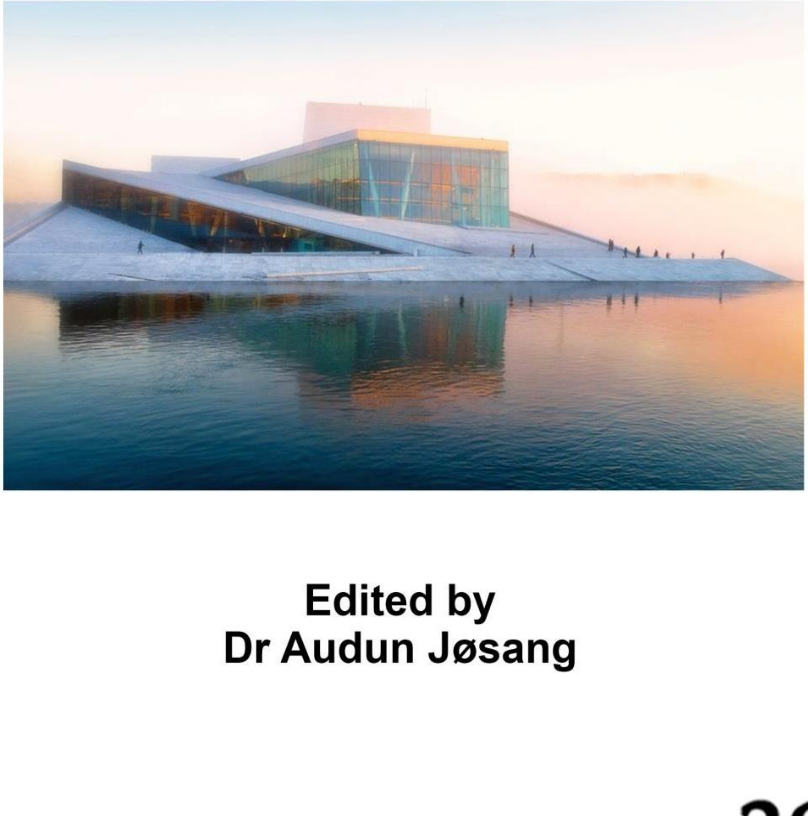
Proceedings of the
17th European Conference on Cyber Warfare and Security

University of Oslo
Norway
28-29 June 2018



Edited by
Dr Audun Jøsang

acpi

A conference managed by ACPI, UK

Building the Ideal Cyber Counterintelligence Dream Team

Victor Jaquire, Petrus Duvenage, and Sebastian von Solms

Centre for Cyber Security, Academy of Computer Science and Software Engineering, University of Johannesburg

duvenage@live.co.za
jaquire@gmail.com
basievs@uj.ac.za

Abstract: "Years ago, small groups working together 'or lone wolves (ninjas)' were the ones who hacked into systems. The days of old have come and gone, and the criminals are now working together without fear of impunity more than ever" [Bodmer *et al*, 2012]. Bodmer *et al* [2012] also indicate that this situation is true for both the hacker and the defender, "as it is easier and safer to work in numbers on the Internet, especially since evidence collection and attribution are so difficult for all involved parties".

In a real world scenario where appropriate cyber counterintelligence (CCI) human resources are scarce and/or expensive and where limited relevant educational sources are available, it is imperative to identify the necessary people, teams and skills to anthropomorphise and mature the CCI effort in order to achieve an organisation's strategic CCI objectives.

In a world where suitable cyber related human resources are scarce and expensive, the process of identifying and building an appropriate, cost effective and functional CCI dream team is essential to ensure that an organisation's' CCI strategic initiatives are achieved.

This paper contributes to the series of previous papers on cyber counterintelligence (CCI) maturity. It aims to add to the emerging considerations on CCI through a discussion on a process of building an ideal CCI dream team as part of an organisation's CCI maturity. It highlights the effectiveness of cybersecurity when incorporating it in an integrated CCI approach. It further deliberates an integrative approach of CCI practices in conjunction with traditional defensive and/or offensive cyber measures in order to leverage on, and further develop existing skilled people. Lastly, it culminates in the discussion of the high level functions required within a CCI environment, setting the basis for putting together the ideal dream team as part of the establishment and / or maturity of a CCI capability that can be tailored for a government and/or private sector environment alike.

Keywords: cyber counterintelligence, dream team, cyber threat intelligence, defensive and offensive cybersecurity, cyber counterintelligence maturity

1. Introduction

Farchi [2016] refers to the requirement for counterintelligence within the private sector. He focusses on the need for a particular form of counterintelligence namely CCI and states that it entails utilising, '**defensive**' and '**offensive**' Counterintelligence **approaches**, with the aim of safeguarding organizations [Farchi, 2016]. In a conceptual overview and theoretical proposition Duvenage, von Solms & Corregedor [2015], describe CCI as "the subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralisation of adversarial attempts to collect, alter or in any other way breach the C-I-A (confidentiality, integrity and availability) of valued information assets through cyber means".

Farchi [2016] further refers to the escalating tendency of information security companies, emphasising their service offering on "gathering information on specific threats against organizations", instead of only the traditional focus on providing defensive solutions.

There are countless volumes written on various Intelligence, Counterintelligence and CCI concepts and approaches. Although some of the previous writings in this regard establishes the basis for CCI and focuses on some of these concepts, there is a notable lack in the availability of literature that provides guidance in both the form of a framework for a CCI maturity model, as well as the associated resources and skills required for such an undertaking.

Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) 'Building the CCI dream team' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June, pp 224-232.

The implementation of a CCI capability is dependent on an organisation's strategy, risk profile and unique requirements. The question then with regard to the requirements for relevant CCI people, skills or focus teams remains, since its requirements can be as diverse as the diversity of every organisation out there.

Due to the complexity of CCI, some guidance on identifying relevant people, skills, focus teams etc. is prudent that can assist organisations in transitioning their traditional defensive-only approach when securing cyberspace, to a more evolved approach in line with the demands for advanced threat mitigation of the present, and beyond. A beneficial starting point for such guidance (among others), emanates in the form of a discussion on an approach.

2. The Approach

A country, government and/or private sector business requires an efficient method to incorporate CCI within their whole security plan and to mature it over a set period into a fully functional CCI ability. This will include the implementation and maturity of CCI teams, skills and focus areas.

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 [Jaquire & von Solms, 2017 (1)]. In order then for an organisation to construct the ideal CCI team, it will be judicious to consider the functions that the CCI environment will perform within that organisation, in line with organisational strategy. This will allow the organisation to identify the CCI team functions accordingly, from which the ideal CCI team can be constructed. This will also provide the organisation with the opportunity to leverage on its existing resources, to assist in the implementation of the CCI capability in a cost effective way.

Even though there are CCI focus areas that will be identified in line with the organisational strategy for each different organisation, which will be specific to that organisation [Bardin, 2011], some base level functions, or grouping of functions will be the same within all organisations. These base level functions will form the foundation for the construction of any CCI team. From this core, further lower level functions and team requirements can be identified and implemented accordingly as per the organisations' needs and CCI maturity plan.

3. Constructing the ideal CCI dream team

When considering a CCI capability, all functions within a CCI maturity model can be grouped within five main high level functions [Jaquire, 2018]. These are the main functions that would be essential within all organisations, which require establishment and / or maturity for the purposes of a CCI capability. These main functions will form the centre for the constructing or identifying of an ideal CCI dream team and they are as follows:

1. **Senior Executive – C Level**
2. **Management**
3. **Analyses**
4. **Technical Specialisation**
5. **Incident / Situation Management and Coordination**

All five of these functions are principal to the effective functioning and maturity of all the Categories within CCI. From these five base functions, all further CCI sub-functions, resources and team requirement can flow in line with the organisational strategy. We will briefly discuss each of these functions within the following sections (Sections 3.1 to 3.5), relating each of them to the effort of building the ideal CCI dream team.

3.1. Function 1 - The Senior Executive (C-Level)

Kajava *et al* (2006) refer to the numerous information security awareness programmes within organisations, and stresses "top management often shies away from them". It is argued that the "damage caused by an individual employee may have far-reaching consequences for a company, but when damage is inflicted by senior management, the effects may be devastating" [Kajava *et al*, 2006].

Likewise, it is therefore not only imperative to ensure that the senior executive management endorse the CCI strategy, programme and efforts unequivocally, but also for the senior executive to understand CCI, cyber and information security in order to take full control and responsibility thereof and actively participate and show their support [Kajava *et al*, 2006].

The senior executive is responsible for the overall strategy and direction of the organisation. CCI, just as is the situation with other organisational efforts, should be in line with the business objectives of the organisation. It is the senior executive who will decide the level of the intensity of focus on each of the dimensions within a CCI framework, as well as the level of maturity required for each of the dimensions within a CCI maturity model.

These decisions will be made in line with the strategic requirement of the organisation as per the organisations unique business realities, requirements and risk profile. These decisions include, among other, issues such as strategy development and approval (including CCI policy development and implementation), Financial Commitment and Strategic Operational Approval.

In order for the senior executive to make effective decisions, it is their responsibility to understand the cyber threats that the organisation faces, to understand the impact that a cyber-attack (in its various forms) can have on the assets of the organisation, and to instil this understanding and situational appreciation within the management and employees of the organisation.

For the senior executive to achieve this, they need to be skilled and trained to understand cyber-related threats that their organisation faces in line with their industry, area of business and own realities. They also need to be skilled and trained in appropriate remedial and proactive actions, as well as related strategies and thought processes in order to develop appropriate strategies and make informed decisions with regard to CCI for their organisation (*cf* Duvenage, Sithole & von Solms, 2017). Senior executives should also be trained and skilled to fully understand CCI and the related CCI maturity model for their organisation, and they should ensure that the management below them are fully trained in this as well.

The senior executive function (accountable for the CCI programme) will therefore be the first essential part of the ideal CCI dream team.

3.2. Function 2 - Management

Management usually deals with general management issues such as (but not limited to) the following:

- Alignment with organisational strategy,
- Financial management,
- Operational management,
- Coordination,
- Approvals.
-

Within a technical, Information security or cyber related environment, managers also deal with the non-technical aspects of cyber and information security related issues such as the following [Soomro *et al*, 2016]:

- "Security policy development,
- Awareness and related training,
- Acquisition of security hardware and software,
- Internal control and decisions regarding data processing".

Due to the nature of such technical environments, there are numerous writings advocating the notion that "the safeguarding of information assets and data security can be ensured through the integration of technical and managerial activities" [Young & Windsor, 2010]. This is specifically the situation with regard to managers who are responsible for every condition within a multi-disciplinary CCI environment. Management, just as is the case with senior executives should be:

- Skilled and trained to fully understand the CCI environment under their control,
- Skilled and trained to fully understand:
    - How their environment fits into the larger CCI programme and strategy
    - What is required from their environment in line with the CCI effort
    - All the technical and non-technical processes and tasks to be performed by the technical and non-technical personnel and systems under their control – without necessarily becoming an expert on every field within their area of responsibility.
- Skilled and trained on the entire CCI process, especially the CCI maturity strategy and plan.

Apart from this, management should also, (in line with the training and skills development for senior executives), be trained and skilled in, among other:

- Threat identification, evaluation and management, including appropriate remedial and proactive actions,
- CCI methodologies including active, passive, defensive and offensive strategies, denial and deception techniques, operations and technical requirements.

Management should also realise their managerial authority and capabilities, especially when dealing with offensive and deception strategies, and be able to guide technical and non-technical personnel within their environment, in line with the organisational CCI strategy.

The CCI management function (responsible for the CCI programme) will therefore be the second essential addition to the ideal CCI dream team.

3.3. Function 3 - Analysis

In his benchmark contribution on Counterintelligence, Godson (2001) states: "Perhaps the queen of the counterintelligence chess board is counterintelligence analysis, both offensive and defensive." Since CCI is a subset of Counterintelligence, Godson's (2001) statement also rings true within CCI. This section argues the CCI analysis function as being:

- Multi-layered in that it pertains to appraisals on the tactical-technical, operational and strategic levels.
- Multi-disciplinary in that it draws from numerous fields of study, specialisation and expertise.
- An all-source endeavour in that it draws from data and information which could range from data feeds to information obtained from human sources. CCI thus includes, but is much wider than, data science.
- An appraisal process which combines various types of analysis – from automated technical analytics to analysis performed by humans.

Maisey [2014] reflects on the current automation of SIEM tools that "focus on automated, predictive analysis of attacks using data mining techniques as a way to reduce the load on analysts". He notes that the "idea is superficially attractive, and can be effective at spotting and preventing simple cases" [Maisey, 2014].

He further cautions that in situations like "fraud detection, similar tools have been found wanting against advanced adversaries such as organised criminals". He relates to the writings by Wilhelm [2014], who noted, "These adversaries are adaptive, and will change behaviour in order to evade specific detection tactics. Automatically derived rules tend to perform poorly when compared to those used by human analysts because they tend to focus on more robust indicators of fraudulent behaviour" [Willhelm, 2014]. Analysis (as one of the main drivers within the CCI domain), needs to heed these cautions [Maisey, 2014].

Analysis has both an internally and externally focussed responsibility. It is also the main player in identifying the level of CCI required within an organisation, based on the organisations strategic needs and unique environment. Borum *et al* (2014), allude to this type of analyses when referring to "Cyber-related considerations that matter in a strategic sense are the ones that impact an organization's ability to achieve its overarching mission objectives. Examples might include answers to the following [Borum *et al*, 2014]:

- "Does the organization operate in a high, moderate or low cybersecurity risk industry?

- What is the value of the organization’s information and information flows to potential threat actors?
- What are the confidentiality, availability and integrity risks to the organization’s assets?
- What legal liabilities exist related to the type of information stored, such as personally identifiable information…?”

Analysis further includes numerous fields of study, specialisation and expertise [Recorded Future, 2015], again depending on an organisations risk profile, strategic needs and unique environment, including, but not limited to analysis with regard to:

- Technical and non-technical defensive and offensive behaviours and strategies,
- Denial, deception and counter deception behaviours and strategies,
- Technical and non-technical behavioural and anomaly identification,
- Historical analyses,
- Predictive analyses,
- Predictive analytics – which can further be grouped under a region, a group of people, a country of origin etc.
- Trending – (Local, Regional, International),
- Language,
- Religion,
- Legal,
- Psychological and behavioural scientists,
- Data Science,
- HUMINT

The training and skills development requirement for CCI analysis needs to keep all these factors in mind to ensure that all requirements are efficiently addressed during the CCI maturity life cycle, in line with a Cyber Counterintelligence Maturity Model (CCIMM).

The analysis function will therefore be the third essential addition to the ideal CCI dream team. The specific analysis needs for each organisation will depend on the strategic CCI requirements of the organisation, and will include a focus on several of the areas within the analysis fields as listed above.

3.4. Function - Technical Specialisation

Seeing that CCI primarily focusses on counterintelligence within the cyber domain, technical operations (together with the analysis function as discussed above) forms the heart of CCI. Due to the numerous possible fields of technical focus within the cyber environment, technical specialisation in a multi-disciplinary approach (see the discussion within Sections 2 and 3.3), especially on a technical/tactical as well as an operational CCI level is essential.

To further strengthen this approach, in our experience the inclination is always there to split defensive and offensive operational and technical/tactical functioning. From a training and skills development point of view, there are major overlaps in the requisite training and skills requirements within both defensive and offensive requirements, as can be highlighted with the following figure:

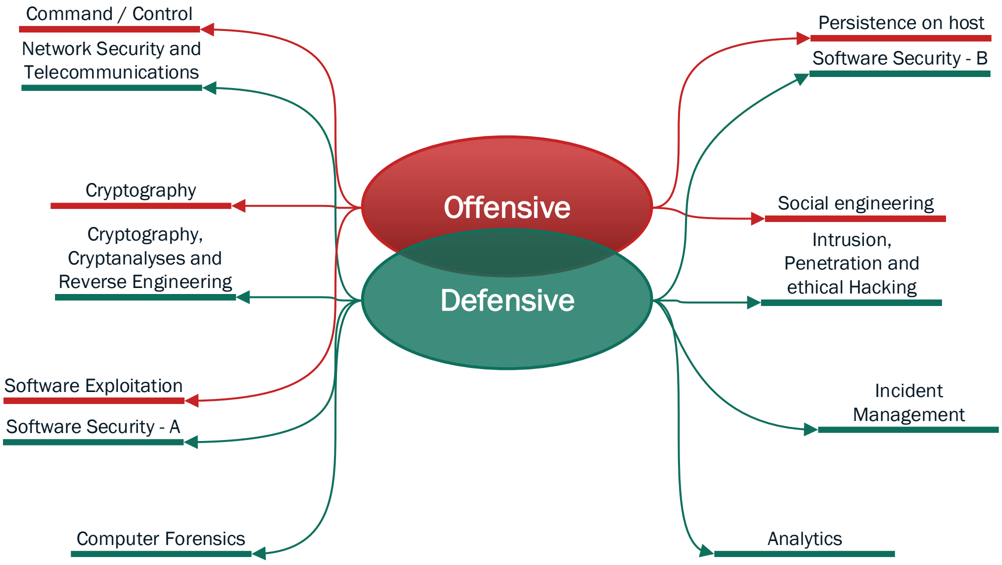


FIGURE 1: (NON-COMPREHENSIVE EXAMPLE) OVERLAP IN DEFENSIVE, OFFENSIVE CCI TRAINING, AND SKILLS DEVELOPMENT REQUIREMENTS (CREATED BY THE AUTHORS)

Even though Figure 1 is merely an example / extract and not an extensive comparison, and although there are specific areas of specialisation that are unique to each discipline (defensive or offensive) a definite functional skills overlap is noted within the requirements between Defensive and Offensive CCI. This at least as far as base knowledge is concerned, allowing for field of interest specialisation.

This integrative approach of CCI practices in conjunction with traditional defensive and/or offensive cyber measures can be done within both a government and/or private sector environment in order to leverage on, and develop existing skilled cyber and information security functions within a CCI environment.

It further indicates that the leveraging on existing cyber and information security functions within an organisation, allows for the cross functional utilisation of these same existing functions for the establishment and maturity of CCI in a CCIMM.

It also further strengthens the notion that cyber counterintelligence is not necessarily a separate unit within an organisation. As indicated earlier, CCI is therefore, more often than not, not a structure, but rather a way of 'functioning', through the maturity of existing and new functionality within an organisation to fulfil the CCI requirement - to achieve the CCI strategic vision and desired outcomes in a cost effective manner.

To this end, structures and activities that we might acknowledge as forming part of the cyber and information security realm can be allocated to each of the five CCI dimensions [Jaquire & von Solms 2017(2)].

Although this may vary from organisation to organisation, the allocation can be demonstrated within an example look as follows (see Figure 2):

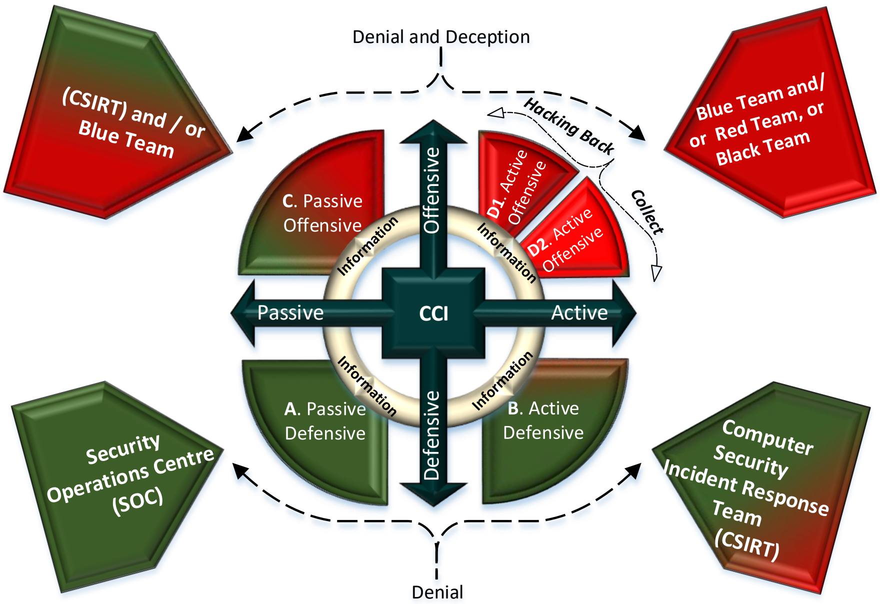


FIGURE 2: EXAMPLE OF AN ALLOCATION OF EXISTING FUNCTIONS / ACTIVITIES PER CCI DIMENSION (CREATED BY THE AUTHORS)

When studying Figure 2, we can utilise a basic Computer Security Incident Response Team (CSIRT) structure as an example (this structuring will be uniquely customised by each different organisation). In this example, the CSIRT is the main entity responsible for the activities allocated to the **Active Defensive** dimension (B), as well as a contributing entity responsible for the activities within the **Passive Offensive** dimension (C).

In an organisation, the CSIRT, for example, might be an existing functioning structure with existing specified activities to fulfil in line with the organisational strategy. In order to integrate this structure into the integrated CCI effort, its existing activities can be taken into account in order to slot them in correctly with the organisations own customised **CCIMM**, within the correct dimension. Examples (non-exhaustive) of CSIRT activities within the **Active Defensive** dimension may for instance include the following:

- *Alerts and warnings*
- *Vulnerability assessments and penetration testing*
- *Secure code analyses*
- *Artefact handling*

Further examples (non-exhaustive) of CSIRT activities within the **Passive Offensive** dimension may, among other, include the following:

- *Implementation, monitoring and analysis of honeynets,*
- *Implementation, monitoring and analysis of tar pits and sandboxing,*
- *Identification and location tracking of perceived threatening IP addresses.*

In examples like these, the exiting activities of the CSIRT within the organisation will form part of the organisations own customised **CCIMM** and will, because they are already existing activities, already be on a higher stage of maturity than the activities that are specified within a **CCIMM**, but which are not currently performed by such a CSIRT. All of these existing and newly identified activities need can then be specified within the organisations **CCIMM** within the sub-categories as Compliance Indicators. In the same way, all other relevant existing functions within the organisation can be integrated within the CCI programme to ensure that existing technical expertise, specialisation and technical generalists are utilised.

The technical specialisation function will therefore be the fourth essential addition to the ideal CCI dream team. As is the case with the analysis function, the specific technical specialisation skills or team focus requirements (examples of which are highlighted within domains A to D within Figure 2), as well as its intensity of utilisation will depend on the organisations CCI strategy.

3.5. Function 5 - Incident / Situation Management and Coordination

Kulikova et al [2012], indicate that "security incidents vary widely in their severity", and that "the composition of the incident response team should reflect the impact the incident has on the organization" [Kulikova et al, 2012]. In the same way, throughout the CCI process, all CCI related outcomes, situations, incidents and efforts needs to be coordinated and managed accordingly.

Although the day-to-day management of the CCI environment is done by the relevant management, and although basic incidents are handled through the normal cyber incident-management functions, certain events and/or situations require a dedicated control from the moment that it is conceived or identified, until fruition and post mortem evaluation.

Either these situations can be planned activities flowing from strategic, operational or technical/tactical needs, or they may originate as a result of the analyses outcome, based on the various analyses spheres [as discussed within Section 3.3 above], such as specific incidents reported from the operational or technical/tactical environment.

This function can also be described as a specialised project management function, which requires extensive insight within the CCI field, as well as extensive experience with regard to CCI, the CCI maturity life cycle and within the different CCI related domains. It especially requires extensive knowledge and experience within the CCI analysis field as in our experience, continuous situational analyses throughout the process is required.

As an example. The incident / situation management and coordination function includes, among other, the following:

- Coordination of Incident / situation handling efforts between strategic, operational and technical / tactical environments, including:
  - Escalation.
  - Resolution authorisation (when the resolution of a specific situation requires approval from management or the executive),
  - Incident / situation handover – Should the handling of the incident or situation require expertise and / or resolution by a third party or external organisation.
- Inter programme coordination of incident / situation handling efforts and resolution,
- Inter organisational coordination of incident / situation handling efforts and resolution

The incident / situation management function will therefore be the fifth and last essential addition to the ideal CCI dream team.

4. Conclusion

In today's reality, the defensive-only solutions, habitually trusted throughout the decades are no longer sufficient to safeguard our environments and our way of life. The advancement of solutions to recognise and deal with the assaults against the confidentiality, integrity and availability of information and infrastructure endures as decisive defensive measures, but it is no longer efficient as a comprehensive resolve.

As identified within the approach, an organisation requires an efficient method to incorporate cyber counterintelligence within their whole security plan and to mature it over a set period into a fully functional cyber counterintelligence ability. This approach will include the implementation and maturity of CCI teams, skills and focus areas.

Constructing a CCI team is very much dependent on what the organisation aims to achieve within its CCI strategy. Building the ideal CCI dream team will require careful consideration between current functions, new functions and costs.

Following a multi-disciplinary and integrated methodology can assist an organisation to utilise its existing skills, teams and functions, together with newly identified requirements as highlighted within its CCI maturity strategy, in order to realise these strategic team requirements.

The approach to align team considerations with the five main functions that would be essential within all organisations for the establishment and / or maturity of a CCI capability, is a promising starting point in building the CCI team. This team can further evolve, together with all the other focus areas as highlighted within an organisations CCI maturity strategy, towards the ideal cyber counterintelligence dream team.

References

Bardin, J. (2011), 'Ten Commandments of Cyber Counterintelligence' - Adapted from James M. Olson , *CSO online*, http://www.csoonline.com /article /2136458/ identity-management / ten-commandments –of - cyber- counterintelligence ---adapted –from –james –m –olson .html, Accessed 18 Feb 2016

Bodmer, S. *et al* (2012), *Reverse deception–Organized cyber threat counter- exploitation*, McGraw-Hill, New York.

Borum, et al (2014), 'Strategic Cyber Intelligence', *Emerald Insight, Information and Computer Security*, Vol 23, No 3, pp 317-332, www.emeraldinsight.com/2056-4961.htm, Page 322.

Duvenage, von Solms, & Corregedor (2015), 'The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition', Paper read at the *14th European Conference on Cyber Warfare and Security, (ECCWS)*, Hatfield, United Kingdom, July 2015.

Duvenage, P.C., Sithole, T.G. & von Solms, S.H. (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters!' in *Published Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland,

Godson, R. (2001) *Dirty tricks or trump cards – U.S. covert action and counterintelligence*, Transaction Publishers, New Brunswick..Heckman, et al (2012), *Cyber Denial, Deception and Counter Deception, A Framework for Supporting Active Cyber Defence*, Springer.

Jaquire, V.J. (2018), *A framework for a cyber counterintelligence maturity model*, unpublished Doctor of Commerce (Informatics) thesis at the University of Johannesburg, Johannesburg, South Africa, Chapter 8.

Jaquire, V. & von Solms, S.H. (2017(1)), 'Cultivating a Cyber Counterintelligence Maturity Model', paper read at the *16th European Conference on Cyber Warfare and Security*, (ECCWS).

Jaquire V. & von Solms S.H. (2017(2)), Towards a Cyber Counterintelligence Maturity Model, *ICCWS 2017*.

Kajava, et al (2006), *Senior Executives Commitment to Information Security - from Motivation to Responsibility'*, University of Lapland, IEEE 1-4244-0605-6/06, Accessed 20 Feb 2017

Kulikova, et al (2012), 'Cyber Crisis Management: A decision-support framework for disclosing security incident information, *2012 International Conference on Cyber Security*, Page 106.

Maisey, M. (2014), Moving to analysis-led cyber-security, Science Direct, http:// www.sciencedirect.com /science /article /pii/S1353485814700492, Page 7, Accessed 10 March 2017

Recorded Future, (2015), *Temporal Analytics for Predictive Cyber Threat Intelligence*, https://www. recordedfuture.com/category/product/ , Page 868

Soomro, et al (2016), Information security management needs more holistic approach: A literature review, *International Journal of Information Management*, 36 (2016) 215–225, Page 219

Willhelm, W.K. (2014), The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management, *Journal of Economic Crime Management*, Spring 2014, Volume 2, Issue 2,. https://library. utica. edu/ academic/ institutes/ ecii/ publications/ articles/ BA309CD2-01B6-DA6B- 5F1DD7850BF6EE22.pdf, Accessed March 2017

Young & Windsor, (2010). Empirical evaluation of information security planning and integration, *Communications of the Association for Information Systems*, 26(1), 245–266.

Jaquire, V.J., Duvenage, P.C. & von Solms, S.H. (2018) 'Building the CCI dream team' in *Published Proceedings of the 17th European Conference on Cyber Warfare and Security*, Oslo, Norway, June, pp 224-232.