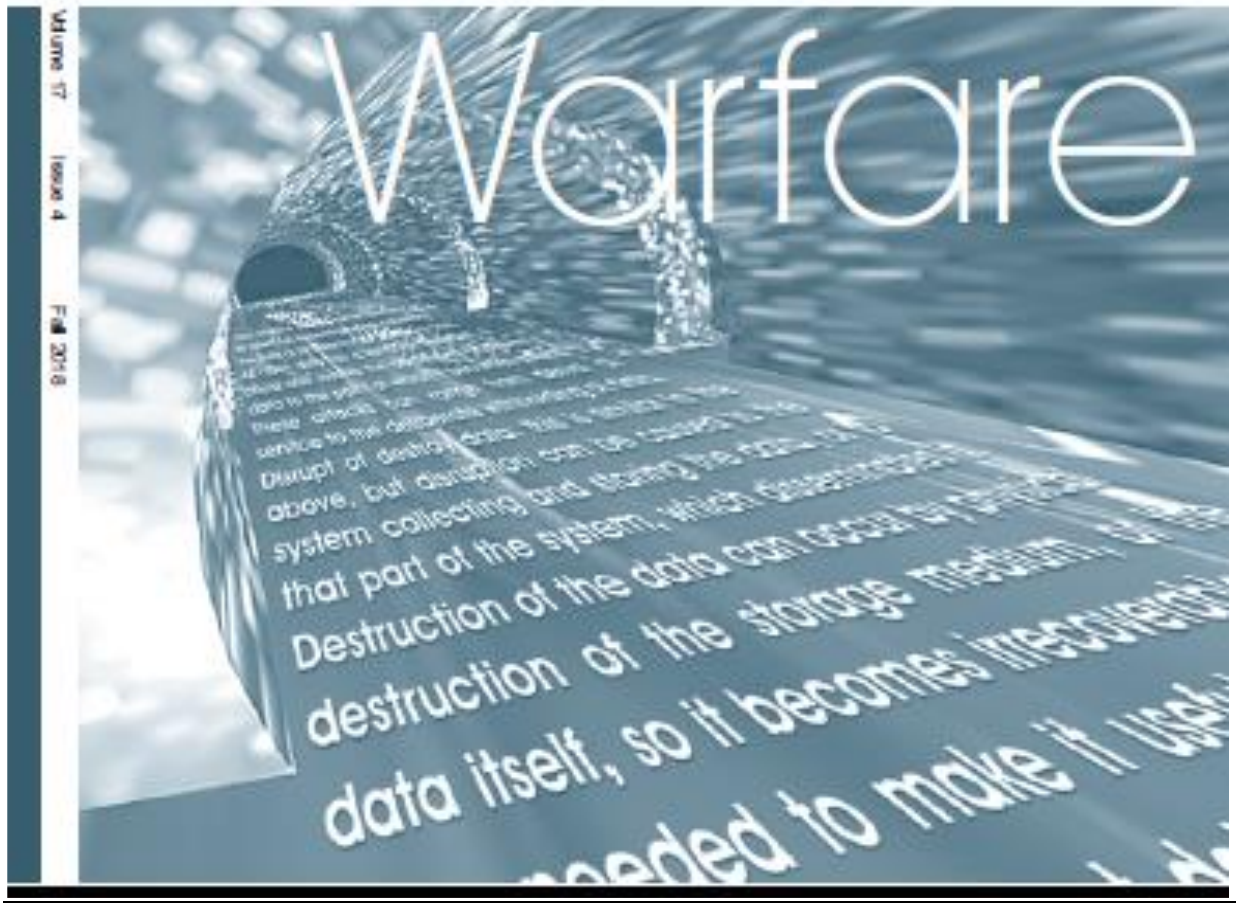
Volume 17, Issue 4, Fall 2018
ISSN 1445-3312 (Printed Journal)
ISSN 1445-3347 (Online Journal)

JOURNAL OF INFORMATION WARFARE

Journal of Information Warfare



Towards a Literature Review on Cyber Counterintelligence

PC Duvenage, VJ Jaquire, and SH von Solms

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

E-mail: duvenage@live.co.za; jaquire@gmail.com; basievs@uj.ac.za

***Abstract**: For those connecting the dots, the threat landscape continues to affirm the necessity of having Cyber Counterintelligence (CCI) at the centre of cybersecurity efforts. Concurrent with the growing interest in CCI in corporate boardrooms and the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. The growing body of CCI-focused literature clearly attests to this evolution. A review of such literature has self-evident academic and practical benefits. This article advances a tentative, selective review of CCI literature that demonstrates the need for a more extensive and in-depth appraisal.*

Keywords: *Cyber Counterintelligence, Cyber Warfare, Cyber Security, Literature, Theory, Denial and Deception*

Introduction

For state and non-state actors with sizable cyber interests, numerous breaches during this decade have affirmed the necessity of having Cyber Counterintelligence (CCI) at the centre of cybersecurity efforts (Prunckun 2018; Stech & Heckman 2018; *The Economist* 2015). Concurrent with the growing interest in CCI in corporate boardrooms and in the corridors of governments, CCI is evolving from a field of academic enquiry to a distinctive academic sub-discipline. Attesting to the growing interest in CCI is the expanding body of peer-reviewed, academic contributions specifically focused on CCI. These contributions include numerous conference papers (such as Sigholm & Bang 2013; Jaquire & von Solms 2017a-c; Duvenage, von Solms & Corregedor 2015) and several completed post-graduate studies (for example Knowles 2013; Black 2014; Fieber 2015; Putnam 2015; Justiniano 2017; Jaquire 2018; Duvenage 2018). As will be shown in this article, commercial literature on CCI has also been growing sharply in recent years.

A literature review not only has self-evident benefits for CCI's academic progress, but it will also be useful to the increasing number of practitioners specialising or interested in this area. Attempting a comprehensive and representative literature review within the confines of a single journal article will be over-ambitious. Moreover, in the case of a field as young as CCI, such an extensive review would arguably be pre-mature. Therefore, the article's aim is to submit a tentative, selective literature review on CCI. Such a pilot literature review reveals the need for a much more comprehensive and inclusive appraisal of CCI literature.

The rest of the article is structured as follows:

- First, the purpose and benefits of a selective literature review on CCI are discussed in more detail.
- Secondly, the scope and the nature of the selective literature review are defined.
- Subsequently, the literature review is presented with reference to four literature categories, namely (1) peer-reviewed papers and articles, (2) masters' and doctoral studies, (3) books and (4) other literature.
- Finally, the conclusion submits key findings and observations regarding the way forward.

The Purpose and Benefits of a Selective Literature Review on CCI

Within academic research in general, there are various types of literature reviews which serve different purposes (Grant & Booth 2009; Mallett *et al.* 2012; Kim 2018). Some better-known examples (of review types) include: argumentative-, integrative-, historical-, systematic-, methodological- and theoretical reviews. From these types, systematic reviews have, for good reasons, been gaining prominence in academic circles (Mallett *et al*. 2012; Grant & Booth 2009). While a systemic review has many benefits, its compilation is an exhaustive and extensive process.

As suggested earlier, even for an academic sub-discipline as young as CCI, it would have been over-ambitious at this stage to endeavour to create a rigorous systematic review of CCI literature and to present the outcome thereof in a single journal article. In a similar vein, the tentative overview presented in this paper does not purport to adhere to the requirements of one of the other review types cited above. Instead, the article follows a less formalistic and selective approach in its review of CCI literature. This selective approach—further scoped and qualified in the next section ('Qualifying the Nature and Scope of the Selective CCI Literature Review')—provides a number of benefits:

- It highlights salient contributions to CCI that are of significant practical and/or academic importance;
- It provides some contours of the state of knowledge and the key directions of CCI research;
- It establishes a 'scaffold' for identifying and positioning future research topics;
- It provides a premise for a more comprehensive, systematic CCI literature survey;
- Because it deals with salient research done thus far, it offers an insight into CCI's academic origin, emergence, and development. As is the case with other academic subjects, such a self-awareness of origin and evolution could contribute to consolidating CCI as a distinctive sub-discipline; and
- It identifies research projects/institutions focused on CCI and, by so doing, encourages academic interaction in this field.

Qualifying the Nature and Scope of the Selective CCI Literature Review

This article has thus far emphasised the 'selective' nature and scope of the CCI literature review to be advanced. For the review to be academically credible, the meaning of the word 'selective' needs to be clarified. The review of literature advanced in this article is selective in that it limits its focus in the following five respects:

1) 'Available literature' is deemed as works in the **public domain**. Due cognisance is taken of the fact that state security structures internationally generate and possess CCI-relevant research and training material, some of which is unclassified but not

freely available. The same applies to some corporate entities and cybersecurity vendors that, for various reasons, do not openly share CCI material. Such material is categorically excluded from this review.

2) 'Available literature' is secondly deemed as referring to work published in **English**. The search which informed the review did not cover untranslated CCI-research possibly published in other languages.
3) The literature review is furthermore 'selective' in that it predominantly focuses on material which **explicitly addresses CCI**. While overlapping themes (such as cyber denial and deception, insider threat mitigation, cyber intelligence, and cyber threat intelligence) are important to CCI, a review of such literature would distract from the article's aim. For purposes of the article, CCI—which constitutes the literature overview's referent object—is defined as that sub-discipline of counterintelligence (CI) "aimed at detecting, deterring, preventing, degrading, exploiting and neutralis[ing] adversarial attempts to collect, alter or in any other way breach the C-I-A of valued information assets through cyber means" (Duvenage, von Solms & Corregedor 2015).
4) The literature review is selective in that it **does not purport be an inventory** of all CCI-focused work. Instead, in terms of academic works, the review reflects on peer-reviewed, published work featured in selected platforms, namely Scopus, EBSCO, Institute of Electrical and Electronics Engineers (IEEE), Explore, Springer Link, Google Scholar, and Proquest.
5) Lastly, the literature review only covers selected contributions **published as of 30 April 2018**.

Moving from the foregoing calibration of the CCI literature overview's selective scope, the next section explains the structural approach to be followed.

Structural Approach to the Selective CCI Literature Review

A literature review should, of course, be structured in a manner optimally achieving its aim and benefits. Given this literature review's earlier discussed aim and benefits, structuring the review per either (a) literature category or (b) chronology of publication was considered. On the one hand, the conventional approach of dividing reviews per literature category (such as articles, masters' and doctoral studies, books) would arguably have been the best suited to plot existing and to provide a scaffold for positioning future CCI research. On the other hand, a chronological literature review would be more effective to convey CCI's academic origin and development. To draw on the advantages both these styles offer, this article opted for a hybrid approach which incorporates a chronological thread with literature type. Practically, this means that the review overall is structured per the literature categories, namely peer-reviewed articles and papers, masters' and doctoral studies, books, and other literature. However, since the bulk of CCI academic work was produced per peer-reviewed articles and papers, this literature category (peer-reviewed articles and papers) is presented chronologically in order to convey CCI's origin and evolution.

This hybrid structural approach to the selective CCI literature review is depicted in **Figure 1,** below.

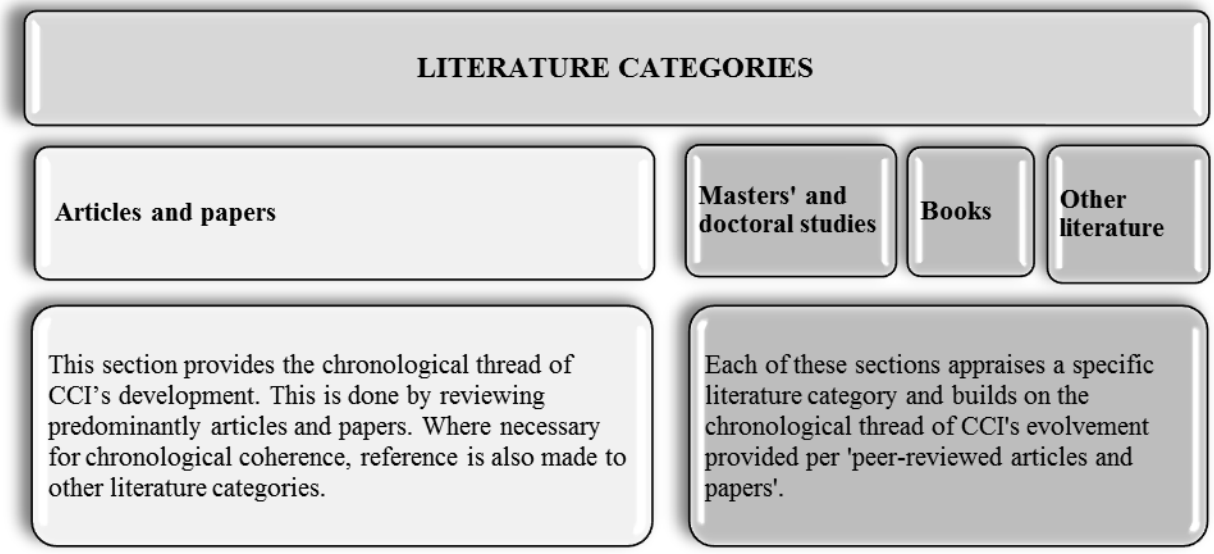


Figure 1: Structural approach to the selective literature review on Cyber Counterintelligence

Peer-Reviewed Articles and Papers

In line with **Figure 1**, this section enumerates CCI's evolution with specific reference to peer-reviewed articles and papers. Although somewhat of an over-simplification, CCI's progression as a distinctive academic sub-discipline consists of the following phases:

- Foundational phase (pre-2009),
- Phase in which Cyber Counterintelligence's emerged as an academic research theme (2009-2012),
- Current stage in which Cyber Counterintelligence crystallised into a distinctive academic sub-discipline (2012-present).

Foundational phase (pre-20

As far as could be surmised from available literature, the explicit term 'Cyber Counterintelligence' first emerged in the United States of America (U.S.) statutory security establishment during the early 2000s (see U.S. 2004; French & Kim 2009). Prior to the 2000s, however, CCI was practiced in the statutory security establishment of the U.S. and the security structures of some other countries. In this regard, French and Kim (2009) rightly assert that "cyber CI has existed *de facto* since the introduction of IT to intelligence, defence, and national security and has grown as FISs [Foreign Intelligence Services] have embraced cyber tradecraft".

Concurrent with CCI's *de facto* existence in statutory security circles, a few sporadic academic articles in the 1980s and 1990s expounded key CCI notions—although without using the actual term 'Cyber Counterintelligence'. Such notions included advocating for an integrated CI approach, which not only has defensive and offensive missions, but which also synchronises human and technical resources. The earliest peer-reviewed article found in consulted literature referring to such application of a CI approach to the IT realm is contained in the electronic library of the Institute of Electrical and Electronics Engineers (IEEE). This item, authored by Stone and Tucker (1988), is entitled 'Counterintelligence and unified technical security programs in security technology'. The authors expound effective CI as a "unified multi-disciplinary concept" consisting of "proactive and defensive" missions. Stone and Tucker (1988) further argue that "advanced technology" is part of the multi-disciplinary

CI entirety and thus serves both "proactive" (offensive) and defensive missions. While Stone and Tucker's (1988) paper centres on rectifying perceived deficiencies in the U.S. national CI endeavour thirty years ago, their key contentions regarding an integrated CI effort are still relevant today.

In a related further contribution in the IEEE library, Stone and Bluitt (1993) further expanded on the idea of executing "advanced technological countermeasures" as part of "a pervasive counterintelligence (CI) mandate". Also, Stone and Bluitt (1993) directed their paper specifically at the U.S. statutory CI effort.

No articles or papers of direct CCI-relevance were found in consulted literature for the seven-year period from 1994 through 2001. The first peer-reviewed article that specifically employs the term "cyber" in conjunction with "counterintelligence" appeared in a 2002 issue of the *Journal of Information Warfare*. As suggested by the title of the article, 'Dominating the attacker: Use of intelligence and counterintelligence in cyber warfare', Davey and Armstrong (2002) examined Intelligence and CI's role in augmenting cyber warfare. Cyberwarfare, in turn, is firmly positioned as a subset of Information Warfare. By "employing intelligence and counterintelligence techniques that are superior to those of the attacker", argue Davey and Armstrong (2002), the "cyberwarfare defender" is more likely to prevail. Davy and Armstrong (2002) urge a more "aggressive" posture that includes deception. One such example cited includes allowing the "attacker [to] gain access to information that is actually incorrect, thus providing incorrect intelligence". In respect to CCI's conceptual evolution and especially CCI's relation to cyber warfare, the contribution of Davy and Armstrong (2002) represents a milestone.

Like the work of Stone and Tucker (1988) and Stone and Bluitt (1993), Davey and Armstrong's 2002 article was part of CCI's foundational phase which, if gauged by academic publications, was characterised by only a few sporadic contributions. In as far as consulted literature goes, no CCI-relevant publications appear for the next five years (2002-2008).

Cyber Counterintelligence's emergence as a research theme (2009 -2012)

Following a sporadic foundational phase, 2009 marked CCI's emergence as a specific research theme attracting growing interest. In that year, a seminal article appeared in the launch edition of the *National Intelligence Journal* (French & Kim 2009). This was the first academic publication (in consulted literature) to use the term "Cyber Counterintelligence". In 'Acknowledging the revolution: The urgent need for Cyber Counterintelligence', French and Kim (2009) call on the U.S. intelligence community to move away from the notion that CCI is mostly part of "defensive Information Warfare". Instead, French and Kim (2009) urge the U.S. to be more active and offensive in its approach to CCI. The work's relevance extends beyond the U.S. context. French and Kim (2009) explicitly define CCI, explain CCI's missions within the context of CI, and offer various other insights on aspects useful to the further development within this field. Such aspects include the role of CCI in information warfare, critical infrastructure protection, and the CCI process and strategy.

No other peer-reviewed articles and papers were found in consulted literature for the 2009 through 2012 period. It must, however, be emphasised strongly that the absence of academic articles on CCI in consulted literature belies CCI's emergence as a research theme for three reasons. First, there were several CCI contributions during this period in other literature categories (see subsequent section entitled 'Other literature') and in publications not covered by this article's selective review. (See, for example, U.S. Naval War College 2018,

"Counterintelligence: Cyber Threat".) Thirdly, the nature and extent of academic contributions regarding CCI from 2013 onward strongly suggest that CCI attracted research interest in the preceding years (2009-2012). Phrased differently, research was done in the 2009-2012 timeframe, but the fruits thereof, in the main, are only reflected from 2013 onward.

Cyber Counterintelligence crystallisation as an academic sub-discipline (2013-present)

From 2013, a consistent stream of peer-reviewed papers and articles signalled CCI's emergence as an academic sub-discipline with significant contributions in English from researchers in the U.S., Sweden, and South Africa.

The bulk of academic contributions from the U.S. stemmed from Utica College's Master of Science Cybersecurity programme that offers CCI as a specialisation subject. This programme resulted in several "capstone project" papers (comparable to mini-dissertations in other countries) as well as a thesis, with CCI as a specific focus (Knowles 2013; Black 2014; Fieber 2015; Putnam 2015; Justiniano 2017). Since these contributions flow from a master's programme, they are discussed in more detail in a later section, which focuses on masters' and doctoral studies). Suffice to state here that this Utica research constitutes indispensable contributions to CCI on the conceptual, theoretical, and praxis levels.

Also, in recent years in the U.S., the concept of CCI has attracted interest from researchers at the Mitre Corporation. Branching out from their leading research on denial and deception in active cyber defence, the "applications of cyber counterintelligence" to "cyber defense" was subsequently examined (Heckman *et al*. 2015; Stech & Heckman 2018). Flowing from this research, Stech and Heckman (2018) contribute a book chapter, which is a undoubtedly one of the most incisive and significant works on CCI to date. (This contribution is discussed in more detail under 'Books'.)

Albeit considerably more limited in scope than the research in the U.S., papers delivered at two IEEE-endorsed conferences in 2013 reflected growing interest also outside the U.S. In August 2013, at the European Intelligence & Security Informatics Conference in Sweden, Sigholm and Bang (2013) submitted a paper entitled 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats'. Coming from a statutory military perspective, the paper is primarily aimed to advance a "comprehensive process that bridges the gap between the various actors involved in CCI". Sigholm and Bang (2013) present this model to specifically configure the "offensive CCI attribution process". The model essentially consists of all-source information flow and analysis architecture to be employed for attribution purposes.

On the heels of Sigholm & Bang in 2013, Duvenage & von Solms (2013) presented 'The case for cyber counterintelligence' at the 5th International Conference on Adaptive Science and Technology in South Africa. The paper defines key CCI concepts and advances conceptual constructs which explain CCI and its relation to CI.

Duvenage and von Solms' (2013) paper formed part of a dedicated CCI research project initiated at the University of Johannesburg's Cybersecurity Centre (UJCC) from which several other contributions would follow (University of Johannesburg 2018). UJCC's website describes the project's aim as establishing CCI as a multi-disciplinary field of academic enquiry within the South African context (University of Johannesburg 2018). To this end, the

UJCC project pursues two complementary yet parallel research streams, aimed respectively at:

1) Designing an overarching framework for conceptualising and explicating CCI as a distinctive academic field of enquiry, and;
2) developing a framework for a CCI maturity model for application by state and non-state actors within developing countries.

Building on Duvenage and von Solms' 2013 contribution, UJCC's first research stream progressively advanced conceptual constructs to explain (in an academic context) what CCI is, how it works, and how it dovetails with other academic disciplines and theory. Such notional constructs include a CCI-posture matrix model and a CCI process model, as well as a taxonomy of CCI Tactics, Tools, Techniques, and Procedures (TTTPs). These notional constructs were submitted per the following peer-reviewed papers and a journal article:

- Duvenage and von Solms (2014), 'Putting counterintelligence in cyber counterintelligence' in *Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece.
- Duvenage and von Solms (2015), 'Cyber counterintelligence: Back to the future' in the *Journal of Information Warfare*.
- Duvenage, von Solms, and Corregedor (2015), 'The cyber counterintelligence process – a conceptual overview and theoretical proposition' in *Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK.
- Duvenage, Jaquire, and von Solms (2016), 'Conceptualising cyber counterintelligence – two tentative building blocks' in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, DE.
- Duvenage, Sithole, and von Solms (2017), 'A conceptual framework for cyber counterintelligence—theory that really matters!', *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

UJCC's second research stream, to recapitulate, aims to develop a CCI maturity model with emphasis on governments and non-state actors in emerging countries (University of Johannesburg 2018). Peer-reviewed papers presented in this regard are as follow:

- Jaquire and von Solms (2017a), 'Towards a cyber counterintelligence maturity model', in *Proceedings of the 12th International Conference on Cyber Warfare and Security*, Wright State University, Air Force Institute of Technology, Dayton, OH, U.S.
- Jaquire and von Solms (2017b), 'Developing a cyber counterintelligence maturity model for developing countries' in *Proceedings of the 2017 IST–Africa Conference*, Windhoek, Namibia.
- Jaquire and von Solms (2017c), 'Cultivating a cyber counterintelligence maturity model' in *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland.

This section examined CCI's academic evolution via an overview of peer-reviewed articles and papers. The next section explores contributions to the field in the form of masters' and doctoral research.

Masters' and Doctoral Studies

The search term 'Cyber Counterintelligence' (and variations thereof) showed numerous masters' and doctoral studies of possible relevance to a CCI literature review. On closer analysis, however, most of these studies do not have CCI as a primary focus, and CCI is not explored in depth. Instead, CCI is cursorily referred to as part of the broader statutory CI mandate and mostly addressed within challenges faced by the U.S. Intelligence community. Ferguson's (2012) thesis entitled *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyber espionage* serves as one such example.

Bucking this trend, masters' studies completed at Utica College from 2013 onwards delivered contributions that are pioneering and invaluable with respect to the academic crystallisation and evolution of CCI. As was noted earlier, these studies are mostly "capstone projects". Also conducted within the context of U.S. national interests and security, these studies have much broader application and academic relevance than just in the U.S. Overall, important contributions have been made to explicating CCI on the conceptual, theoretical, and praxis levels. The following are some examples:

- In his research entitled *Applying computer network operations for offensive counterintelligence efforts,* Knowles (2013) identifies key aspects of Computer Network Operations (CNO). These aspects are then aligned with the broader intelligence and CI processes. In so doing, "counterintelligence skills and techniques" are leveraged to "assimilate cyber activities" into an organisation's Intelligence endeavour.
- Effective CCI, argues Black (2014), is multidisciplinary and involves unique skill sets. In his thesis, entitled *The complexity of cyber counterintelligence training*, Black proceeds with identifying the implications thereof for CCI training. Black then advances two useful notional constructs, namely (1) a CCI training model and (2) a CCI training proficiency path.
- As suggested by the research title, Putnam's (2015) *Digital mirrors casting cyber shadows - The confluence of cyber technology, psychology, and counterintelligence* emphasises CCI's multidisciplinary nature. Putnam points out that a successful CI (and thus CCI) programme should consider the opportunities that technology presents as well as certain psychological "principles of persuasions" and motivation. The study details some offensive and defensive CCI applications of these opportunities and principles. Emphasis is placed in this regard on optimizing the CCI targeting and the recruitment processes.
- The interplay between practice and theory which characterises Utica College's research is reflected in Fieber's (2015) commendable contribution: *The Iranian computer network operations threat to U.S. critical infrastructures.* Fieber analyses "the Iranian computer network operations (CNO) threat to U.S. critical infrastructures" and proceeds with recommending defensive measures to mitigate this threat. The paper culminates in a handy proposition on a phased, CCI process model "designed to mitigate conditions favorable to the attacker and restore the advantage to the organizational defenders" (Fieber 2015).
- Justiniano's 2017 outstanding and pioneering contribution, entitled *Advancing the capacity of a theatre special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone,* examines CCI's role in the U.S. military milieu with a focus on the hybrid threats posed by Russia and the role of CCI in mitigating and engaging this threat. Justiniano's (2017) research is indispensable reading for

examining CCI's role in hybrid warfare more generally. The study identifies critical CCI roles and skillsets before proceeding to propositions on integrating CCI with the U.S. "Cyber Mission Assurance (C-MA)" process in a manner supportive of "Theater Special Operations Command (TSOC)".

Although the bulk of post-graduate CCI studies in consulted literature originated from Utica College's Master's programme, the research project of the University of Johannesburg's Cyber Security Centre (UJCC), mentioned earlier, recently resulted in a master's dissertation and doctoral thesis focussing on CCI. These studies, which mirror UJCC's two CCI research streams (discussed in the article's previous section), are as follow:

- Jaquire (2018) *A framework for a cyber counterintelligence maturity model*, Doctor of Commerce thesis, University of Johannesburg, South Africa.
- Duvenage (2018) *A conceptual framework for cyber counterintelligence*, Master of Commerce dissertation, University of Johannesburg, South Africa.

The preceding two sections focused on academic, peer-reviewed literature—which ranges from papers and articles to masters' and doctoral studies. In the next section, books published on CCI are reviewed.

Books

The past two decades has seen an exponential rise in the number of books from reputable publishers dealing with aspects of cybersecurity. However, until very recently, even outstanding books that address aspects of high relevance to CCI make scant reference to CI and CCI. One such example is Heckman *et al*.'s (2015) *Cyber denial, deception and counter deception – A framework for supporting active cyber defense*. Despite the likelihood that this work sets the standard for future works on cyber denial and deception in general, only four sentences in the entire book mention the term 'counterintelligence', and there is no mention of 'Cyber Counterintelligence'.

The first book identified by the survey conducted for this article that has a significant CCI focus was published in 2012 with the title *Reverse deception—Organized cyber threat counter-exploitation* (Bodmer *et al.* 2012). Pitched as a practical guide for "IT security professionals", this text is highly significant from an academic perspective. The book comprehensively examines the role of CCI in countering cyber threats through the engagement of hostile actors. In addition to describing CCI Tactics, Techniques, and Procedures (TTPs), the authors also explore CCI on a conceptual level. This includes postulations on CI missions as well as CCI's interface with CI and other Intelligence fields. In nutshell, Bodmer *et al.* (2012) is essential reading for any researcher interested in CCI.

The next book to include a pertinent and significant CCI focus appeared under the editorship of Prunckun (2018) and is entitled *Cyber weaponry: Issues and implications of digital arms*. While the book has several chapters useful to CCI, Chapter Two is specifically dedicated to CCI. Under the title, 'Human Nature and Cyber Weaponry: Use of Denial and Deception in Cyber Counterintelligence', Stech and Heckman (2018) make a masterful contribution which anyone serious about CCI should consult. The chapter's primary aim is to advance a "cyber counterintelligence framework in active cyber defences". This system is "referred to as the cyber deception chain, to mitigate cyber spy actions within the cyber espionage 'kill chain'" (Stech & Heckman 2018). To lay a foundation for their CCI framework, Stech and Heckman explain the need for CCI. They proceed by appraising CI definitions, status, and existing

frameworks with a view on application to active defense in CCI. The text also observes the existing body of CCI academic research. Proceeding from this basis, Stech and Heckman (2018) present their CCI framework for "active cyber defense". This framework applies and synergises earlier postulations by Duvenage and von Solms (2014) and Prunkun (2014). Stech & Heckman (2018) demonstrate the framework's application by means of a hypothetical case involving the North Atlantic Treaty Organisation (NATO) and the Russian Federation.

Other Literature

In the past eight years, there has been an upsurge in literature dealing with "threat intelligence", "cyber intelligence", and "cyber threat intelligence" (Duvenage, von Solms & Corregedor 2015). Cybersecurity vendors, who are increasingly modelling their products and services on concepts derived from the state security and intelligence realms, in part fuel this upsurge. In contrast to the bourgeoning discourse on, for example, 'threat intelligence' and 'cyber intelligence', contributions to CCI are more limited but are growing. In the main, contributions offer high-level explanations of what CCI is and point to the advantages that CCI practices could have in proactively addressing cyber insecurity. While 'commercial', such works nonetheless contribute to explicating CCI in concrete terms and, in some instances, are consequently also of academic value. In this regard, works by Bardin (2011), Farchi (2012), and Lee (2014) can be singled out.

The following examples of article headlines give a sense of the nature of contributions in commercial online literature:

- 'Cyber counter intelligence', in *Defense Tech Magazine* (Carrol 2009);
- 'Ten commandments of cyber counterintelligence' by Bardin (2011), first featured on the IDG News Service's online platform *CSO Online*;
- 'Offensive counter-intelligence and cyberwarfare—A paradigm shift in information security' on the *Information System Control and Audit Association (ISACA)* website (Farchi 2012);
- 'To thwart hackers, firms salting their servers with fake data', in *The Washington Post* (Nakashima 2013);
- 'Cyber counter-intelligence makes a difference', featured on the South African ITWeb website (von Solms 2014);
- 'Cyber counterintelligence: From theory to practice' by Lee (2014), first published on the website of the cybersecurity vendor *Tripwire*;
- 'Shifting paradigms: The case for cyber counter-intelligence', in *InformationWeek* (Firestone 2015); and
- 'Counter-intelligence techniques may help firms protect themselves against cyber-attacks', published in *The Economist* (2015).

While videos are not typically included in literature reviews, CCI's incipient status as well as the merits of a contribution in video format, warrant an exception. This video covers a presentation by Evron (2014), then chairman of the board of the Israeli Computer Emergency Response Team (CERT). This high-level presentation provides a concise, yet incisive and conceptually sharp overview of key CCI fundamentals.

This section reviewed some examples of other literature on CCI. In the section that follows, the article concludes with findings and observations regarding the way forward.

Conclusion

This article advanced a tentative, selective literature review on CCI. This review shows CCI to have evolved, in less than a decade, from a research theme to a distinctive academic sub-discipline. As far as consulted literature is concerned, the bulk of peer-reviewed academic CCI research—documented in papers, articles and post-graduate studies—was conducted at Utica College (U.S.) and the University of Johannesburg (South Africa). The nature and focus of these institutions' CCI research are inevitably influenced by the respective contexts of a super power (U.S.) and an emerging mid-income country (South Africa). Perhaps because of these differences, the work done is complementary in several respects. Collectively, the research covers diverse topics ranging from general theory and conceptualisation; to CCI training, process models, and maturity frameworks, as well as CCI's application in the military domain. With respect to books and other literature categories, outstanding contributions include works by Stech and Heckman (2018), Evron (2014), Bardin (2011), Farchi (2012), and Lee (2014).

Although CCI is gaining traction internationally, this literature review shows that it is still in its academic infancy and, thus, offers numerous exciting research opportunities. A comprehensive literature review, much broader in scope than this article, would be an invaluable tool for CCI's progression. Such a review would have to cover research in languages other than English and in numerous other databases. Initial research on a comprehensive literature review is being conducted and is already delivering promising results. Those interested in cooperating in this venture are invited to contact the article authors.

Acknowledgments

The research presented in this article forms part of a project at the University of Johannesburg's Centre for Cyber Security. More detail can be viewed at <http://adam.uj.ac.za/csi/CyberCounter intelligence.html>.

References

Bardin, J 2011 'Ten commandments of cyber counterintelligence', *CSO Magazine*, 21 June, viewed 7 May 2015, <http://www.csoonline.com/article/2136458/identity-management/ten-commandments-of-cyber-counterintelligence>.

Black J M 2014, *The complexity of cyber counterintelligence training*, Master of Science dissertation, Utica College, New York, US.

Bodmer, S, Kilger, M, Carpenter, G & Jones, J 2012, *Reverse deception—Organized cyber threat counter-exploitation*, McGraw-Hill, New York, US.

Carrol, J 2009, 'Cyber counter intelligence' *Defense Tech*, 9 March, viewed 10 October 2014, <https://www.military.com/defensetech/2009/03/09/counter-cyber-intelligence>.

Davey, J & Armstrong, H 2002, 'Dominating the attacker: Use of intelligence and counterintelligence in cyberwarfare', *Journal of Information Warfare*, vol. 2, no. 1, pp. 23-31.

Duvenage, PC, Jaquire, VJ, & von Solms, SH 2016, 'Conceptualising cyber counterintelligence—Two tentative building blocks', *Proceedings of the 15th European Conference on Cyber Warfare and Security*, R Koch & G Rodosek (eds), Munich, DE,

viewed 2 November 2018, <http://adam.uj.ac. za/csi/docs/ECCWS2016_DJVS_PDF.pdf>, pp. 93-103.

Duvenage, PC, Sithole, TG & von Solms, SH 2017, 'A conceptual framework for cyber counterintelligence—theory that really matters!', M Scanlon & L Neihn-An (eds), *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, Ireland, viewed 11 December 2018, <http://adam.uj.ac.za/csi/docs/ECCWS_2017_DSV_Prof_MS.pdf>, pp.109-19.

Duvenage, PC & von Solms SH 2013, 'The case for cyber counterintelligence', *Proceedings of the 5th international conference on Adaptive Science and Technology,* IEEE, T Fogwill (ed.), Pretoria, South Africa, viewed 7 August 2014, <https://ieeexplore.ieee.org/document/6707493/>, pp. 1-8.

——2014, 'Putting counterintelligence in cyber counterintelligence', A Liaropoulos & GA Tsihrintzis (eds), *Published Proceedings of the 13th European Conference on Cyber Warfare and Security*, Piraeus, Greece, pp. 70-9.

——2015, 'Cyber counterintelligence: Back to the future', *Journal of Information Warfare*, vol. 13, no. 4, pp. 42-56.

Duvenage, PC, von Solms, SH & Corregedor, M 2015, 'The cyber counterintelligence process—A conceptual overview and theoretical proposition', *Proceedings of the 14th European Conference on Cyber Warfare and Security*, N Abouzakhar (ed.), Hatfield, UK, viewed 2 September 2018, <http://adam.uj.ac.za/csi/docs/ECCWS2015_Duvenage %20Von%20Solms%20Corregedor.pdf >, pp. 42-51.

Duvenage, PC 2018, *A conceptual framework for cyber counterintelligence*, Master of Commerce (Informatics) dissertation, University of Johannesburg, South Africa.

The Economist 2015, *Counter-intelligence techniques may help firms protect themselves against cyber-attacks*, viewed 24 May 2016, <http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves>.

Evron, G 2014, *Cyber Counter Intelligence: An attacker-based approach*, Honeynet Project Workshop, Warsaw, Poland, May 2014, viewed 7 October 2017, <https://www.youtube.com/watch?v=lJC3c-jMALU>.

Farchi, J 2012, 'Offensive counter-intelligence and cyberwarfare—A paradigm shift in information security', *Information System Control and Audit Association (ISACA)—Blog*, viewed 16 February 2016, <http://www.isaca.org/Knowledge-Center/..../Post.aspx?List=ef7cbc6d%2D9997%2D4b62%2D96a4% >.

Ferguson CJ 2012, *Increasing the effectiveness of U.S. counterintelligence: Domestic and international micro-restructuring initiatives to mitigate cyberespionage*, Master's dissertation, US Naval Postgraduate School, Monterey, California, US.

Fieber, TJ 2015, *The Iranian computer network operations threat to U.S. critical infrastructures*, Master of Science (capstone project), Utica College, New York, US.

Firestone, A 2015, 'Shifting paradigms: The case for cyber counter-intelligence', *InformationWeek*, 2 April, viewed 7 July 2016, <http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/a/d-id/1318929 >.

French, GS & Kim, J 2009, 'Acknowledging the revolution: The urgent need for cyber counterintelligence', *National Intelligence Journal*, vol. 1, no. 1, pp. 71-90.

Grant, MJ & Booth, A. 2009, 'A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies', *Health Information & Libraries Journal*, vol. 26, pp. 91-108.

Heckman, KE, Stech FJ, Thomas RK, Schmoker B & Tsow AW 2015, *Cyber denial, deception and counter deception—A framework for supporting active cyber defense*, Springer International Publishing, Cham, CH.

Jaquire, VJ 2018, *A framework for a cyber counterintelligence maturity model*, Doctor of Commerce (Informatics) thesis, University of Johannesburg, South Africa.

Jaquire, VJ & von Solms, SH 2017a, 'Towards a cyber counterintelligence maturity model', *Proceedings of the 12th International Conference on Cyber Warfare and Security*, AR Bryant & RF Mills (eds), Wright State University, Air Force Institute of Technology, Dayton, OH, US, pp. 432-40.

——2017b, 'Developing a cyber counterintelligence maturity model for developing countries', *Proceedings of the 2017 IST–Africa Conference*, Windhoek, NA.

——2017c, 'Cultivating a cyber counterintelligence maturity model', M Scanlon & L Neihn-An (eds), *Proceedings of the 16th European Conference on Cyber Warfare and Security*, Dublin, viewed 11 December 2018, <http://adam.uj.ac.za/csi/docs/ECCWS_2017_DSV_Prof_MS.pdf>, pp.109-19.

Justiniano, JE 2017, *Advancing the capacity of a theater special operations command (TSOC) to counter hybrid warfare threats in the cyber gray zone*, Master of Science (capstone project), Utica College, New York, NY, US.

Kim, JS 2018, *The importance of literature review in research writing*, viewed 10 January 2018, <https://owlcation.com /misc./literature_review>.

Knowles, JA 2013, *Applying computer network operations for offensive counterintelligence*, Master of Science (capstone project), Utica College, New York, NY, US.

Lee, RM 2014, 'Cyber counterintelligence: From theory to practice', *Tripwire (blog series 4)*, 4 May, viewed 4 January 2015, <http://www.tripwire.com/state-of-security/security-data-protection/cyber-counterintelligence-from-theory-to-practice/>.

Mallett, R, Hagen-Zanker, J, Slater, R & Duvendack, M 2012, 'The benefits and challenges of using systematic reviews in international development research', *Journal of Development Effectiveness, v*ol. 4, no. 3, pp. 445-55.

Nakashima, E 2013, 'To thwart hackers, firms salting their servers with fake data', *Washington Post*, 2 January, viewed 22 July 2018, <https://www.washingtonpost.com/world/national-security/to-thwart-hackers-firms-salting-their-servers-with-fake-data/2013/01/02/3ce00712-4afa-11e2-9a42-1ce6d0ed278_story.html?noredirect=on&utm_term=.ab586f749056>.

Prunckun, H 2018, 'Weaponization of computers', *Cyber weaponry: Issues and implications of digital arms*, H Prunckun, (ed.), Springer, Cham, CH.

Putnam, RT 2015, *Digital mirrors casting cyber shadows—The confluence of cyber technology, psychology, and counterintelligence*, Master of Science (capstone project), Utica College, New York, NY, US.

Sigholm, J & Bang, M 2013, 'Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats', *Proceedings of the European Intelligence and Security Informatics Conference (EISIC), IEEE*, Uppsala, SE.

Stech FJ & Heckman KE 2018, 'Human nature and cyber weaponry: Use of denial and deception in Cyber Counterintelligence', *Cyber weaponry: Issues and implications of digital arms*, H Prunckun (ed.), Springer, Cham, CH.

Stone, GM & Bluitt, K 1993, 'Future law enforcement and internal security communications architecture employing advanced technologies', *IEEE Publication CH3372-0/93*, pp. 194 - 202.

Stone, GM & Tucker RS 1988, 'Counterintelligence and unified technical security programs', *Proceedings of the IEEE International Carnahan Conference on Security Technology: Crime Countermeasures*, New York, NY, US.

United States of America 2004, Department of Defense, *Dictionary of military and associated terms (12 April 2011 as amended through 7 October 2004)*, viewed 7 January 2018, <http://www.bits.de/NRANEU/others/jp-doctrine/jp1_ 02%2804%29.pdf>.

United States of America (U.S.) 2018, *Counterintelligence: Cyber threat*, Naval War College, viewed 2 August 2018, <https://usnwc.libguides.com/c.php?g=661096&p=4695517>.

University of Johannesburg 2018, *The Cyber Counterintelligence Project—Centre for Cybersecurity*, viewed 16 April 2018, <http://adam.uj.ac.za/csi/ CyberCounterintelligence. html>.

von Solms, SH 2014, 'Cyber counter-intelligence makes a difference', *ITWeb*, viewed 11 November 2014, <http://www.itweb.co.za/index.php?option=com_content>.