ICCWS 2019

Stellenbosch, South Africa

14th International Conference on Cyber Warfare and Security

Stellenbosch University

28 February -1 March 2019

ISBN 978-1-911218-74-6

90000

9 781911 218746

For further information contact

info@academic-conferences.org

or telephone

+44-(0)-118-972-4148

Eating the Elephant - A structural outline of Cyber Counterintelligence Awareness and Training

Thenjiwe Sithole, Petrus Duvenage, Victor Jaquire and Sebastian von Solms
Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa
duvenage@live.co.za
thenjiwes@icloud.com
jaquire@gmail.com
basievs@uj.ac.za

Abstract: It is widely acknowledged that conventional cyber security solutions alone are wholly insufficient in the face of threats posed by role players such as nation states, criminal syndicates, corporate spies, terrorists, hacktivists and rogue individuals. The securing of cyber space depends not only on raising the bar in respect of defensive measures, but also needs to involve proactive action focussing on threat agents. For organisations with sizable assets, cyber counterintelligence (CCI) offers a practicable approach which combines both the defensive and offensive dimensions. CCI's effective implementation and execution above all requires a coherent organisational awareness and training programme (ATP). For larger organisations, A cyber counterintelligence awareness and training programme (CCI ATP) programme has to be multi-tiered and will typically range from the elementary (e.g. basic cybersecurity awareness and skills training for all personnel) to the advanced (e.g. courses for CCI specialists on the cyber frontlines). The design of such a multi-tiered programme is self-evidently a daunting task and published academic research on this topic is very limited. This proverbial elephant thus needs to be eaten one bite at a time. This paper advances three such first 'bites', namely (i) the conceptualisation and contextualisation of a CCI ATP; (ii) a proposition on the structuring of the CCI ATP's design and implementation process; and (iii) a high-level structuring of a multi-tiered CCI ATP. The multi-tiered CCI ATP we advance in this paper consists of four tiers which are explicated with reference to *inter alia* target group, training objectives and training content. The paper concludes with observations on the CCI ATP research conducted thus far.

Keywords: Cyber security, cyber counterintelligence, offensive cybersecurity, threat intelligence, training.

1. Introduction

Cyber security is a continuously changing and fast growing field which demands of an organisation's work force at all levels to keep up the pace. It is also widely acknowledged that conventional cyber security solutions alone are wholly insufficient to deal with sophisticated and fast-growing cyber risks and threat actors who take advantage of vulnerabilities availed by emerging technologies. There is growing recognition that the security and prosperity of organisations require a more proactive, intelligence-driven approach in mitigating cyber risks. Especially for larger organisations with sizable interests such a proactive approach need to incorporate cyber counterintelligence (CCI). CCI can be defined as measures to "identify, deter, exploit, neutralise and protect against adversarial attempts to collect, alter or in any other way breach the C-I-A [confidentiality, integrity and availability] of valued information assets and where cyber is a principal instrumentality and/or a target" (Duvenage & von Solms, 2013; Duvenage & von Solms, 2015).

CCI's effective implementation and execution above all requires a skilled CCI workforce as well as CCI-conscious employees. Such awareness and skilling is best achieved as part of an organisation's broader CCI awareness, education and training (AET) endeavour. Ideally, this CCI AET endeavour would have a multi-tiered CCI training and awareness programme (CCI ATP) as a main thrust. The design and implementation of a CCI ATP is a daunting task. Factors contributing to the complexity of this task include the following:

- Unclassified information and research on CCI ATP is scarce. This can in part be ascribed to CCI being a relatively new academic field with very limited published academic research on CCI awareness, education and training in general. In as far as surveyed literature is concerned, only two (outstanding and commendable contributions) could be found, namely (Black, 2014; Van Derwerken & Ubell, 2011)
- CCI cuts across multiple disciplines and involves several skillsets. Ideally, CCI ATP would draw an all these disciplines and skillsets – with self-evident implications for the (CCI ATP's) design process.

Sithole, T.G., Duvenage, P.C., Jaquire, V.J. & von Solms, S. H. (2019) 'Eating the elephant – A structural outline of cyber counterintelligence awareness and training' in *Published Proceedings of the 14th International Conference on Cyberwarfare and Security,* Stellenbosch, South Africa, February, pp 396-404

- Organisations differ vastly not only in strategic objectives, but also in their workforces' CCI-relevant skilling and awareness. Therefore, there is no 'one-size-fits-all' CCI ATP. Instead, a CCI ATP's design should be congruent with an organisation's unique features and strategic objectives.

As is clear from the above, the design of a CCI ATP is a proverbial elephant that needs to be eaten one bite at a time. This paper advances three such first 'bites', namely:

- Conceptualisation and contextualisation of a CCI ATP.
- A proposition on the structuring of the CCI ATP's design and implementation process.
- A high-level structuring of a multi-tiered CCI ATP.

In this section we motivated the need for CCI ATP and highlighted some challenges pertaining to the design of such a programme. Subsequently, we introduced the three propositions this paper aims to advance. In the next section, we discuss the first of these propositions, namely CCI ATP's conceptualisation and contextualisation.

2. Conceptualising and contextualising of a CCI ATP

Conceptually, and in practice, an effective CCI ATP is designed with due cognisance of an organisation's (i) strategy, intelligence and counterintelligence efforts and (ii) CCI broader awareness, education and training (AET) endeavour.

An effective CCI ATP is thus not a standalone 'plug in' or 'add on'. An effective CCI ATP is conceptualised and executed as part of the broader organisational CCI awareness, education and training (CCI AET) endeavour. The AET in turn forms part of the wider organisational strategy, intelligence and counterintelligence efforts. This interconnectedness, which will ultimately shape the CCI ATP's design, is graphically depicted in Figure 1:

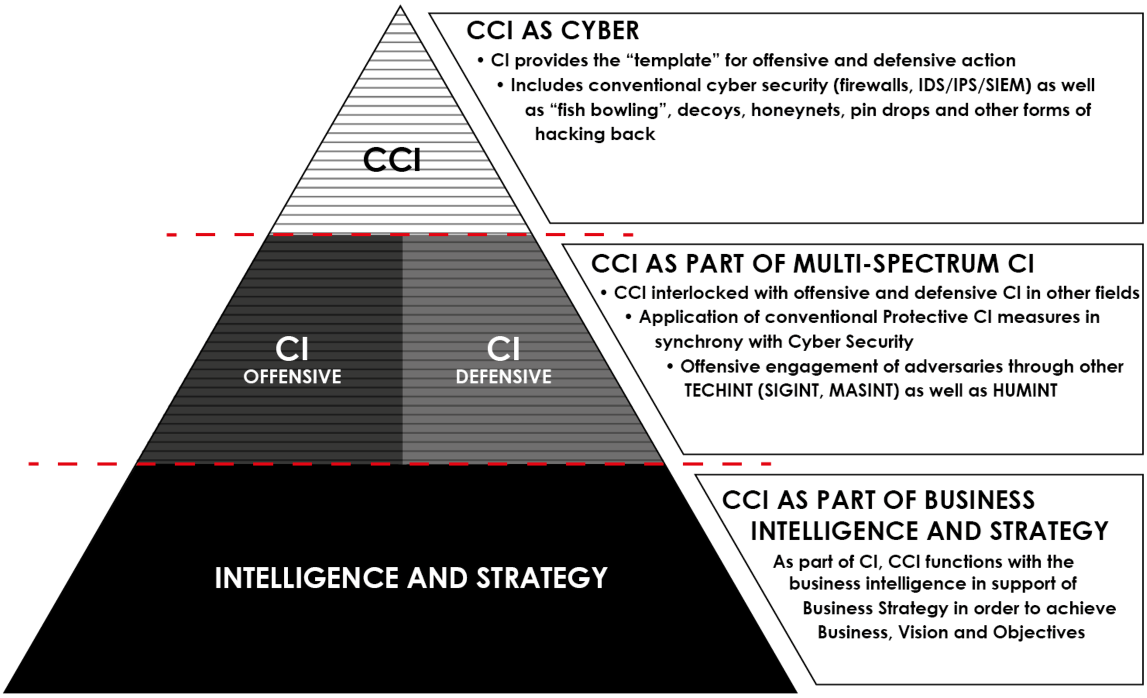
CCI
CI OFFENSIVE
CI DEFENSIVE
INTELLIGENCE AND STRATEGY
CCI AS CYBER
• CI provides the "template" for offensive and defensive action
• Includes conventional cyber security (firewalls, IDS/IPS/SIEM) as well as "fish bowling", decoys, honeynets, pin drops and other forms of hacking back
CCI AS PART OF MULTI-SPECTRUM CI
• CCI interlocked with offensive and defensive CI in other fields
• Application of conventional Protective CI measures in synchrony with Cyber Security
• Offensive engagement of adversaries through other TECHINT (SIGINT, MASINT) as well as HUMINT
CCI AS PART OF BUSINESS INTELLIGENCE AND STRATEGY
As part of CI, CCI functions with the business intelligence in support of Business Strategy in order to achieve Business, Vision and Objectives

Figure 1: CCI three-tiered relationship with Strategy, CI and Cyber *(*Duvenage & von Solms, 2015*)*

Sithole, T.G., Duvenage, P.C., Jaquire, V.J. & von Solms, S. H. (2019) 'Eating the elephant – A structural outline of cyber counterintelligence awareness and training' in *Published Proceedings of the 14th International Conference on Cyberwarfare and Security,* Stellenbosch, South Africa, February, pp 396-404

The design, development and implementation of a CCI AET is typically dependent on objectives described in an organisation's holistic AET policy. CCI AET is further dependent on the expertise of workforce that the organisation already has and the target group, that is, does the organisation has an assigned CCI team? If not, does the organisation need to train the existing counterintelligence (CI) personnel in cyber or existing cyber workforce in CI, or recruit new personnel to be trained in the CI and cyber? In this regard, care should be taken not to confuse CCI as being a duplicate to cyber security. Instead, CCI is a combination of traditional CI and cyber security as well as advanced technical abilities (Black, 2014). Figure 1 shows CCI as being proactive and including offensive dimensions. It is therefore linked with, but goes beyond cyber risk management.

A skilled specialised CCI team alone, however, is insufficient. In fact, most smaller organisations will not have such a dedicated team. In this regard, Jaquire, Duvenage & von Solms (2018) state:

> CCI is not necessarily a separate structure. It is rather a manner for existing and some new functionalities within the organisation to work together in a multi-disciplinary approach to achieve the CCI strategic vision and desired outcomes.

In addition, employees in general remain the weakest link in the organisational armour and continue to be the main reason of data breaches resulting from cyber incidents link (Thomason, 2013; Monk, *et al* 2010; Dtex, 2017). Since it is important that every employee know and understand their roles and responsibilities, a CCI AET has to, at the very least, provide for CCI awareness to all employees regardless of occupational group.

As AETs in general, a CCI AET should thus not be considered as a single, uniform “training” program but as having three different functions, namely 'Awareness', 'Education' and 'Training' (cf. Kissel & Wilson, 2010). Each of these functions differs in target group, specific objectives, outcomes, content and approaches (Kissel & Wilson, 2010). These functions can be differentiated in more detail as follow:

- **Awareness** is about being cognisant or knowledgeable of a situation or one’s surrounding. It is an AET's critical base function - the first line of defence that affords employees with an opportunity to learn about the importance of personal security as well as protecting organisation’s critical information systems assets. The NIST Special Publication 800-16 defines an awareness as “a learning process that sets the stage for training by changing individual and organisational attitudes to realise the importance of security and the adverse consequences of its failure” (de Zafra, *et al*., 1998).

- **Education** is about the facilitation of learning or teaching and the gaining of knowledge. Caballero (2017) defines education as “a formal curriculum created for the purpose of educating individuals in a broad array of security topics that will build a body of knowledge essential for a career in information security” (Caballero, 2017).

- **Training** is about the acquisition of competence (knowledge, skills and attitude) to improve performance and enhance expertise for a specific job or function. Amankwa *et al* (2014) define training as “any endeavour that is undertaken to ensure that every employee is equipped with the information security skills and information security knowledge specific to their roles and responsibilities by using practical instructional methods such as seminars and workshops” (Amankwa, Loock & Kritzinger, 2014)

For purpose of this paper, 'Education' is deemed as a function provided by tertiary and training institutions outside the organisation. Our proposition in this paper, however, centres on an *organisational* CCI awareness and training programme (ATP). The CCI ATP thus *excludes* 'Education' but *includes* 'Awareness' as its first proficiency level. Our CCI ATP then subdivides the 'Training' function in three further proficiency levels namely: fundamental, functional and advanced. These resultant four proficiency levels of our CCI ATP can graphically be depicted as follow:

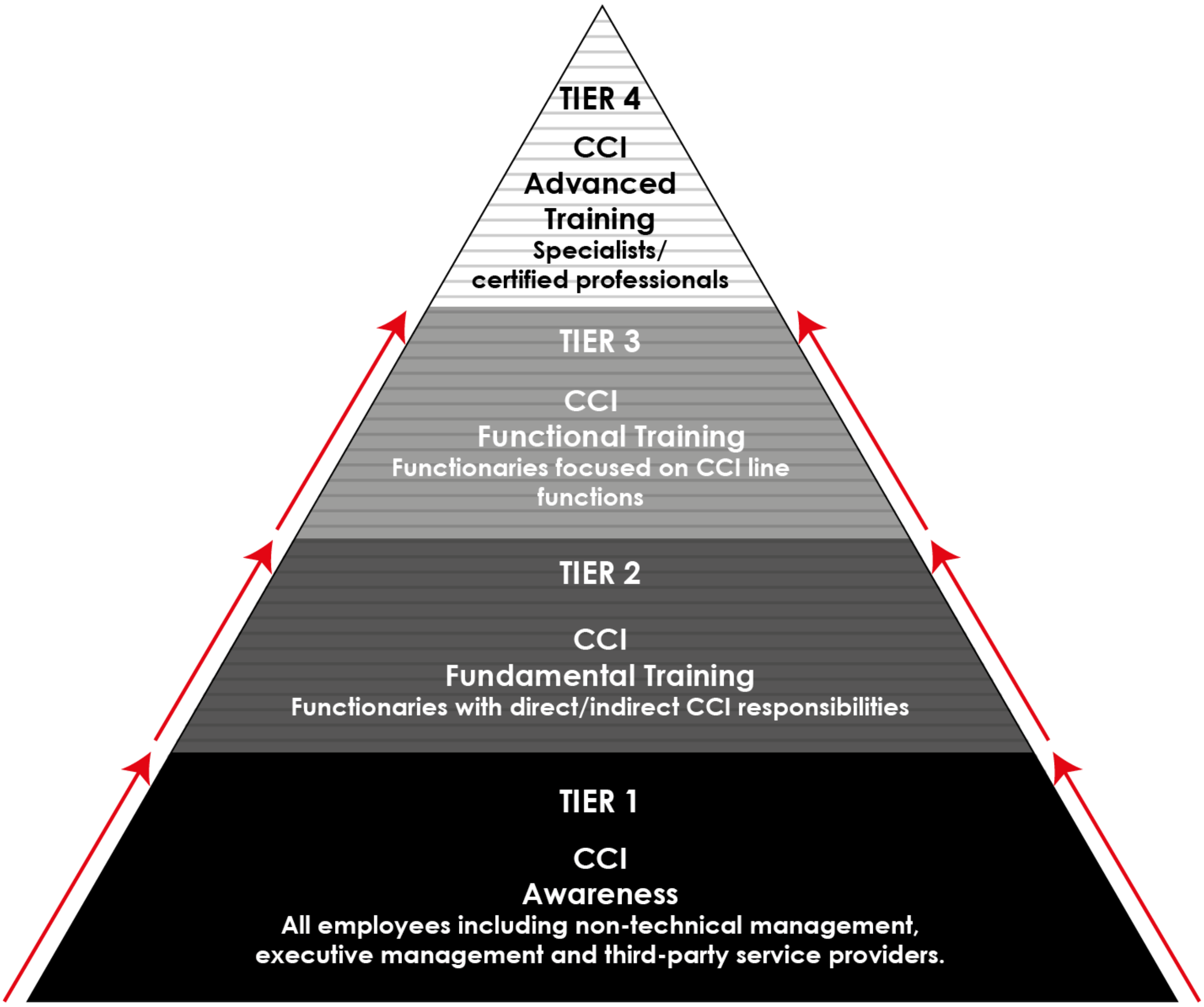
TIER 4
CCI
Advanced
Training
Specialists/
certified professionals
TIER 3
CCI
Functional Training
Functionaries focused on CCI line
functions
TIER 2
CCI
Fundamental Training
Functionaries with direct/indirect CCI responsibilities
TIER 1
CCI
Awareness
All employees including non-technical management,
executive management and third-party service providers.

Figure 2: *Proficiency Levels (Tiers) of a Cyber Counterintelligence* Awareness *and* Training Programme *(CCI ATP) (Authors)*

This section conceptualised and contextualised a CCI ATP as part of organisational strategy and the organisation's broader awareness, education and training (AET) endeavour. This was done to infer the four proficiency levels of a CCI organisational awareness and training programme (CCI ATP). In the next section we advance a structural outline for the process by means of which the CCI ATP can be designed and implemented.

3. Structural Outline of the CCI ATP's Design and Implementation Process

The proficiency levels as discussed in the previous section, provide a scaffold for the design and implementation of a CCI ATP. This design and implementation are done by means of structured process comprising the four steps depicted in Figure 3:

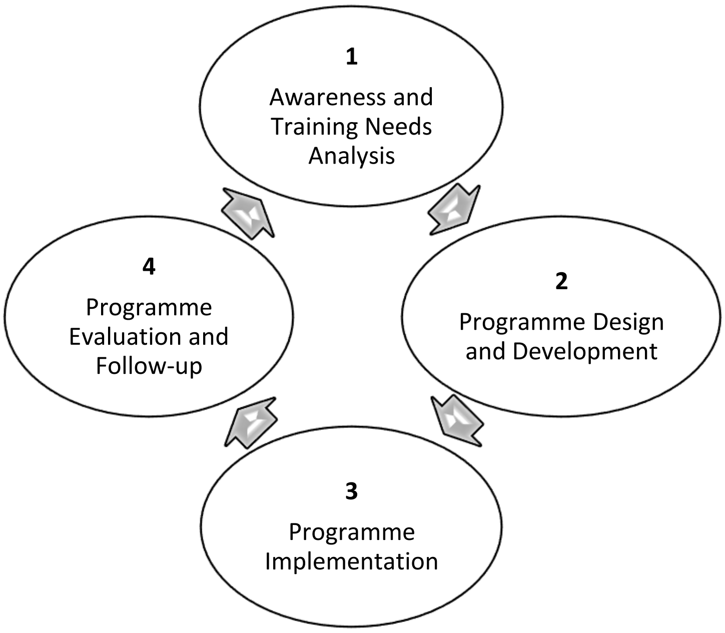
1
Awareness and Training Needs Analysis
2
Programme Design and Development
3
Programme Implementation
4
Programme Evaluation and Follow-up

Figure 3: CCI ATP Design and Implementation Process (adapted from MacCauvlei Learning Academy, 2016)

The four critical steps, depicted in Figure 3, that need to be followed for the CCI ATP's design and implementation, can concisely be described as follow (adapted from MacCauvlei Learning Academy, 2016):

1) An **awareness and training needs analysis** determines the organisation's awareness and training needs according to the strategic objectives. It looks at the skills and knowledge required by the workforce generally and the CCI team specifically, with due cognisance of the organisation's strategy well as its intelligence and counterintelligence thrusts.

2) The **programme design and development** derives the programme objectives from the training needs and then design and develop the training material. It determines content, the duration of the programme, the training methods and techniques. The three proficiency of CCI training (fundamental, functional and advanced – see Figure 2) will be designed according to the functional specialities such as CCI collection, CCI analysis, CCI investigation, CCI offensive and CCI defensive

3) The **programme implementation,** communicates the training implementation to the respective target groups and their management echelons. Various training methods can be used for the implementation of awareness and training, such as classroom, online, practical, simulations, on-the-job training and so on.

4) **Programme evaluation and follow-up** appraises the effectiveness of the programme in terms of the increase in knowledge and skills and the improvement of attitude on the job as a result of the awareness and training programme. Follow-ups are done in the workplace after a certain period about the sustainability of knowledge, skills and attitude.

In this section, we advanced a structured process which can be applied for the design and implementation of a CCI ATP. In the next section a high-level outline of the programme itself is provided.

4. A High-level Outline of the multi-tiered CCI Awareness and Training Programme

A multi-tiered CCI Awareness and Training Programme (CCI ATP) can of course not be presented in any detail within the confines of a conference paper. In this section we thus only provide some high level contours of a

CCI ATP. To this end, we discuss each of the four proficiency levels (see figure 2) with reference to the key elements of target group, objectives, content and delivery methods and techniques.

4.1 CCI Awareness – the first line of defence and offence (Tier 1 – Figure 2)

Since employees cannot protect information systems against something they are oblivious of, e CCI awareness is a foundation and fundamental to enlighten employees of the cyber threats faced individually and as an organisation. A CCI awareness programme is a first line of defence and a foundation for the stronger cyber security posture of an organisation. Awareness focuses on people rather than technology with the key purpose of an awareness programme is to direct the attention of people to information security (Toth & Klein, 2013) It conveys the possible cyber risks and cyber threats faced by the organisation and provides skills to mitigate basic cyber-related risks and counter cyber threats (Roper, Grau, & Fischer, 2006).

The key elements of CCI awareness are as follow:

1) Description: A blended cyber security and CI awareness programme that increases employee awareness on the cyber threat landscape, type of adversaries and their techniques, and provide appropriate countermeasures. The emphasis is on personal and workplace practices which will limit the risk of individuals being exploited as an attack vector.

2) Target group: All employees including new employees, contractors and, in some instances, third-party service providers.

3) Objectives**:** After completing the awareness, individuals will be able to
   - Identify basic cyber threats and risks,
   - employ sound personal and workplace cyber security practices,
   - be aware of critical organisational assets,
   - be aware of the exploitation of the human element as attack vector,
   - understand policies and procedures to secure information systems, and
   - understand and recognise the countermeasures.

4) Overview of content
   - Cyber risks, cyber threats and cyber attacks
   - what is CI and CCI
   - policies and procedures
   - insider threat
   - techniques used by cyber actors
   - data security and privacy
   - personal security
   - computer and mobile security
   - internet and email security

5) Delivery methods and techniques.
   Several methods or techniques can be used to deliver an awareness programme, namely classroom tuition, workshops, online courses, seminars and open lectures. Supplementary techniques include intranet postings, posters, videos, games, quizzes, screensavers, etc

4.2 CCI Fundamental Training (Tier 2 – Figure 2)

CCI training, to reiterate is essential for improving the effectiveness of the organisation in achieving its strategic objectives. Training addresses employee competencies (knowledge, skills and attitude), skills gaps, re-skilling and upskilling. Training programmes are structured according to proficiency levels (fundamental, functional and advanced – see figure 2) and customised, where relevant, as *per* the requirements of functions or roles.

Since CCI training is multi-disciplinary, fundamental training should transfer a sound grasp of CCI as subset of counterintelligence and intelligence. It should also convey the CCI modes of active-offensive, active-defensive, passive-offensive and passive-defensive. To this end, the eight notional building blocks described by Duvenage, Sithole & von Solms 2017) in their' Framework for Cyber Counterintelligence' could be of value. This framework can graphically be depicted as follows:

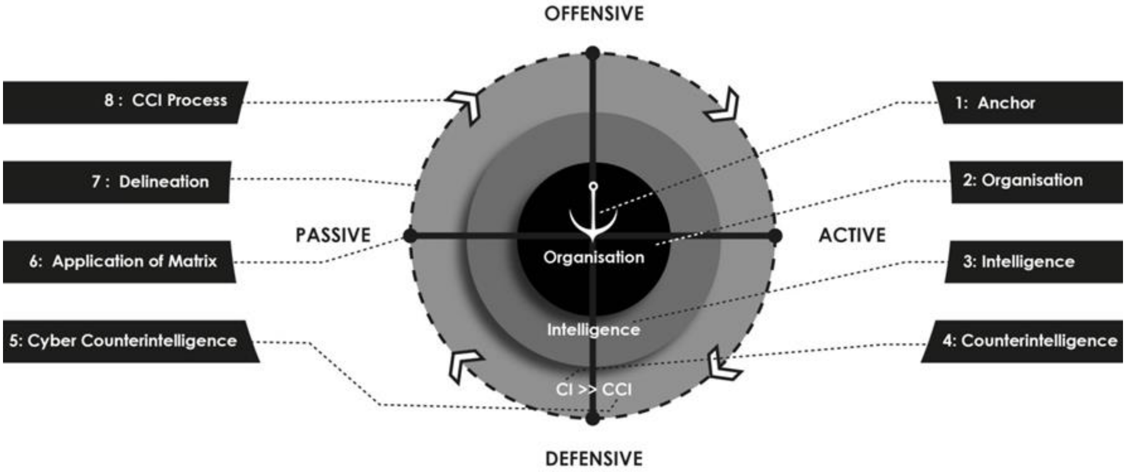

Figure 5: Conceptual Framework for Cyber Counterintelligence (Duvenage, Sithole, von Solms 2017)

CCI fundamental training is an entry level for functionaries with direct/indirect CCI responsibilities and serves as the foundation for functional and advanced training later on.

The key elements of CCI functional training can be summarised as follow:

1) Description: A blended cyber security and CI training that is a bridging programme between CCI awareness and CCI functional training. This level covers a fundamental understanding of CI skills, computer hardware, software, networks and systems. It introduces both offensive and defensive domains so that CCI team at the fundamental level will be able to, on a basic level, counter cyber intelligence threats

2) Target group: Functionaries with direct/indirect CCI responsibilities CI and personnel wanting to enter the CCI realm.

3) Objectives**:** After completing after completing fundamental training, individuals will
   - be equipped with knowledge, skills and tools to counter cyber threats,
   - understand the cyber threat landscape,
   - understand software security, networks security and systems security vulnerabilities,
   - understand and can apply software security, networks security and systems security measures,
   - have been introduced to basic offensive and defensive CI, cyber warfare and CCI strategies, and
   - be able to demonstrate CI and fundamental CCI skills.

4) Overview of content
   - Information Technology Security (computer security, networks security, data security)
   - Physical security
   - Cyber Threat landscape

- Cyber actors and attack vectors
- Cyber intelligence (cyber collection)
- Social Media and its role to cyber collection, threats and attacks
- Policies, Procedures and Standards (CI, Information and Cyber Security)
- Fundamentals of aspects such as penetration testing, cryptography, digital forensics, etc.
- Cyber resilience or cyber risk management based approach.

5) Delivery methods and techniques.
Several methods or techniques can be used to deliver a fundamental programme, namely classroom tuition, online, hands-on or virtual and practical.

4.3 CCI Functional Training (Tier 3 – Figure 2)

CCI functional training is at an intermediate level. It is a role-based training because it is structured according to the roles and responsibilities of the CCI job or position, depending on how the CCI function is structured in an. Design and development of the training curriculum will differ according to specific skills as required by a particular role. Some of the suggested roles such as CCI investigation, CCI Analysis, CCI Collection organisation, CCI technical specialisation (Black, 2014; Jaquire, et al., 2018).

1) Description: A blended cyber security and CI training that builds on the knowledge and skills acquired in the fundamental CCI training. This training structured according to the roles and responsibilities of the CCI job or position.

2) Target group: The training for CCI workforce and all functions in both CCI offensive and defensive domains.

3) Objectives: After completing the awareness, individuals will be able to

- equipped with knowledge, skills, attitude and tools to conduct CCI functions according to specific domain.
- As CCI is multi-disciplinary, some of the training objectives and skills development will overlap as illustrated by Jaquire, et al. (2018) in figure 5.

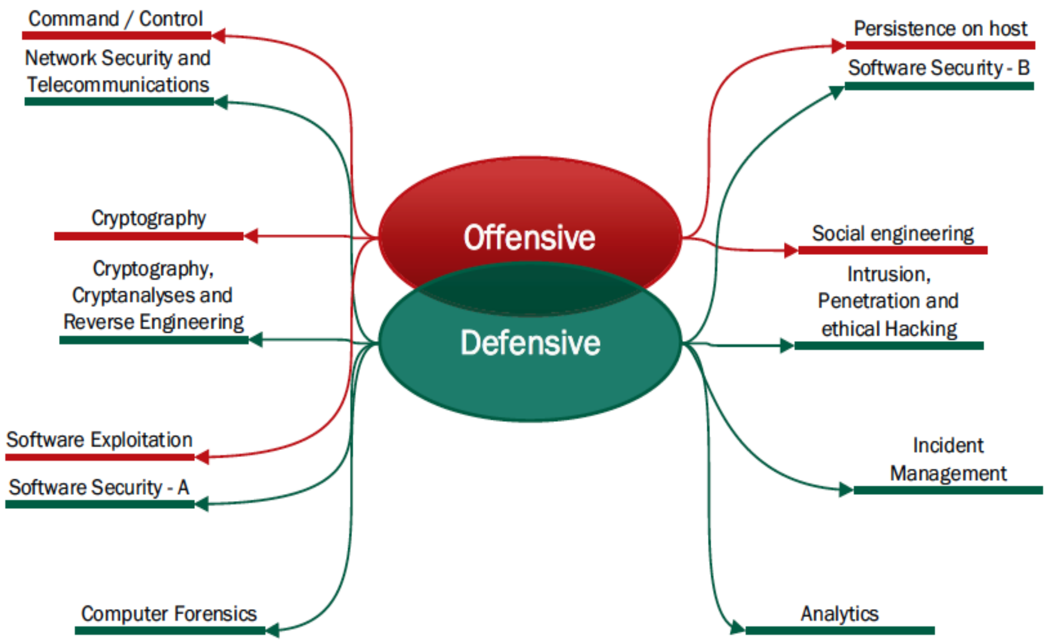

Figure 5: (Non-comprehensive example) overlap in defensive, offensive CCI training, and skills development - (Jaquire, Duvenage, & von Solms, 2018).

4) Overview of content - the topics are for both offensive and defensive CCI training; the list is not exhaustive. Each topic can be broken down into sub-topics.

- Cyber threat intelligence
- Data collection: OSINT, HUTMENT & SOCMINT
- Digital Forensics
- Advanced networks
- Cryptography
- Penetration testing
- Vulnerability assessment
- Exploitation
- Ethical hacking
- Incident response management
- cyber intelligence analysis
- data analytics

5) Delivery methods and techniques

There are many methods or techniques that exist to deliver a functional training programme: classroom, online, hands-on or virtual practical, cyber games, emulation and simulation exercises (blue team, red team), research.

4.4 CCI Advanced Training (Tier 4 – Figure 2)

This training proficiency level equips individuals with relevant specialist knowledge and skills. According to Toth & Klein (2013), this level "integrates training, education and experience with an assessment mechanism to validate knowledge and skills, resulting in the 'certification 'of a predefined level of competence". For a certain part, this level of training thus draws on industry-based knowledge. Serving as examples are the training and assessment conducted by external certification bodies such as EC-Council, ISACA, (ISC)², SANS and CompTIA. Within statutory state security structures internationally, however, external industry-based training is complemented by advanced in-house training in especially CCI's offensive dimensions.

5. Conclusion

Cyber counterintelligence offers a proactive approach in countering cyber threats and cyber-attacks. This paper presented the outlines of a four-tiered CCI training programme with reference to *inter alia* target group, training objectives, training content and delivery methods or techniques. The design and development of the CCI ATP must follow the four step training cycle as it will ensure continuous update and relevance of the content.

The CCI ATP's proficiency levels discussed were awareness, fundamental training, functional training and advanced training. All these levels have content that incorporates both the CI and cyber skill sets. Within the confines of a conference paper only some contours of CCI ATP could be provided. Furthermore, and for self-evident reasons of sensitivity, some aspects of functional and advanced CCI training are not reflected in academic research in the public domain.

References

Amankwa, E., Loock, M., & Kritzinger, E. (2014). 'A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions', The *9th International Conference for Internet Technology and Secured Transactions* (ICITST-2014) (pp. 248-252). IEEE.

Black, J. M. (2014). *The Complexity of Cyber Counterintelligence Training*, Master of Science in Cybersecurity, Utica College. Unpublished.

Caballero, A. (2017). ‘Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems’ in J. R. Vacca (dd.), *Computer and Information Security Handbook* (Third Edition) (pp. 393-419). Morgan Kaufmann.

Caballero, A. (2017). ‘Security Education, Training, and Awareness’ in *Computer and Information Security Handbook* (Third Edition) (pp. 497-505). Morgan Kaufmann.

de Zafra, D. E., Pitcher, S. I., Tresses, J. D., & Ippolito, J. B. (1998, April). NIST, National Institute of Standards and Technology. Computer Information Resource Center. Information Technology Security Training Requirements: a Role- and Performance-Based Model. Retrieved September 2018, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Dtex. (2017). *2017 Insider Threat Intelligence Report*. Retrieved October 2017, from Dtex Systems: https://www.dtexsystems.com/2017-insider-threat-intelligence-report/

Duvenage, P., & von Solms, S. (2013). ‘The Case for Cyber Counterintelligence’, International *Conference on Adaptive Science and Technology*. Pretoria, South Africa: IEEE.

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

Duvenage, P., Sithole, T., & von Solms, S. (2017). ‘A Conceptual Framework for Cyber Counterintelligence – Theory That Really Matters’, 16th *European Conference on Cyber Warfare and Security*, (pp. 109-119). Dublin, Ireland.

Jaquire, V., Duvenage, P., & von Solms, S. (2018). ‘Building the Ideal Cyber Counterintelligence Dream Team’, *17th European Conference on Cyber Warfare and Security*, (pp. 224-232). Oslo, Norway.

Kissel, R., & Wilson, M. (2010). 'Cyber Security Education, Training, and Awareness' in J. G. Voeller (Ed.), Wiley *Handbook of Science and Technology for Homeland Security*, 4 Volume Set. John Wiley & Sons.

MacCauvlei Learning Academy. (2016). *Higher Certificate in Occupational Directed Education, Training and Development Practices*. Pretoria: unpublished.

Monk, T., van Niekerk, J., & von Solms, R. (2010). 'Sweetening the Medicine: Educating Users about Information Security by means of Game Play', *2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists* (pp. 193-200). Bela Bela, South Africa: SAICSIT.

Roper, C., Grau, J., & Fischer, L. (2006). *Security Education, Awareness, and Training: From Theory to Practice*. Oxford: Elsevier Inc.

Thomason, S. (2013). 'People –The Weak Link in Security', *Global Journal of Computer Science and Technology Network*, Web & Security, 13(11).

Toth, P., & Klein, P. (2013, October). *NIST Special Publication 800-16. A Role-Based Model for Federal Information Technology/ Cyber Security Training*. Retrieved September 2018, from http://csrc.nist.gov/publications/PubsDrafts.html#800-16-rev1

Van Derwerken, J., & Ubell, R. (2011). 'Training on the Cyber Security Frontlines' *American Society for Training & Development*, pp 46-50.

.