A Cyber Counterintelligence Competence Framework: Developing the Job Roles

Thenjiwe Sithole, Jaco Du Toit and Sebastian H von Solms
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

thenjiwes@icloud.com
jacodt@uj.ac.za
basievs@uj.ac.za

Abstract: In recent years, there have been intensifying cyber risks and volumes of cyber incidents prompting a significant shift in the cyber threat landscape. Both nation-state and non-state actors are increasingly resolute and innovative in their techniques and operations globally. These intensifying cyber risks and incidents suggest that cyber capability is inversely proportional to cyber risks, threats and attacks. Therefore, this confirms an emergent and critical need to adopt and invest in intelligence strategies, predominantly cyber counterintelligence (CCI), which is a multi-disciplinary and proactive measure to mitigate risks and counter cyber threats and cyber-attacks. Concurrent with the adoption of CCI is an appreciation that requisite job roles must be defined and developed. Notwithstanding the traction that CCI is gaining, we found no work on a clear categorisation for the CCI job roles in the academic or industry literature surveyed. Furthermore, from a cybersecurity perspective, it is unclear which job roles constitute the CCI field. This paper stems from and expands on the authors' prior research on developing a CCI Competence Framework. The proposed CCI Competence Framework consists of four critical elements deemed essential for CCI workforce development. In order of progression, the Framework's elements are: CCI Dimensions (passive-defensive, active-defensive, passive-offensive, active-offensive), CCI Functional Areas (detection, deterrence, deception, neutralisation), CCI Job Roles (associated with each respective Functional Area), and Tasks and Competences (allocated to each job role). Pivoting on prior research on CCI Dimensions and CCI Functional Areas, this paper advances a proposition on associated Job Roles in a manner that is both intelligible and categorised. To this end, the paper advances a five-step process that evaluates and examines Counterintelligence and Cybersecurity Job Roles and functions to derive a combination of new or existing Job Roles required for the CCI workforce/professionals. Although there are several cybersecurity frameworks for workforce development, establishing the CCI Job Roles is specifically based on the expression of the Job Roles defined in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

Keywords: cyber counterintelligence, cyber counterintelligence job roles, counterintelligence functions, cybersecurity job roles.

1. Introduction

The rapid shift in the cyber threat landscape indicates that cyber threats and cyber-attacks in various forms are a peril to technological advances and to the confidentiality, integrity and availability and availability of information systems and critical information infrastructure. Both nation-state and non-state actors are increasingly resolute and innovative in their cyber techniques and operations at a global scale. Cyber-attacks are not only increasing in sophistication, magnitude and quantity, but they are becoming more aggressive (World Economic Forum, 2022). The World Economic Forum on the Global Risks Report for 2023 flagged cyber-attacks on critical (information) infrastructures as one of the top risks possessing considerable global impact (World Economic Forum, 2023).

We are in an era where technological advancement is inevitable; it has created smart cities, the interconnectedness of critical infrastructures through the convergence of information technology and operational technology, and digital services in sectors such as government, healthcare, education, and banking. This is also an era where cyber risks, cyber-attacks and the spread of disinformation are also inevitable. Threat actors are already increasing their capabilities, using artificial intelligence-powered cyber-attacks (Guembea, et al., 2022; Jaber & Fritsch, 2023). There has been a 38% increase in cyber-attacks worldwide in 2022 compared to 2021, with education/research, government/military and healthcare being the most attacked sectors (Check Point Research, 2023). There has also been an increase in cyber disruption of critical infrastructures between 2021 and 2022, with some of the infrastructures targeted by nation-state actors (Microsoft, 2022; Trend Micro, 2022)

These intensifying cyber risks and attacks suggest that cyber capability is inversely proportional to cyber risks, threats and attacks. How, then in this era of complexity, can governments and organisations be resilient and thrive? How can governments and organisations protect the confidentiality, integrity and availability (CIA) of their information systems? It is no longer refutable that traditional cybersecurity measures are not enough. Therefore, this confirms an emergent and critical need for organisations to adopt and invest, predominantly, in

cyber counterintelligence (CCI), which is a multi-disciplinary and proactive measure that can identify, deter, prevent, destruct, exploit and neutralise adversarial attempts to collect, alter or breach the CIA of critical information systems through cyber means (Duvenage & von Solms, 2015).

Although CCI is gaining recognition, CCI is an emerging multi-disciplinary field that lacks a well-defined workforce structure and competences. It is apparent that a competent CCI workforce is needed to counter the escalating cyber-attacks and mitigate the cyber risks. However, there is no work on a clear categorisation of the CCI Job Roles or competences in the academic or industry literature reviewed. Furthermore, from a cybersecurity perspective, it is unclear which Job Roles or competences constitute the CCI field.

Based on the authors' previous research on building a CCI Competence Framework, this paper primarily aims to advance a proposition on CCI Job Roles in an intelligible and categorised manner. The Job Roles are the core of the CCI Competence Framework as they concretise the tasks and the competences required to achieve the organisational CCI agenda, as well as to be used to guide the design of education, training and development programmes.

This paper is structured as follows: Section 2 examines the concept of a Job Role and why it is essential for workforce development. Section 3 outlines and selectively illustrates the approach for identifying and creating the Job Roles for the CCI Competence Framework. This five-step process utilises, but also moves beyond, the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Section 4 concludes the paper by outlining aspects for further research in refining the proposed CIC Competency framework.

2. What is a job role, and is it important?

Prior to exploring the identification of Job Roles, it is crucial to understand what a Job Role is and how it relates to workforce development because it will impact the design of the CCI Competence Framework. Job Roles refer to a comprehensive set of tasks, of which each task is associated with competences (knowledge, skills and abilities) for which someone must perform that role and their capability or competence level to perform the task is determined by the proficiency levels (Neal, et al., 2012). A Job Role has the following fundamental components:

- Job title – means the name used to refer to a particular Job Role.
- Job code – a unique code identifier used to reference the Job Role
- Job purpose – comprises an overview of what the Job Role entails: the primary purpose and objectives of the Job Role.
- Tasks – a detailed, specific list of primary responsibilities needed for the Job Role.
- Level of proficiency – description of the levels of proficiency required for each task and competences of the Job Role.
- Competences – a detailed list of all competences (knowledge, skills and abilities) required to perform the tasks.

A critical component of a well-defined job role is ensuring that organisations have the right people at every level to perform the tasks optimally. The fundamental rationale for job role identification and description is the requirement to identify, recruit, train, develop and retain an appropriately qualified and competent workforce, which is accomplished by describing the whole range of related tasks and competences (knowledge, skills and abilities) that must be performed (Saltz & Grady, 2017). Job roles will also assist education and training institutions in designing and developing relevant programs based on common taxonomy and competences (knowledge, skills and abilities) required for particular job roles in a particular industry (Hajny, et al., 2021).

This section provided an overview of what a job role entails and why a job role is important for a competence framework and workforce development. The following section explains the approach to developing the Job Roles for the CCI Competence Framework.

3. Identifying job roles for the CCI Competence Framework

In this paper, we evaluate and examine counterintelligence, CCI and cybersecurity functions to construct practical, intelligible and categorised new or existing job roles for the CCI workforce /professionals. Prior research by the authors proposed a CCI Competence Framework consisting of four critical elements deemed essential for CCI workforce development. In order of progression, the Framework's elements are CCI Dimensions (passive-defensive, active-defensive, passive-offensive, active-offensive), CCI Functional Areas (detection,

deterrence, deception, neutralisation), CCI Job Roles (associated with each respective Functional Area), and Tasks and Competences (allocated to each job role) (Sithole & Du Toit, 2022). The interlinkages between these elements, dimensions and functional areas are graphically depicted in Figure 1.

In their previous research, the authors identified and defined the first two elements of the CCI Competence Framework, namely CCI Dimensions and CCI Functional Areas (see Figure 1). As Figure 1 also shows, the construct of these two elements aligns with the concept of the four dimensions of counterintelligence (Prunckun, 2019) and the CCI (Duvenage & von Solms, 2014).

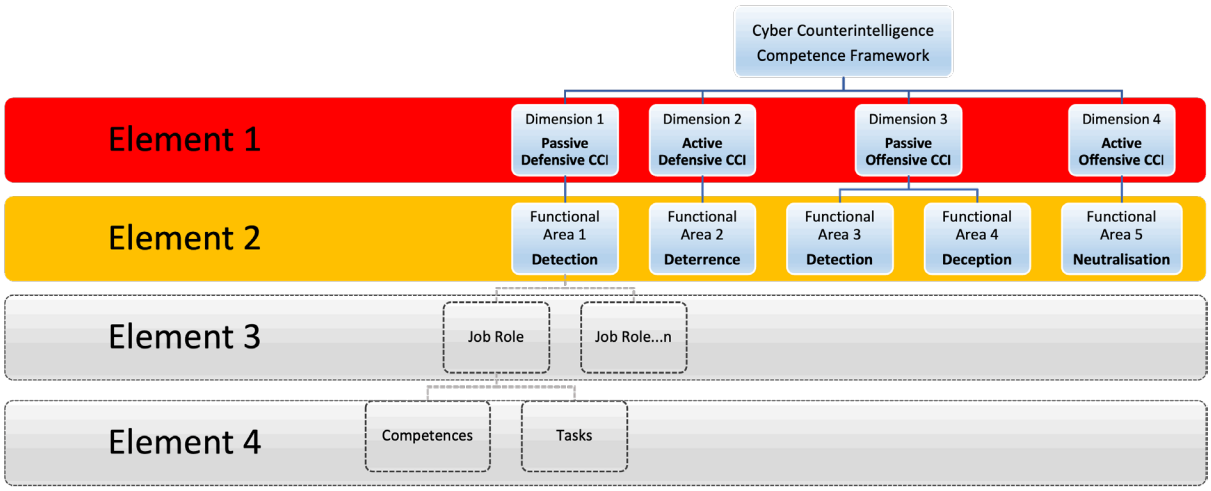

Figure 1: Elements 1 and 2 of the CCI Competence Framework - the Four Dimensions and Five Functional Areas (Source: Sithole & Du Toit, 2022)

The paragraph above demonstrated that two Elements of the CCI Competence Framework (Figure 1) had been developed in preceding research. The rest of this section proceeds with discussing the approach in building Element 3, namely Job Roles. To this end, the following sub-sections outline a five-step process to identify and create Job Roles for the CCI Competence Framework. This process commences with selecting an appropriate cybersecurity framework to use as a reference resource and 'mapping template'.

3.1 Choosing the NICE Framework

To identify the Job Roles, it is crucial to recognise cybersecurity-related skills or workforce development frameworks for their usability and relevance to achieve the objective of this paper. We identified the widely considered NICE framework, which represents the foundation of cybersecurity workforce development, and is also used as a reference source or guide for developing cybersecurity education and training programmes (Furnell, 2021; Hajny, et al., 2021; SPARTA, 2020). The NICE Framework is analysed to identify the Job Roles that are within the broad context of our CI Competence Framework and CI in general.

The NICE Framework is an initiative of the National Institute for Standards and Technology (NIST) as a foundation for cybersecurity education and workforce development. The goal of the NICE Framework is to provide a common, consistent terminology for precise categorisation and description of work roles and their associated tasks, knowledge, skills and abilities needed for cybersecurity work, education and training. (Newhouse, et al., 2017).

As illustrated in Figure 2, the NICE Framework comprises several hierarchal components – Categories, Specialty Areas, Work Roles, Tasks, and Knowledge, Skills and Abilities. The NICE Framework is arranged into seven overarching categories based on a general grouping of cybersecurity functions – Analyse, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Secure Provision. Spread across these categories are 31 Specialty Areas, each having one or more Work Roles. The NICE Framework has 52 Work Roles with several associated Tasks, Knowledge, Skills and Abilities.

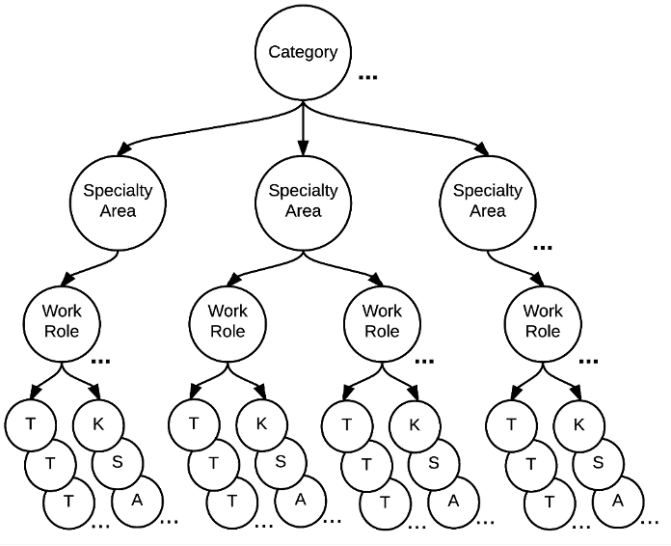

Figure 2: A hierarchical relationship of the NICE Framework components (Source: Newhouse et al., 2017)

The rationale for using the NICE Framework as a basis for identifying the Job Roles for the CCI Competence Framework is that it provides applicable, practical and detailed cybersecurity Work Roles.

3.2 Mapping of the CCI Competence Framework with the NICE Framework

CCI is a subset of CI; therefore, it is essential to note that CCI is underpinned, not only by the four CI dimensions but, also by the functions of CI – CI Analysis, CI Investigations, CI Operations and CI Collection that apply to all the dimensions of CI (Prunckun, 2019). These CI functions will also be applicable to the functional areas of the CCI Competence Framework. Considering the limited research on the CCI field in general and the blurriness of cybersecurity skills/workforce frameworks on which Job Roles and competences constitute the CCI field, the CI functions will assist when identifying the Job Roles during mapping with the NICE Framework. In accordance with its dictionary description, we deem "mapping as an operation that associates each element of a given set … with one or more elements of a second set" (Oxford Dictionary of English, 2010).

By mapping the CCI Competence Framework to the NICE Framework, we aim to identify Job Roles that are comparable to the CCI Competence Framework Functional Areas, and the functions (analysis, collection, investigation and operations) and activities (identity, deter, prevent, destruct, manipulate, exploit and neutralise) of CI and CCI. A top-down approach is found to be the most suitable for identifying or creating Job Roles for the CCI Competence Framework through the mapping process. The 5-step mapping process used is depicted in Figure 3, and a detailed description for each step follows.

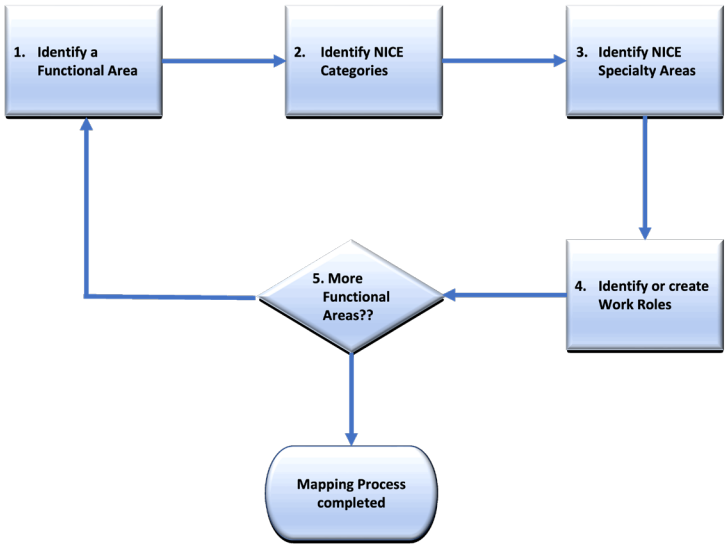

Figure 3: A Job Role mapping process

Step 1 – identify Functional Areas

This step aims to identify the CCI Competence Framework Functional Area and examine its description for mapping with the NICE Framework. However, due to the complexity of CCI and limited information regarding CCI Job Roles, in this step, we determine characteristics that typically identify each Dimension and each Functional Area for ease of reference during the mapping process. These characteristics are extracted from the description, functions, responsibility expectations and goal of each Dimension and its Functional Areas. Therefore, these characteristics are compared to the NICE Framework's Category and Specialty Area, which will be reflected in Step 2.

This paper limits the mapping process of identifying Job Roles to one Dimension and One Functional Area of the CCI Competence Framework. For example, we use Functional Area 5, Neutralisation under Dimension 4 – Active Offensive CCI (see Figure 1) to illustrate the practicality of the mapping steps. The characteristics are determined by the following:

a. The Offensive CCI is concerned with 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)
b. The Active Offensive CCI's ultimate goal is to infiltrate, penetrate, exploit or counterattack the adversary's covert cyber operations. The adversary is likewise provided with disinformation and has its interpretation manipulated (Duvenage, et al., 2020a).
c. Neutralisation is about conducting CCI activities that render the adversary's cyber activities and capabilities ineffective, inactive, a failure, and collapse (Stech & Heckman, 2018). 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 proactively, in real-time or immediately after the initial attack, counteracts or destruct an adversary's cyber offensive activities.

As discussed in the first paragraph of this step, Figure 4 shows the identified characteristics for Functional Area 5, Neutralisation, and Dimension 4, Active Offensive CCI extracted from points (a), (b) and (c) above.

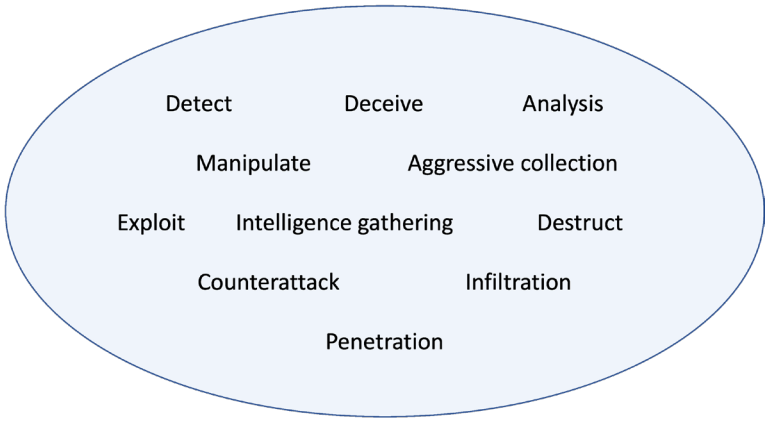

Figure 4: Example of characteristics for the Functional Area 5: Neutralisation [Dimension 4: Active Offensive CCI].

The following step identifies NICE Framework's Category for mapping with CCI Competence Framework's Functional Area.

Step 2 – identify NICE Categories

This step involves examining the descriptions of each of the seven NICE Framework Categories and then comparing them with the Functional Area characteristics identified in step 1 (see Figure 4). The outcome will be categories that have similarities with the characteristics and similar connotations of the descriptions of the Functional Area. For example, the result of this step is two NICE Framework Categories that correspond to the Functional Area 5, Neutralisation, of the CCI Competence Framework:

a. Analyse: performs highly specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence

b. Collect and Operate: provides specialised denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

The next step identifies the NICE Framework's Specialty Area to map with CCI Competence Framework's Functional Area.

Step 3 – identify NICE Specialty Areas

In this step,

a. We analyse and map every NICE Framework Specialty Area for each Category identified in Step 2 to the CCI Competence Framework's Functional Area identified in step 1.
b. Every Specialty Area that has similarities to Functional Area (based on the characteristics identified in Step 1) is selected. For example, the following seven Speciality Areas in Table 1 were identified for mapping Functional Area 5, Neutralisation, to every NICE Framework's Specialty Area.

Table 1: Identified NICE Framework Specialty Areas corresponding to the CCI Competence Framework Functional Area

CCI Competence Framework	NICE Framework Categories/Speciality Areas	
Dimensions/ Functional Areas	**Analyse**	**Collect and Operate**
Active-Offensive CCI: Neutralisation	All-Source Analysis Exploitation Analysis Targets Threat Analysis	Collection Operations Cyber Operational Planning Cyber Operations

Subsequently, the next step will identify relevant Job Roles from the NICE Framework Specialty Areas.s

Step 4 – identify or create Job Roles

This step involves two approaches:

a. Identify Job Roles from the identified Specialty Areas in Step 3 that are relevant to CCI Competence Framework. The mapping is based on examining whether the NICE Framework's Work Role is associated with the CCI Competence Framework's Functional Area, the CI/CCI functions (analysis, collection, investigation and operations) and CI/CCI goal/activities (identity, deter, prevent, destruct, manipulate, exploit and neutralising). It should be noted that the identified job role through this step is subjected to modification of job role name, code and description so that all CI and CCI taxonomy is reflected to appropriate the adaptation of the CCI Competence objective.
b. Create new Job Roles – this approach involves conducting further analysis of each CCI Competence Framework's Functional Area to determine missing responsibilities, functions or activities to reflect the purpose of the Functional Area and, in a broader sense, the mission of CCI. The creation of the new Job Roles is not yet conducted because they go beyond the scope of this paper.

For example, each Work Role from every identified NICE Framework's Specialty Area (Analyse, and Collect and Operate) is mapped to the CCI Competence Framework's Functional Area 5, Neutralisation, by examining whether the definition of the Work Role is associated with Neutralisation. The outcome of the mapping effort has identified nine relevant Job Roles, as shown in Table 2.

Table 2: Identified NICE Framework Job Roles for the CCI Competence Framework Functional Area Neutralisation (source: Newhouse, et al. (2017))

Category	Speciality Area	Work Role	Work Role description
Analyse	All-Source Analysis	Mission Assessment Specialist	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
		All-Source Analyst	Analyses 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.
	Exploitation Analysis	Exploitation Analyst	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorised resources and analytic techniques to penetrate targeted networks.

Category	Speciality Area	Work Role	Work Role description
	Targets	Target Network Analyst	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
	Threat Analysis	Threat/Warning Analyst	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyses, and disseminates cyber threat/warning assessments
Collect and Operate	Collection Operations	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
	Cyber Operational Planning	Cyber Intel Planner	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronisation, and execution of cyber actions. Synchronises intelligence activities to support organisation objectives in cyberspace
		Cyber Ops Planner	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronisation, and enables integration during the execution of cyber actions.
	Cyber Operations	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.

Based on the mapping results shown in Table 2, Figure 5 presents the nine identified Job Roles relevant for the CCI Competence Framework.

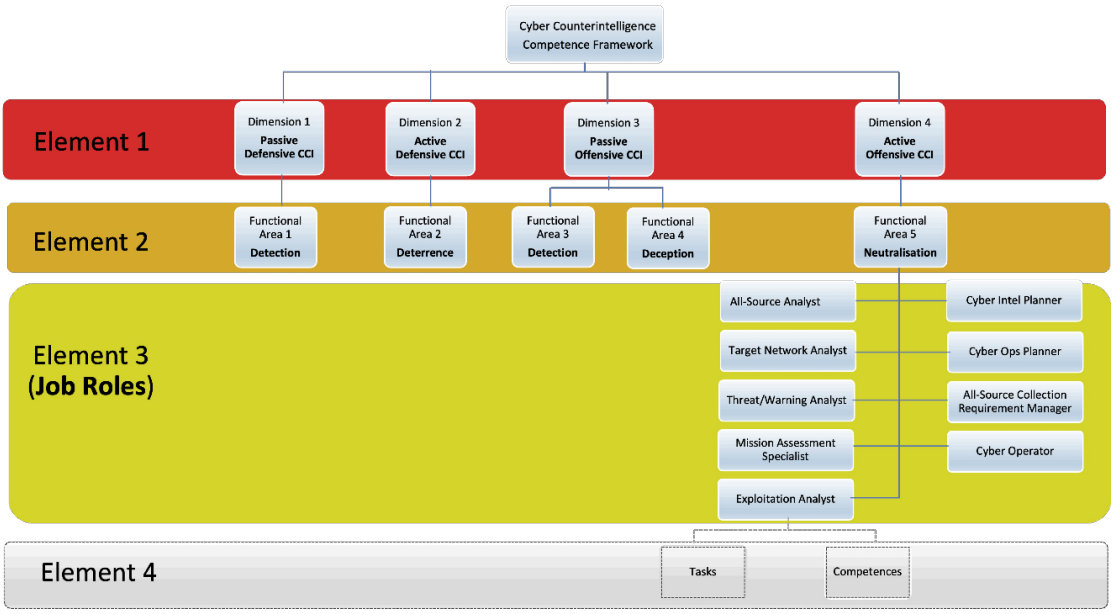

Figure 5: A CCI Competence Framework with Identified Job Roles (Element 3) for the Functional Area Neutralisation

Step 5 – More Functional Areas?

This step repeats the mapping process from Step 1, selecting the next Functional Areas until all Functional Areas are identified and have been associated with Job Roles.

This section presented a 5-step mapping approach for identifying Job Roles for the CCI Competence Framework.

For the purpose of this paper, the focus was solely on technical Job Roles and other critical determinants of CI and CCI. Owing to the comprehensive process, which goes beyond the scope of this paper, for job role identification and description, Functional Area Neutralisation was used as an example. The results can be

implicitly interpreted as a guideline for defining high-level identification, categorisation and definitions of Job Roles for the CCI Competence Framework.

4. Conclusion

This paper proposed a 5-step mapping process for identifying Job Roles, using a NICE Framework as a base framework. The mapping effort demonstrated the practicability of the relationship between some of the NICE Framework Categories / Specialty Areas and CCI Competence Framework Functional Areas. Although the paper was limited to identifying Job Roles for one Functional Area, nine Job Roles appropriately matched the Functional Area Neutralisation's purpose and functions. Each identified job role can be modified to fit the CCI discipline. The 5-step process allows for creating new Job Roles where Functional Areas' function and purpose are not adequately addressed. In completing the identification of Job Roles for the CCI Competence Framework, the following future work will need attention: (i) modification of identified Job Roles to align with the CCI-specific context, (ii) creation of new Job Roles to ensure that the CCI discipline a pool of requisite Job Roles to counter cyber-attacks, and (iii) for each identified and created job role, provide detailed information of the fundamental components of the job role (job title, job code, job purpose, tasks, level of proficiency and competences (knowledge, skills and abilities).

References

Check Point Research, 2023. *Check Point Research.* [Online] Available at: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ [Accessed 15 January 2023].

Duvenage, P. & von Solms, S., 2014. P*utting 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.

Furnell, S., 2021. The cybersecurity workforce and skills. *Computer & Security ,* Volume 100, p. 102080.

Guembea, B. et al., 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36,(1), pp. e2037254-2378.

Hajny, J. et al., 2021. Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access,* Volume 9, pp. 94723-94747.

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.

Jaber, A. & Fritsch, L., 2023. *Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators.* 249-257, International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

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

Microsoft, 2022. *Microsoft Digital Defense Report 2022 Illuminating the threat landscape and empowering a digital defense.,* s.l.: Microsoft.

Neal, A., Yeo, G., Koy, A. & Xiao, T., 2012. Predicting the form and direction of work role performance from the Big 5 model of personality traits. *Journal of Organizational Behavior,* Volume 33, pp. 175-192 .

Newhouse, W., Keith, S., Scribner, B. & Witte, G., 2017. *NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework..* [Online] Available at: https://www.nist.gov/file/359276 [Accessed 2 July 2018].

Oxford Dictionary of English, 2010. *Oxford Dictionary of English,* s.l.: Oxford University Press.

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

Saltz, J. S. & Grady, N. W., 2017. *The Ambiguity of Data Science Team Roles and the Need for a Data Science Workforce Framework.* Boston, MA, USA,, 2017 IEEE International Conference on Big Data (BIGDATA).

Sithole, T. & Du Toit, J., 2022. *A Cyber Counterintelligence Competence Framework.* Chester, Proceedings of the 21st European Conference on Cyber Warfare and Security ECCWS 2022.

SPARTA, 2020. *Strategic Programs for Advanced Research and Technology in Europe: D9.1 Cybersecurity Skills Framework.* [Online] Available at: https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

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.

Trend Micro, 2022. *A Trend Micro Survey Report The State of Industrial Cybersecurity Prevent supply disruptions and ensure resilient operations,* s.l.: Trend Micro .

World Economic Forum, 2022. *The Global Risks Report 2022, 17th Edition, Insight Report,* Geneva: World Economic Forum.

World Economic Forum, 2023. *The Global Risks Report 2023, 18th Edition, Insight Report,* Geneva: World Economic Forum.