities), and tasks for each CCI job role. The CCI framework also outlines five levels of proficiency expected for each job role. The identification of competences and levels of proficiency are integral to the successful implementation of the framework and workforce development. The CCIC Framework is intended to be used as a tool to retain, assess, and monitor knowledge, skills, and abilities for CCI workforce development. In addition, the CCIC Framework can be used to assist in providing the basis for individual performance management, education, training, and development pathway, as well as career progression. Therefore, this paper presents a CCIC Framework which is an overarching, integrative construct that synergistically combines different components required to develop a competent workforce for the emerging field of CCI.

Keywords: cyber counterintelligence, cyber counterintelligence job roles, competence framework, proficiency levels, cybersecurity

1. Introduction

Hyperconnectivity, sharing of big data and information at high speed and in real-time, amongst other things, is the order of the day in today's world shaped by cyberspace and inevitable advanced technologies. Therefore, this implies cyberspace and advanced technologies are fundamentally and increasingly integrating into the global population, positively changing the way people live and communicate with one another and improving the quality of services in organisations (Li & Liu, 2021; Petrillo, et al., 2018). In 2020 the world experienced an unprecedented acceleration of internet connectivity due to the novel Covid-19 pandemic (ITU, 2021). Public and private sector organisations and educational institutions had to rethink, adapt, and accelerate the use of technology and cyberspace, in magnitude, for remote working and teaching and learning.

Certainly, cyberspace and technology advancement bring opportunities, but at the same time, they come with cyber risks, fundamentally changing the cyber threat landscape. There has been an unprecedented increase in cyberattacks, which are becoming frequent, complex, on a large scale, destructive and stealthy, with cyber attackers becoming more efficient (Meier, et al., 2021; Check Point, 2018). State and non-state actors continuously leverage disruptive technologies to develop advanced and sophisticated tools for expediting their efforts in conducting cyber espionage, cyber warfare, cyber-surveillance, or cybercrime (Public-Private Analytic Exchange Program, 2019). These actors may launch attacks on any private and public organisation globally.

Conventional cybersecurity alone is no longer sufficient and effective. The recent events of unprecedented cyberattacks should highlight the significance of new thinking on countering these cyberattacks and cyber risks. Therefore, in this increasingly hyperconnected cyber world, it is imperative for organisations to adopt a proactive approach in responding to cyber risks, preventing cyberattacks before they even happen and protecting their critical information systems. More particularly, the threat landscape, in which threat actors of various types have expanding intelligence capabilities, is underlining the need for organisations to incorporate counterintelligence (CI) – and thus cyber counterintelligence (CCI) - as part of their security approaches (Duvenage et al., 2020a; Duvenage & von Solms, 2015; Jelen, 2020). Duvenage (2019) defines CCI as "the subset of multi-disciplinary CI

aimed at deterring, preventing, degrading, exploiting and neutralising adversarial attempts to collect, alter or in any other way to beach the C-I-A of valued information assets through cyber means."

This paper introduces a high-level outline of the cyber counterintelligence competence (CICC) Framework and its constituents. The CCIC Framework is an overarching, integrative construct that combines different constituents required to develop a competent workforce for the emerging field of CCI.

This paper is structured as follows: Section 2 motivates for development of the CCIC Framework. Section 3 introduces the CCIC Framework structured into four elements: Dimensions, Functional Areas, Job Roles, and Competences (knowledge, skills, abilities, and attitude). The section also presents five levels of proficiency required for each job role. Section 4: provides a conclusion on the proposed CICC framework.

2. Motivation for developing the CCIC framework

CCI is a developing field gaining ground internationally (Duvenage, et al., 2020a). Therefore, more and more companies are implementing a CCI approach as part of their endeavour to engage and neutralise proliferating threats. This escalating trend is increasingly pushing the availability of a skilled CCI workforce equipped with the necessary capabilities to the centre. However, the CCI field lacks the fundamental body of knowledge relating to a professional and capable workforce, such as describing and understanding the requisite CCI competences (Duvenage, et al., 2020b; Duvenage, et al. 2019; Black, 2014). A review of the CCI industry and peer-reviewed academic research - conducted for the purposes of this paper - found no existing CCI framework explicitly referring to the requisite competences (knowledge, skills, and attitude) for CCI workforce development in the consulted literature. As substantiated in further paragraphs of this section, identifying such competences is a critical requisite for developing a CCI capable workforce and is thus a defining feature of the CCIC Framework.

Note should be taken that literature shows the two similar terms – "competency" or "competence" – being used interchangeably or to define two different concepts. This paper adopts "competence" for consistency and to avoid confusion.

Competence can be defined as a demonstrated ability to apply relevant characteristics for achieving recognisable performance to the levels of a set appropriate standard and can be improved through continuum education, training and development (Apollo Education Group, 2015; CWA, 2014). Within the context of this definition, 'characteristics' refer to applicable knowledge, skills, and attitudes. In further elucidating the definition, 'standard' denotes the degree of proficiency required for different competences or job roles. Proficiencies, in turn, can be a valuable tool for career planning and career pathing (Griffiths & Washington, 2015).

The identification of CCI competences will assist organisations in determining the kind and level of capabilities required for the CCI workforce to execute their jobs effectively. Therefore, it is essential to correctly identify such CCI competences as they are paramount to elevating performance in countering escalating cyber threats and incidents. CCI competences will differ according to assigned job roles and different levels of employment (i.e., CCI Execution levels: strategic, operational, and tactical) (Kansal & Singhal, 2018). CCI competences are based on the CI and CCI dimensions, CI categories as well as CI functions (Prunckun, 2019; Stech & Heckman, 2018; Duvenage & von Solms, 2014; Kuloğlu, et al., 2014; US Army Publishing Directorate, 2009) and blend with other relevant cybersecurity competences. The next session will provide an overview of the CCIC Framework.

3. Overview of the CCIC framework

CCI is becoming a significant part of combating cyber risks and cyber-attacks. Therefore, A CCIC Framework is essential for the development CCI workforce. The notion of CCI is multi-disciplinary and incorporates two distinct fields of expertise – Cyber security and CI. Therefore, effective CCI depends on the two corresponding distinctive skillsets of cyber security and CI (Black, 2014). The CCIC Framework is aligned to the underlying four dimensions/categories of CI and CCI Framework: defensive, offensive, active, and passive. This section will expound these as dimensions of the underlying structure that underpins the CCIC Framework's other elements.

Governments and the private sector have developed several cybersecurity skills frameworks to improve cybersecurity practices, providing a comprehensive range of cybersecurity roles, tasks, and competences. However, none of the frameworks explicitly make mention of the CCI and CCI competence or skills or workforce development. The concept for CCIC Framework takes inspiration from international frameworks such as the NIST

NICE Cybersecurity Workforce Development Framework, CyBOK, Skills Framework for the Information Age (SFIA) and Chartered Institute of Information Security (CIISec) Skills Framework, but it is modified to highlight CCIC (SFIA, 2021; CyBOK, 2019; NIST, 2017; CIISEC (IISP), 2010).

The CCIC Framework is a construct that comprises four elements: dimensions, functional areas, job roles, competences (knowledge, skills, abilities, and attitude) and tasks. The CCIC Framework is organised into four dimensions, which is an overarching structure of the CCIC Framework. Each CCI dimension comprises one or more CCI Functional Areas. Each CCI functional area has various associate job roles. Each job role has associated competences and numerous tasks. The relationship between the elements of the CCIC Framework is depicted throughout this section. The mapping of the framework *per* four elements considers, but further evolves and adds to, notions advanced in the international frameworks cited in the previous paragraph. Figure 1 illustrates an overview of the CCIC Framework showing these four elements. Each of these elements is discussed in sections 3.1 to 3.4.

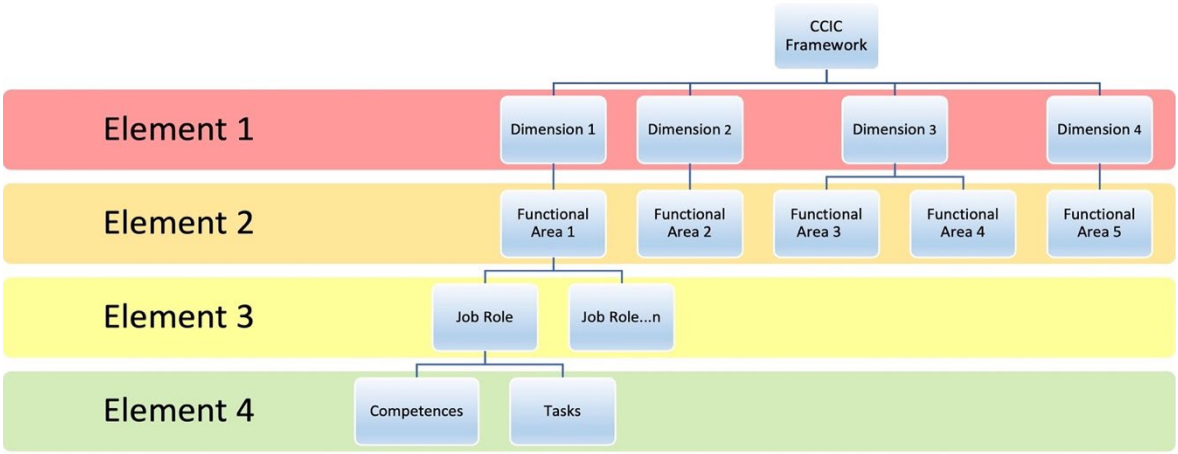

Figure 1: An overview of the CCIC Framework

3.1 Element 1: Dimensions

Element 1 provides an underlying structure of the CCIC Framework, referred to as Dimensions. As mentioned earlier in this section, the CCI incorporates two distinct fields, CI and cybersecurity. Basically, CCI uses CI principles, concepts, and functions within the cyberspace. Therefore, the CCI dimensions are derived from the two fundamental categories of CI, defensive CI and offensive CI (Prunckun, 2019; Sims, 2009).

Defensive CI/CCI applies the detection and deterrence techniques to deny access and collect information on espionage threats (Prunckun, 2019; Duvenage & von Solms, 2014). Defensive CCI is concerned about preventing the adversaries' endeavour from penetrating the organisation's information systems and, at the same time, collecting intelligence against the adversaries and minimising the threat landscape. An example of defensive CCI is performing vulnerability assessments and threat analysis (Lee, 2015). The offensive CI/CCI applies techniques to detect, deceive, and neutralise espionage threats and covert threats (Prunckun, 2019; Duvenage & von Solms, 2014). Offensive CCI is concerned about detecting and directly gathering intelligence about adversaries' covert, espionage, or cyber operations or deceiving and manipulating them. This can be done inter alia by creating honeypots containing files with misinformation (Lee, 2015).

The defensive CI and offensive CI can be implemented in both passive and active measures. Thus, formulating the four CI dimensions - active defensive, passive defensive, active offensive, and passive offensive (Prunckun, 2019; Stech & Heckman, 2018; Duvenage & von Solms, 2014; Sims, 2009; US Army Publishing Directorate, 2009). The dimensions are also derived from various conventional defensive and offensive cybersecurity processes and procedures (Jaquire, et al., 2018). The four CI/CCI dimensions are illustrated as quadrants in Figure 2.

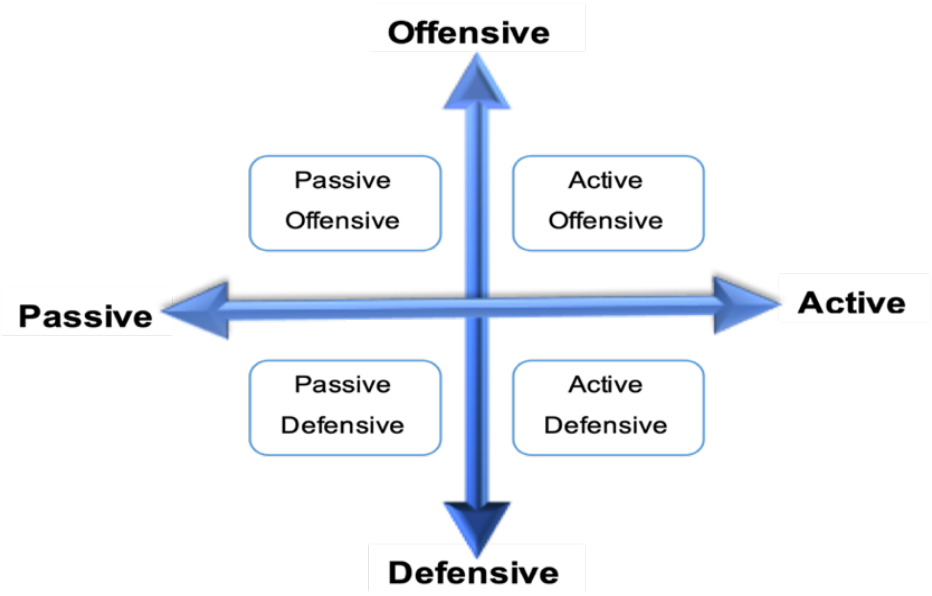

Figure 2: The four dimensions of CCI (Duvenage & von Solms, 2014; Sims, 2009)

As depicted in Figure 2 that both defensive and offensive CI/CCI have passive and active modes. These four dimensions can be explained in tabulated format (Table 1) as follows:

Table 1: Four-sector counterintelligence matrix (Duvenage, et al., 2020a)

Passive Defensive	**Active Defensive**
Denies the adversary access to information through physical security measures and other security systems and procedures.	The active collection of information on the adversary to determine its sponsor, modus operandi, network, and targets. Methods include physical and electronic surveillance, dangles, double agents, moles, and electronic tapping
Passive Offensive	**Active Offensive**
Reveals selected information to the adversary. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.	The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through, for example, double agents and moles. Active offensive CI could include some forms of covert action.

The identification of the four dimensions forms the first element of the CCIC Framework – passive defensive, active defensive, passive offensive, active offensive and is graphically depicted in Figure 3.

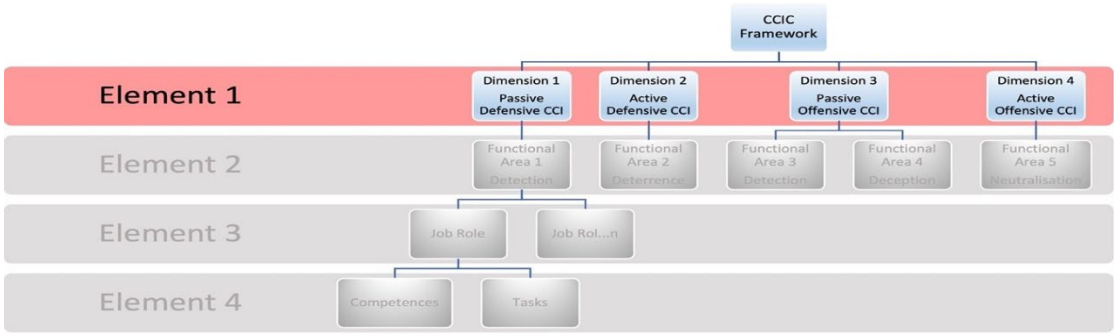

Figure 3: Element 1 of the CCIC framework - the four dimensions

3.2 Element 2: Functional areas

The four dimensions mentioned above have one or more associated functional areas. The functional areas are underpinned by the principles of CI to accomplish CI missions. The principles are detection, deterrence, deception, and neutralisation (Stech & Heckman, 2018). Mapping the dimensions with the principles, defensive CCI is concerned with detection and deterrence, whereas offensive CCI is concerned with detection, deception, and neutralisation (Prunckun, 2019; Stech & Heckman, 2018). The four CCI dimensions and the identified corresponding functional areas form the second element of the CCIC Framework illustrated in Figure 4.

- Dimension 1: Passive-defensive CCI
- *Functional Area1: detection*
- Dimension 2: Active-defensive CCI
- *Functional Area 2: deterrence*
- Dimension 3: Passive-offensive CCI
- *Functional Area 3: detection*
- *Functional Area 4: deception*
- Dimension 4: Active-offensive CCI
- *Functional Area 4: neutralisation*

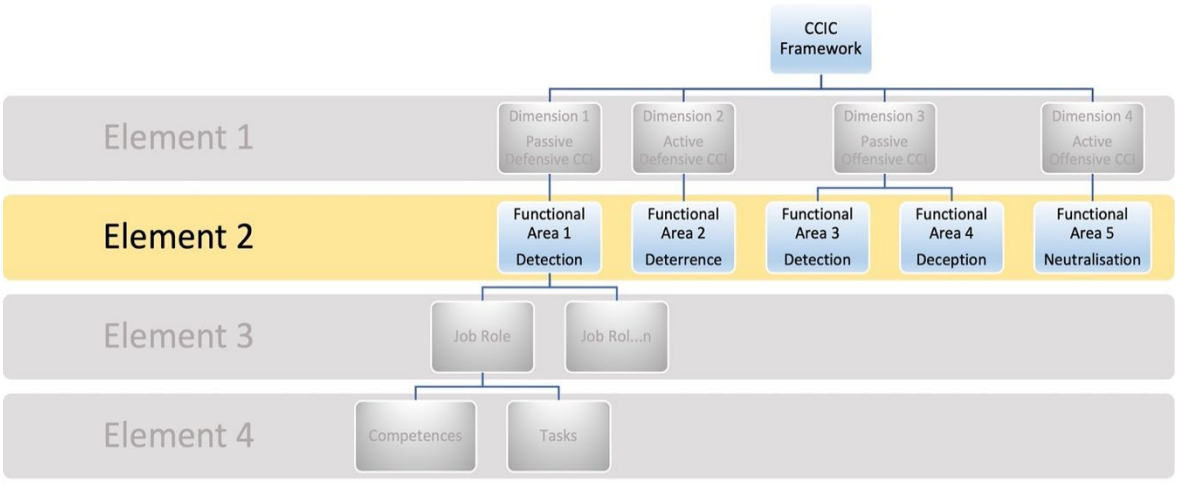

Figure 4: Element 2 of the CCIC framework - the five functional areas

*3.2.1 Functional Areas 1 and 3: Detection**

To discover the existence of any cyber activities, anomalies and threats targeting the information systems and associated compromise or possible compromise of the confidentiality, integrity, and availability of the information systems. Prunckun (2014) offers five premises that include the detection principle, and for the objective of this paper, identified as the following abilities:

- 1.Ability to identify the cyber event, activity or incident of concern;
- 2.Ability to identify the person(s) who are involved in the event;
- 3.Ability to identify the organisational association of the person(s) of interest;
- 4.Ability to identify the current location of the person(s) of interest; and
- 5.Ability to gather the facts that indicate that the person(s) committed the event, activity or incident.

*Cyber detection constitutes a functional area within Passive Defensive (Functional Area 1) and Passive Offensive CCI (Functional Area 3). In both these areas, 'cyber detection' has the same meaning and requires the five premises stated above. For this reason, Functional Area 3 is not discussed in a separate subsection. Detection under passive defensive is reactive, the process of identifying or discovering occurrences of CCI events has no

human interaction, and it is not in real-time. In contrast, detection under passive offensive is proactive and there is real-time human interaction and information gathering or actively hunting for threats to learn from and respond to the adversary.

3.2.2 Functional Area 2: Deterrence

Deterrence is the ability to dissuade an adversary from attempting intrusive cyber operations on information systems or by preventing an adversary from conducting cyber intelligence by ensuring that the adversary perceives the risks and costs of their action outweighing the benefits or that the advantages they expect (Soesanto & Smeets, 2020; Jensen, 2012). Deterrence is active defensive because it proactively stops adversaries before they can achieve their objectives. Deterrence can be achieved through (Prunckun, 2019; Jensen, 2012):

- 1. Deterrence by punishment – that is, threatening to retaliate, an organisation must be able to conduct an attack back on its adversary.
- 2. Deterrence by denial – that is, discouraging the adversary and denying the benefits of an attack. This approach must be perceived by an adversary and must look credible to succeed.

3.2.3 Functional Area 4: Deception

Deception is used to mislead and confuse the adversary about operations, capabilities, intentions, plans or vulnerabilities through manipulation, distortion, or falsification to make them believe what is fabricated, is accurate and make them either take action or not so that these actions prove ineffective (Prunckun, 2019; Heckman, et al., 2011). Deception is a passive offensive measure as it can deliberately mislead an advisory and conceal certain information from the adversary.

3.2.4 Functional Area 5: Neutralisation

Neutralisation renders the adversary's cyber activities and capabilities inactive, failure, collapse. Stech & Heckman (2018) assert that neutralisation of adversary cyber activities can be achieved by “destruction, paralysis, loss of interest or loss of confidence that collection will be able to achieve its objective”. Neutralisation is active offensive because it proactively and in real-time counteract or destruct an adversary's activities.

3.3 Element 3: Job roles

Sections 3.1 and 3.2 gave an overview of the first two elements of the CCIC Framework. These two elements, the Dimensions, and the Functional Areas, are the foundation for identifying Job Roles aligned to the CCI approach. That is, each Functional Area has corresponding Job Roles. Furthermore, each Job Role has a job title, job purpose, levels of proficiency and associate competences (knowledge, skills, abilities, attitudes (KSA), and tasks required for optimal performance of the role. The third element of the CCIC Framework is illustrated in Figure 5.

3.3.1 Job role

The term ‘job role’ denotes a detailed grouping of related jobs consisting of competences (knowledge, skills, and abilities), a group of defined tasks and levels of proficiency required to achieve the job role. The job role has the following components:

- Job title – means the name used to refer to a particular job.
- Job code – a unique code identifier used to reference the job
- Job purpose – comprises an overview of what the job entails: the primary purpose and objectives of the job.
- Tasks – a detailed, specific list of primary responsibilities needed to be performed for the job role.
- Level of proficiency – description of the levels of proficiency required for each job role for tasks and competences.
- Competences – a detailed list of all competences that will be required to carry out the tasks.

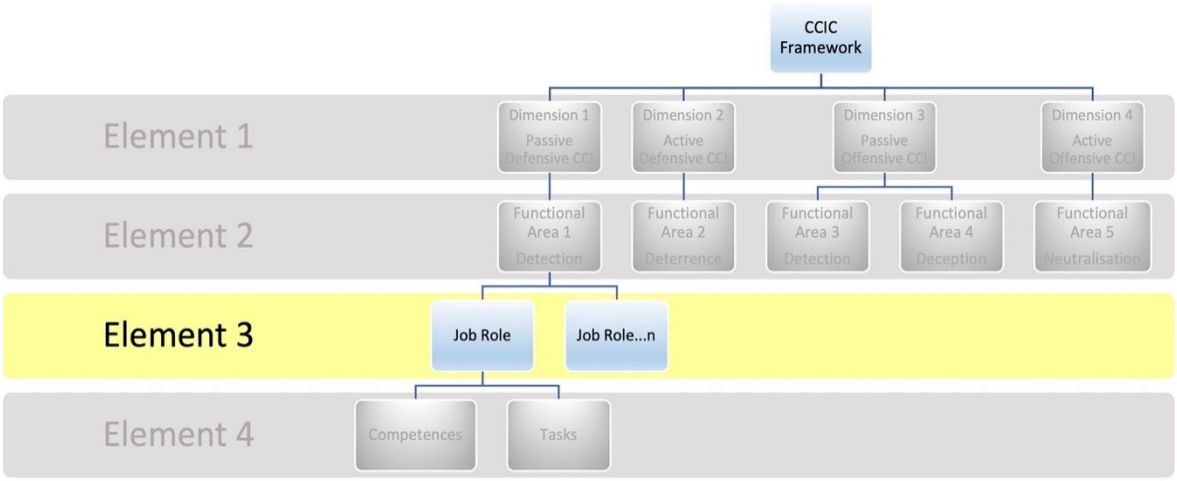

Figure 5: Element 3 of the CCIC framework - the job roles

3.3.2 Levels of proficiency

Levels of proficiency describe an individual's level of expertise for a particular job role. The levels of proficiency are essential for the successful implementation of the CCIC Levels of proficiency. Furthermore, proficiency levels represent the degree of the development of competences and the complexity of the tasks (Carretero, et al., 2017). The levels of proficiency are defined per competence per each job role. The CCIC Framework proposes five levels of proficiency described in Table 2. The levels of proficiency presented in Table 2 draw from those advanced in some other frameworks (SFIA, 2021; Bashir & Miyamoto, 2020; Department of Higher Education and Training, 2016; United Nations Population Fund, 2003)

Table 2: Five levels of proficiency

Proficiency Level	Description
Level 1: Awareness - All employees, including management	The learning point involves being cognizant or knowledgeable of the field and the required skills without practical experience. Follow instructions or others.
Level 2: Foundation - Junior Practitioner	Acquired basic knowledge and understanding. Ability to assist, demonstrate or apply basic knowledge and skills for comprehensible tasks. Work under the direct supervision and focus on enhancing knowledge and skills.
Level 3: Intermediate - Practitioner	Ability to apply knowledge and skills to basic tasks without supervision and complex tasks with limited supervision. Ability to work independently.
Level 4: Advanced - Senior Practitioner	Acquired a deep understanding of the knowledge associated with the skill. Ability to apply advanced knowledge and skills in a range of complex tasks with no supervision. Capable of leading, advising, initiating, and influencing any task. A seasoned practitioner with a track record and the ability to make decisions and take responsibility.
Level 5: Specialist /expert	Acquired broad and deep knowledge, skills, and experience to apply in extensive and diversified circumstances. Deep understanding of the implications associated with the field and industry. Has authority and is accountable for all functions and decisions. Lead, advise, initiate, and influence implementations, innovations, transformation, and developments. Has a sustained track record that leads to extensive recognition in the field and industry.

3.4 Element 4: Competence and tasks

The last element of the CCIC Framework provides an overview of the competences (knowledge, skills, abilities, and attitudes - KSA) and the tasks required to perform a specific job role. Numerous specific tasks need to be completed in a particular job role. The element is also about identifying competences (KSA) required to execute tasks within a particular CCI job role and deliver superior performance. The competences are acquired through learning and development. Competences for each job role can be used as a guideline to design and develop competence-based education, training and development curriculum required to be competent in the job role (Parsona, et al., 2018). To achieve effective performance: cognitive competence, functional competence, social

competence are the guide in identifying or developing a set of competences (KSA) for each job role. This relation can be expounded as follows:

- Knowledge: relates to the set of cognitive competences required for a specific job role in conjunction with the ability to apply the knowledge effectively. Knowledge (theoretical, facts, concepts, and information) must be known and understood to accomplish job roles and tasks effectively.
- Skills: pertains to the set of functional competences required to execute the tasks of the specific job role effectively, and the tasks can be effortlessly demonstrated. Skills are about how to use the knowledge gained.
- Attitude: denotes an individual's mindset to execute and yield outstanding performance. Attitudes refer to an individual's way of thinking, belief, or feeling that they can use knowledge and skills gained to perform tasks effectively. Attitude relates to social competences and influences ability, motivation, commitment, confidence, responsibility, performance, and adaptability.

To have outstanding performance and a competent workforce requires complete continuous integration of these three competences. The cognitive and functional competences correspond to the professional aspect, as they are about the functional expertise in the job role. Social competence corresponds to the personal aspect as they have to do with personal attitude, behavioural traits, and motives (Arifin, et al., 2017).

The addition of competence and tasks, is the fourth element that completes the CCIC framework, is graphically depicted in Figure 6.

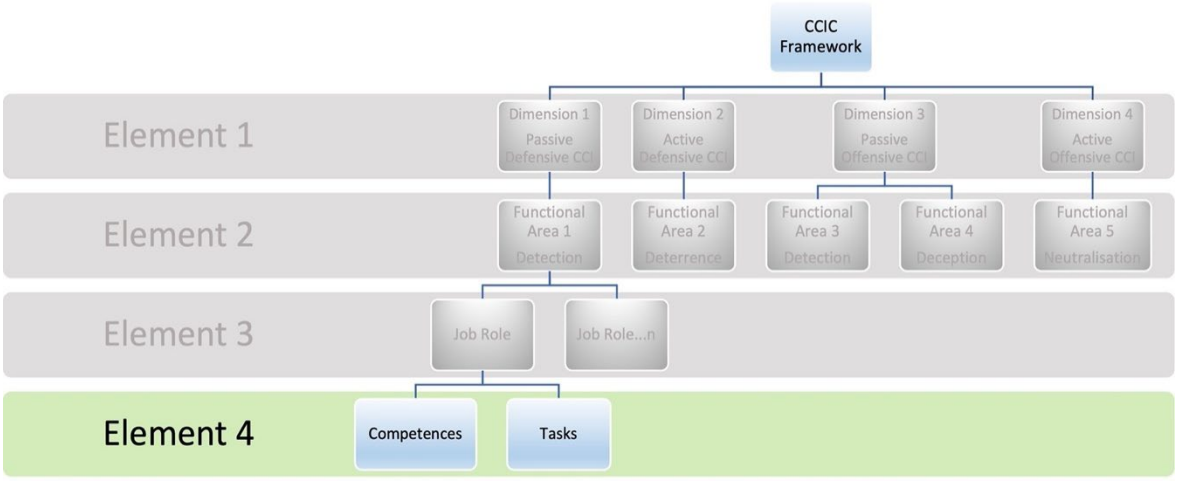

Figure 6: Element 4 of the CCIC Framework - competences and tasks

This section presented an overview of the CCIC Framework, a construct of four elements. These elements have a symbiotic relationship to achieve effective performance, and each element is integral to the successful implementation of the CCIC Framework. The four elements are Dimensions, Functional Areas, Job Roles, and Competences (KSA) and Tasks.

4. Conclusion

Cyber counterintelligence is gaining momentum in both the public and private sectors. A skilled workforce is required for the effective execution of CCI to counter advanced and unprecedented cyber threats. A comprehensive competence framework is essential for CCI workforce development at all CCI employment or execution levels to create such a skilled workforce.

This paper gave an essential introduction to the CCIC Framework and outlined four elements. The first and second elements have been identified using the four principles of CI. Subsequently, the CCIC Framework was progressed and expanded with the addition of job roles (element three) as well as competences and tasks (element four). Ongoing research is focused on detailing all of the CCIC frameworks elements. The CCIC Framework can be implemented by any type and size of a public or private sector organisation. The CCIC Framework will assist in identifying competence gaps, designing and developing competence-based education, training, and

development curricula, providing career progression guidance, and developing CCI practitioners with the requisite knowledge, skills, and attitude for optimising CCI performance. Future research will explore the following job roles, task analysis and competence, and legal ramifications of attacking back and neutralisation.

Acknowledgements

This research benefitted, in part, from support from the Faculty of Science at the University of Johannesburg.

References

Apollo Education Group, 2015. Competency Models for Enterprise Security and Cybersecurity Research-Based Frameworks for Talent Solutions, University of Phoenix: Apollo Education Group, Inc..

Arifin, M. A., Rasdi, R. M., Anuar, M. A. M. & Omar, M. K., 2017. Addressing Competency Gaps for Vocational Instructor through Competency Modelling. International Journal of Academic Research in Business and Social Sciences, 7(4), pp. 1201-1216.

Bashir, S. & Miyamoto, K., 2020. Digital Skills: Frameworks and Programs, Washington: International Bank for Reconstruction and Development / The World Bank.

Black, J. M., 2014. The Complexity of Cyber Counterintelligence Training, Unpublished Thesis Submitted for Master of Science in Cybersecurity, Utica, New York: Utica College.

Carretero, S., Vuorikari, R. & Punie, Y., 2017. DigComp 2.1 The Digital Competence Framework for Citizens With eight proficiency levels and examples of use, s.l.: Luxembourg: Publications Office of the European Union.

Check Point, 2018. the Generation Cyber Attacks are Here and Most Businesses are Behind: A New Model For Assessing and Planning Security. [Online] Available at: https://www.checkpoint.com/downloads/product-related/whitepapers/preventing-the-nextmega- cyber-attack.pdf [Accessed 3 December 2021].

CIISEC (IISP), 2010. *IISP INFORMATION SECURITY SKILLS FRAMEWORK.* [Online] Available at: https://apmg-international.com/sites/default/files/documents/products/iisp_skills_framework_v1_0.pdf [Accessed 19 March 2021].

CWA, 2014. European e-Competence Framework 3.0: A common European framework for ICT Professionals in all industry sectors, s.l.: European Committee for Standardization (CEN) Workshop Agreement (commonly abbreviated CWA).

CyBOK, 2019. *The Cyber Security Body of Knowledge Version 1.0.* [Online] Available at: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf [Accessed 19 February 2020].

Department of Higher Education and Training, 2016. Competency Framework for Career Development Practitioners in South Africa, Pretoria: Department of Higher Education and Training.

Duvenage, P. 2019. A conceptual framework for cyber counterintelligence, Unpublished Thesis Submitted for PhD (DCom) in Computer Science, University of Johannesburg, South Africa.

Duvenage, P. & von Solms, S., 2014. Putting Counterintelligence in Cyber Counterintelligence. University of Piraeus, Greece, 14th European Conference on Cyber Warfare and Security.

Duvenage, P. & von Solms, S., 2015. Cyber Counterintelligence: Back to the Future. Journal of Information Warfare, 13(4), pp. 42-56.

Duvenage, P., Jaquire, V. & von Solms, S., 2020a. Cyber Counterintelligence Matrix for Outsmarting Your Adversaries. Journal of Information Warfare, 19(1), pp. 1-11.

Duvenage, P., Jaquire, V. & von Solms, S., 2020b. Counterintelligence: Some Contours towards the Academic Research Agenda. Chester, UK, 19th European Conference on Cyber Warfare and Security ECCWS 2020.

Duvenage, P. Jaquire, V.& von Solms, S., 2019. Towards a literature review on cyber counterintelligence. Journal of Information Warfare, 17(2), pp. 1-12.

Duvenage, P., von Solms, S. & Corregedor, M., 2015. The Cyber Counterintelligence Process - a Conceptual Overview and Theoretical Proposition. University of Hertfordshire, Hatfield, Proceedings of the 14th European Conference on Cyber Warfare & Security, 2-3 July 2015.

Griffiths, B. & Washington, E., 2015. Competencies at Work Providing a Common Language for Talent Management. New York, NY: Business Expert Press, LLC.

Heckman, K. E. et al., 2011. Cyber Denial, Deception and Counter Deception A Framework for Supporting Active Cyber Defense. Advances in Information Security, Volume 64, p. 2011.

ITU, 2021. easuring digital development Facts and figures 2021. [Online] Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf [Accessed 2 December 2020].

Jaquire, V., Duvenage, P. & Solms, S. v., 2018. Building the Ideal Cyber Counterintelligence Dream Team. University of Oslo Norway , 17th European Conference on Cyber Warfare and Security ECCWS 2018. 28 29 June 2018 .

Jelen, S., 2020. Cyber Counterintelligence: When Defense Alone is No Longer Sufficient. [Online] Available at: https://securitytrails.com/blog/cyber-counterintelligence [Accessed 4 July 2020].

Jensen, E. T., 2012. Cyber Deterrence. Emory International Law Review, 26(2), pp. 773-824.

Kansal, J. & Singhal, S., 2018. Development of a competency model for enhancing the organisational effectiveness in a knowledge-based organisation. International Journal of Indian Culture and Business Management, 16(3), pp. 287-301.

Kuloğlu, G., Gül, Z. & Erçetin, Ş. Ş., 2014. Counterintelligence as a Chaotic Phenomenon and Its Importance in National Security. In: Chaos Theory in Politics. Dordrecht: Springer, pp. 178-188.

Lee, R. M., 2015. Cyber Intelligence Part 4: Cyber Counterintelligence From Theory to Practices, s.l.: Tripwire.

Li, Y. & Liu, Q., 2021. a comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, Volume 7, pp. 8176-8186.

Meier, R. et al., 2021. Towards an AI-powered Player in Cyber Defence Exercises. Tallinn, Estonia, 2021 13th International Conference on Cyber Conflict Going Viral.

NIST, 2017. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* [Online] Available at: https://www.nist.gov/file/359276 [Accessed 2 July 2018].

Parsona, L., Childs, B. & Elzie, P., 2018. Using Competency-Based Curriculum Design to Create a Health Professions Education Certificate Program the Meets the Needs of Students, Administrators, Faculty, and Patients. Health Professions Education, Volume 4, pp. 207-218.

Petrillo, A., De Felice, F., Cioffi, R. & Zomparelli, F., 2018. Fourth Industrial Revolution: Current Practices, Challenges, and Opportunities. In: Digital Transformation in Smart Manufacturing. s.l.:BoD – Books on Demand, pp. 1-20.

Prunckun, H., 2019. Counterintelligence Theory and Practice. Lanham, Maryland: Rowman & Littlefield Publishing Group, Inc.

Public-Private Analytic Exchange Program, 2019. Geopolitical Impact on Cyber Threats from Nation-State Actors. Commodification of Cyber Capabilities A Grand Cyber Arms Bazaar. [Online] Available at: https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threatsnation- state-actors.pdf [Accessed 2 July 2020].

SFIA, 2021. *Skills Framework for the Information Age SFIA 8 The framework reference.* [Online] Available at: https://sfia-online.org/en/sfia-8/documentation/sfia-8-the-framework-reference-v8-0-sfiaref-en-210928.pdf/@@download/file/SFIA%208%20The%20frame [Accessed 11 January 2022].

Sims, J. E., 2009. Twenty-first-Century Counterintelligence The Theoretical Basis for Reform. In: J. E. Sims & B. Gerber, eds. Vaults, Mirrors, and Masks: Rediscovering US Counterintelligence. Washington, D. C.: Georgetown University Press., pp. 19-50.

Soesanto, S. & Smeets, M., 2020. Cyber Deterrence: The Past, Present, and Future. In: F. Osinga & T. Sweijs, eds. NL ARMS Netherlands Annual Review of Military Studies 2020 Deterrence in the 21st Century—Insights from Theory and Practice. The Hague: T.M.C. ASSER PRESS, pp. 385-400.

Stech, F. J. & Heckman, K., 2018. Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence. In: Cyber Weaponry, Advanced Sciences and Technologies for Security Applications. Cham: Springer, pp. 13-27.

US Army Publishing Directorate, 2009. Army Publishing Directorate. [Online] Available at: https://armypubs.army.mil/ProductMaps/Pubform/Details.aspx?PUB_ID=85844 [Accessed 2 July 2018].

United Nations Population Fund, 2003. Competency Framework, s.l.: Office of Human Resources United Nations Population Fund.