Proceedings of the
14th European Conference on Cyber Warfare & Security

University of Hertfordshire
Hatfield, UK
2-3 July 2015

Edited by

Dr. Nasser Abouzakhar
University of Hertfordshire, UK

A conference managed by ACPI, UK

The Cyber Counterintelligence Process - a Conceptual Overview and Theoretical Proposition

Petrus Duvenage[1], Sebastian von Solms[2], Manuel Corregedor[3]
[1] Centre for Cyber Security, University of Johannesburg, South Africa
[2] Centre for Cyber Security, University of Johannesburg, South Africa
[3] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa.
duvenage@live.co.za
basievs@uj.ac.za
200503063@student.uj.ac.za

With the ineffectiveness of the defensive cyber security toolkit against advanced threats now commonly accepted, the quest is intensifying for viable and practical alternatives. While Cyber Counterintelligence (CCI) is gaining traction as such an approach, it is still in its infancy as a field of academic enquiry. This paper aims to contribute to an area largely underexplored, namely the conceptual structuring of the CCI process.

The paper argues a proposition on the CCI process to be of critical academic and practical importance. On an academic level, such a proposition serves as a notional concept for directing and delineating further research into CCI. On a practical level, the conceptual outline of the process provides an organising template for performing CCI work in practice. On both accounts the proposition is an idealisation - where the CCI process appears to be optimally effective and where everything goes as planned.

The paper is based on the premise that CCI can only be performed effectively as part of a multi-disciplinary Counterintelligence (CI) process. Moving from this premise, a contextual overview is provided of some existing postulations on the Intelligence, CI and CCI processes. Since existing propositions do not sufficiently explain CCI, an alternative process model is presented in the form of a diagram and a narrative conceptual outline. The aim is not to describe the process in detail, but to rather present a high-level theoretical framework.

Keywords: cyber counterintelligence, cyber-counterintelligence process, offensive cybersecurity, cyber security.

1. Introduction

Key events during 2015 have affirmed the continued deterioration in cyber security and the degree to which the landscape for the foreseeable future will favour the aggressor. There are various reasons perpetuating this trend. One of these is that current security approaches, for the overwhelming part, remain stuck in antiquated processes models which are compliance-driven, defensive in posture and which emphasise technical solutions at the expense of a more holistic approach.

In an endeavour to capitalise on the market demand for alternatives, commercial cyber-security vendors are increasingly drawing on concepts, principles and approaches that have their origin, and have been proven, in state security circles. Terms and marketing slogans that have thus been gaining popularity include “threat intelligence”, “cyber intelligence” “cyber threat intelligence” and to a lesser degree “cyber counterintelligence” (Deloitte 2014*a*-b, iSight 2014, Lee 2014*a*-*e*, Firestone 2015, INSA 2011). In this regard, KPMG (2013) states: “The number of cyber threat intelligence providers is on the rise and the concept of threat intelligence is now pervasive ..... Much can be learned from law enforcement and intelligence organizations. They have long recognized that intelligence-led decision making sits at the heart of their organizational culture and operations”. More recently Kaspersky’s General Manager for Security Government Solutions, Adam Firestone (2015) warned that threat intelligence is being overemphasised at the cost of sound CCI, which draw on established CI practices. Views and interpretations sharply diverge on what the said intelligence and CI-related approaches entail, and even more so on the processes, by which they are executed. (Deloitte 2014*b*, EMC[2] 2014, Firestone 2015, INSA 2013, INSA 2014*a*-*b*, VeriSign 2012, Lee 2014*a*-*e).*

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) ‘The cyber counterintelligence process – A conceptual overview and theoretical proposition, *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July, pp 42-51.

This paper holds CCI to be the most apt and viable in academically explaining and practically executing an integrated cyber security approach to confronting sophisticated threats. (The case for CCI has been argued in an earlier contribution – Duvenage & Von Solms 2013). While practised by state security structures for over twenty years, CCI remains poorly understood in the public and commercial domains. Also as a field of academic enquiry, CCI is in its infancy. While innovative research is important, it is equally imperative to first get the basics right. These basics entail the laying out and application of existing knowledge in a manner conducive to the CCI academic discourse. This paper builds on previous articles which defined various CCI concepts, positioned CCI as part of multi-disciplinary counterintelligence (CI) and explained CCI's defensive and offensive modes (Duvenage & Von Solms 2013, 2014). This paper is focussed on a further fundamental aspect, namely the CCI process. It seeks to address the problem statement: How can the counterintelligence process be structured conceptually?

To this end, the paper firstly defines concepts that are central to unpacking CCI and the CCI process. Given the prolific and confusing use of the terms 'threat intelligence' and 'cyber intelligence' when it comes to cyber security processes, care is taken to distinguish these concepts from CCI. The paper proceeds with examining the concept of a process model with a view on answering: What is a process model and why is it needed? This is followed by a brief examination of some existing process models. Existing postulations are demonstrated as describing aspects, but not the whole, of the CCI process. The paper proceeds with advancing a CCI process model which allows CCI to be executed as an integral part of the broader CI process. The paper concludes with highlighting the need for further research.

2. What is Intelligence, Counterintelligence and where does Cyber Counterintelligence fit in?

Any discussion of the CCI process firstly requires the clarification of the key concepts of 'Intelligence', CI and CCI. We can, after all not describe the process if we are not clear about what processes we are talking about. Adding to the need for such clarification, is the earlier noted prevalence in the use of "threat intelligence", "cyber intelligence" and "cyber threat intelligence" – sometimes loosely and without due consideration of their original and actual meanings of these concepts (iSight 2014, EMC^2 2014, Verisign 2012, KPMG 2013, Lee 2014*a*-*e*, INSA 2011, 2013, 2014 *a*-*b*).

Since these terms in an academic sense originate from conventional Intelligence Studies, the latter offers a useful premise. (In the interest of simplicity, and less otherwise qualified, the term Intelligence Studies is subsequently used as referring to both conventional 'Intelligence Studies' [sub-discipline of Political Science] and 'Business Intelligence' [which includes Competitive Intelligence]). While there is no consensus within Intelligence Studies on a single denotative definition, the following description conveys the meaning of intelligence in the statutory context: "Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers, the products of that process", the safeguarding of this information through counterintelligence and the carrying out of covert action (Lowenthal 2012, Godson 2001). In what can be confounding, Intelligence Studies' literature use CI juxtaposed with 'intelligence' (Sims 2009, Bodmer *et al* 2012). In this juxtaposed use, 'intelligence' is an abbreviated reference to the concept 'positive intelligence'. This double meaning underpins ambiguous uses of concepts also in the cyber field in general, and cyber processes in particular. Since the paper is primarily focused on a cyber-related process, these concepts are now distinguished in more detail. The distinction is graphically depicted in Figure 1 and then explained:

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition, *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July, pp 42-51.

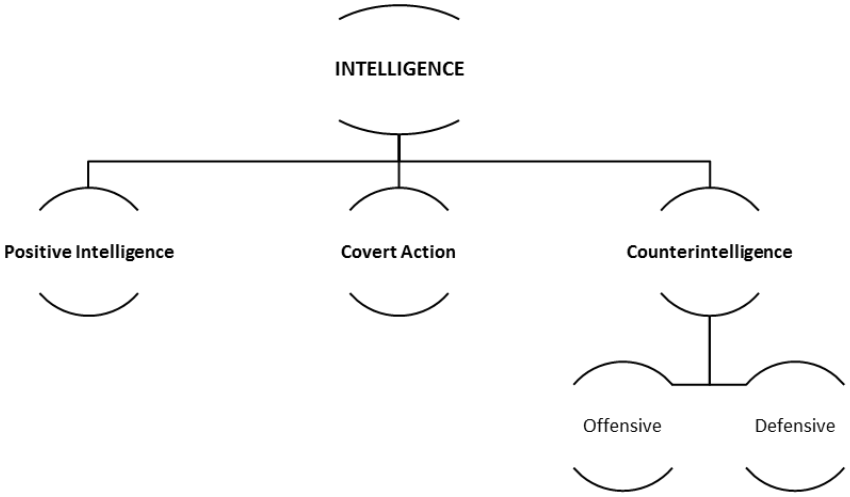

Figure 1: Intelligence and its primary disciplines (Created by the authors)

Simplified for the purpose of this paper, Intelligence is deemed to have three primary disciplines or fields, namely:

- *Positive Intelligence* that primarily aims to provide information "to facilitate one's own side achieving its ends." (Bodmer *et al* 2012). This information varies from analysed open-sources to an opponent's secrets obtained through espionage. As noted above, 'Intelligence' is frequently used interchangeably as referring to 'Positive Intelligence', with the context determining what meaning is implied (Sims 2009).
- *Covert action* which targets an adversary through the influencing of events, conditions, individuals, groups or institutions to the benefit of the client in a manner not attributable to the sponsor or offering plausible deniability. In the information sphere, covert action can take the form of propaganda, deception and disinformation (Godson, 2001).
- *Counterintelligence* is an abbreviated form for the countering of hostile intelligence activities. Counterintelligence defensively and offensively guards against adversarial intelligence (i.e. hostile positive, counterintelligence and covert action) operations (Prunkun 2012, Sims 2009).

Intelligence involves the execution of these primary disciplines in a mutually supportive manner and with functions such as collection, analysis and management performed in all three. Of these disciplines, CI is central to this paper and requires some further unpacking. CI relies on, and informs Intelligence. Similarly, CI protects and utilises some forms of covert action. CI denotes the collective of measures to identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to its own interests. It is directed against the actions of adversaries which include nation states, corporate entities, criminals, activists, terrorists, individuals and others. CI includes but is wider than conventional passive security. It also entails active-offensive actions to exploit and pre-emptively neutralise adversaries. CI should engage adversarial intelligence thrusts on the human (HUMINT) and technical (TECHINT) level. The cyber sphere is of course one of the technical conduits increasingly used by adversaries. It is in the latter arena which CCI functions as part a broader CI endeavour. More definitively, CCI can be described as that subset of multi-disciplinary CI aimed at detecting, deterring, preventing, degrading, exploiting and neutralising 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, 2014).

The preceding definition of terms underscores the paper's contention on the loose, confusing and often incorrect use of terms such as 'threat intelligence', 'cyber intelligence', 'cyber threat intelligence' and 'cyber counterintelligence.' It is clear from the explanation 'cyber intelligence' could have two meanings. Firstly, and in its broader meaning, cyber intelligence denotes the collective of (i) positive intelligence gathered through cyber means on the environment and adversaries; (ii) cyber counterintelligence and (iii) covert action in the cyber sphere. Secondly, in a narrower connotation, 'cyber intelligence' refers to the positive cyber intelligence endeavour. Positive cyber intelligence, will involve focussing on aspects

far wider than only cyber threat actors. In both its broader and narrow connotations, 'cyber intelligence' may entail the focussing, with cyber means, on actors who do not necessarily pose a cyber threat. However, it is not uncommon to find 'cyber intelligence' and 'cyber threat intelligence' being used as referring to information collected and analysed with a view on countering mostly high-end cyber threat actors (Deloitte 2014a-*b*, EMC^2 2014, Firestone 2015, INSA 2013, INSA 2014*a*-*b*, VeriSign 2012, Lee 2014*a*-*e*.) These terms are employed to describe intelligence and actions against high-end actors who themselves execute malicious cyber following, or as part of, intelligence operations. 'Cyber intelligence' and 'cyber threat intelligence', in their popular use, furthermore denote actions aimed at detecting, deterring and neutralising these adversarial attempts. Employing the definition of CCI provided above, however, it is clear that these terms then actual deal with some aspects of CCI.

This section has delineated concepts key to the later unpacking of CCI process model. The next section reflects on the importance of a CCI process model.

3. CCI process model – what is it and why is it important?

A CCI process model, in stating the obvious, is important since CCI is of pivotal importance. Properly conceptualised and executed, CCI offers a viable approach to proactively mitigate the high-end cyber threats. Proper conceptualisation and execution in turn, has a sound process model as requisite. This is so, since CCI is an intricate process, involving a wide array of means, methods and actions; executed in various modes and manners; and for complementary ends. It is practically and academically infeasible to attempt describing the CCI process in all its detail. The strategic management and guidance of the CCI process and the demands of academic research, call for a simplification at higher level of abstraction. At this higher level, a 'bird's eye view' ought to emerge of the overarching process that coherently binds and drives the work of CCI.

As process models in general, the CCI process should be presented as a model that acts as "idealizations of processes that are more subtle and more complex in practice." (Berkowitz & Goodman, 2000). A model ought to be simultaneously congruent with reality and an idealised, simplified representation of reality. Since it is an idealisation, a model is "an aim point, of what the process should look like if everything goes as planned." (Lowenthal, 2012) Academically, it serves as a notional concept for theorising and a premise or soundboard for research. More practically, it provides a template for the organised execution of CCI functions and activities. These activities are typically clustered in various steps or stages by means of which the CCI work is conducted.

Proceeding from this demarcation of the CCI process, the next section examines some existing propositions.

4. Current propositions on, or relating to, the Cyber Counterintelligence Process

Right from the onset, the CCI process needs to be distinguished from the cyber security process. Over years, the term cyber security process has come to denote the cluster of compliance-driven activities, in which the technical aspects predominate. The implementation and adoption practices as prescribed by ISO27001 and ISO22301 were, and are still seen, as providing cyber-security processes for all types of entities. While critically important, such processes are individually and wholly insufficient.

In as far as academic and published literature is concerned, contribution on models that pertinently deal with the CCI processes are rare. One of the most authoritative works on CCI, Bodmer (et al 2012) *Reverse Deception – Organized Cyber Threat Counter- Exploitation*, for example, does not advance such a process. A notable academic work, and one of few addressing the CCI process, is that of Sigholm & Bang's (2013) entitled *Towards Offensive Cyber Counterintelligence*. With the qualification that Sigholm & Bang's (2013) work is placed within a statutory military context, their paper sets out to offer a "comprehensive process that bridges the gap between the various actors involved in CCI" (Sigholm & Bang 2013). The work subscribes to Clark's (2004) "Target-centric Intelligence Process" which was specifically developed for statutory intelligence Analysis and not the whole range of Intelligence and CI functions. Graphically Clark's model can be depicted as follows:

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition, *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July, pp 42-51.

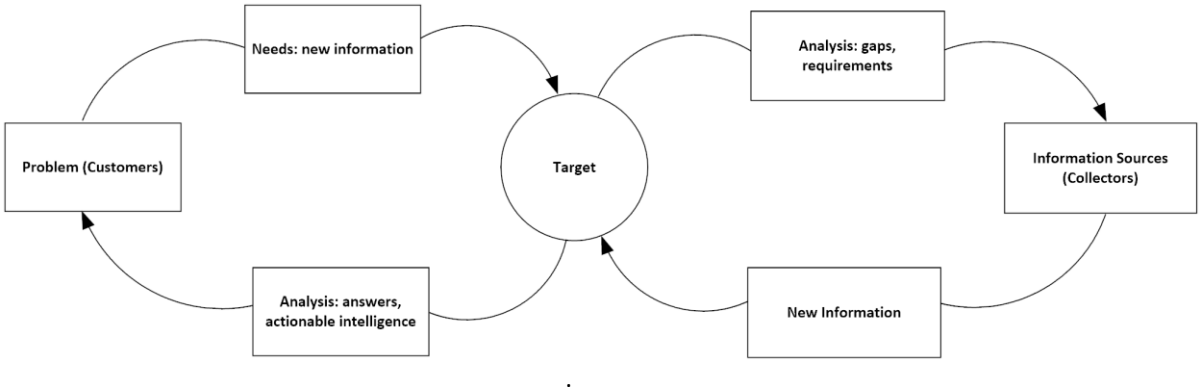

Figure 2: Target-Centric Intelligence Process (Adapted from Clark, 2004)

Drawing on this model Sigholm & Bang (2013) postulate a model for the "offensive CCI attribution process". Rather than an overarching, "comprehensive" CCI process, their proposition is on closer examination limited to one aspect of the CCI process, namely attribution and more specifically an information flow and analysis architecture to be employed for this (attribution) purpose. In their proposal, offensive CCI is neither incorporated with defensive CCI nor is it dovetailed with the broader CI process. This concept is illustrated in the following diagram provided by Sigholm & Bang (2013):

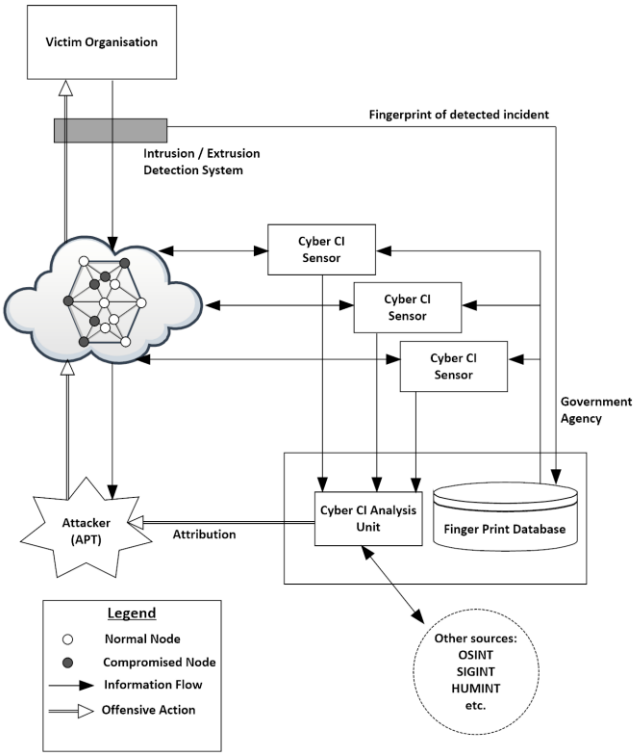

Figure 3: A layout of the offensive CCI attribution process (Adapted from Sigholm & Bang, 2013)

Literature published by cyber security entities offering CCI services do in some instances contain references to the CCI process. These vendors' contributions are cursory, aimed at expanding market share and not substantiated academic research. None of the promotional publications reviewed, purport to offer a model specifically linked to the CCI process. However, as noted earlier, the terms 'cyber intelligence' and 'cyber threat intelligence' in popular use often denote what is actually CCI. Consequently, this paper's review of the CCI process should also consider processes with these other tags. Process propositions under the tags 'cyber intelligence', and 'cyber threat intelligence' are more

common. Several of these propositions strongly draw on their descriptions of the 'cyber intelligence' process on what is known in Intelligence Studies as the traditional intelligence cycle. As it has done for more than sixty years within Intelligence Studies and statutory intelligence practice (Hulnick 2007), the traditional intelligence cycle now strongly influences thinking on Intelligence and CI processes in the cyber realm. Reduced to its essence, the intelligence cycle consists of the execution in a circular flow of the following activities: direction of the process through the clients expressing its intelligence requirements collection of information, analysis and dissemination:

Within cyber-security sphere, subscription to the intelligence cycle varies from simple adoptions at one end of the spectrum; to customised expansions at the other. Serving as an example of a simple adoption is VeriSign's (2012) *Establishing Formal Cyber Intelligence Capability (White Paper)* which states: "To successfully mount and implement an intelligence capability, it's essential to understand the intelligence lifecycle model… [the]… Traditional Intelligence Cycle comprise of Direction, Collection, Analysis and Dissemination." This description concurs exactly with the cycle as described above.

At the other end of the spectrum, KPMG (2013) advances a customised, expanded proposition as a "Basic Intelligence Operating Model" for "cyber threat intelligence". While dimensions such as "cyber intelligence strategy and budget" and "cyber intelligence sources" are added and described, the core of model – on closer analysis – still closely resembles the traditional intelligence cycle.

As would have been noted, the intelligence cycle in its simple or expanded format does not explain and / or mention CI. As is the case in Intelligence Studies, proponents of this cycle in cyber security realm may argue or imply that counterintelligence is performed throughout the cycle (cf Lee 2014 a-e, VeriSign 2012). The counterintelligence processes, this argument proceeds, mirrors and protects the intelligence cycle. In reality, these 'counterintelligence-throughout-the-cycle' and 'counterintelligence-follows-the-cycle' positions do simply not work. The intelligence cycle was originally conceived to explain positive intelligence and is not particularly good at that either. The following observation by distinguished Intelligence practitioner and scholar Arthur Hulnick (2007) is just as applicable to the cyber field: "[t]he intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence ... [C]ounterintelligence follows an entire different and unique path of its own ... It has nothing to do with the intelligence cycle. Instead there is counterintelligence methodology that is unique ... So when one looks at the pattern of counterintelligence functions, it does not look at all like the intelligence cycle."
If the intelligence cycle does not work for counterintelligence generally, it can of course not work in the cyber ream generally and for cyber counterintelligence specifically.

5. Are there alternatives in Intelligence Studies that can be applied to CCI?

Could Intelligence Studies offer a CI process that can be utilised as the basis for a CCI model? Contrary to what might have been expected, there are no current postulations offering a quick fix solution. Endeavours within Intelligence Studies over the past two decades to offer alternatives remains overwhelming directed to positive intelligence (Johnson 2007; Lowenthal 2012, Clark 2004). One of the very few propositions pertinently advanced for CI is that by Hulnick (2007). He proposes a "counterintelligence model" comprising of a five-clustered "pattern", namely "identification", "penetration", "exploitation", "interdiction" and "claim success". Summarised, Hulnick's description of the phases of the counterintelligence model are as follows:

- the identification of espionage adversaries;
- the penetration of adversarial espionage intelligence structures;
- exploitation – as referring to the collection of information (on adversaries) and the institution of measures such as deception;
- interdiction, which ensues when the "the case is turned over to law enforcement"; and,
- Public declarations by state authorities of successful counterintelligence actions.

Hulnick (2007) explicitly limits the model above to "active counterintelligence". In adding a qualification, "defensive measures in counterintelligence", are described as not fitting into "either the traditional intelligence cycle or the model just described." Within state security structures, these long-established

defensive measures are commonly referred to as Operational Security (OPSEC) and comprise the following steps five steps (US 1996): Identify critical information and other assets, Analyse threats, Determine vulnerabilities, Asses risks and lastly develop and implement Countermeasures.

Effective CI requires the integrated execution of offensive/active and defensive/passive modes. They are, after all, different sides of the same coin. Are there examples of integrative proposals which combine defensive and offensive CI dimensions? While none could be found in conventional Intelligence Studies (cf Duvenage & Hough 2011), propositions exist within Business Intelligence which attempt to combine the offensive and defensive dimensions. A seminal model in this regard was forwarded by Nolan (1997). While copyright restriction prevents an inclusion of Nolan's graphical depiction in this paper, subsequent Business Intelligence propositions, convey the same thinking. The following proposal by Brouard (2004) shown in Figure 4 is an example:

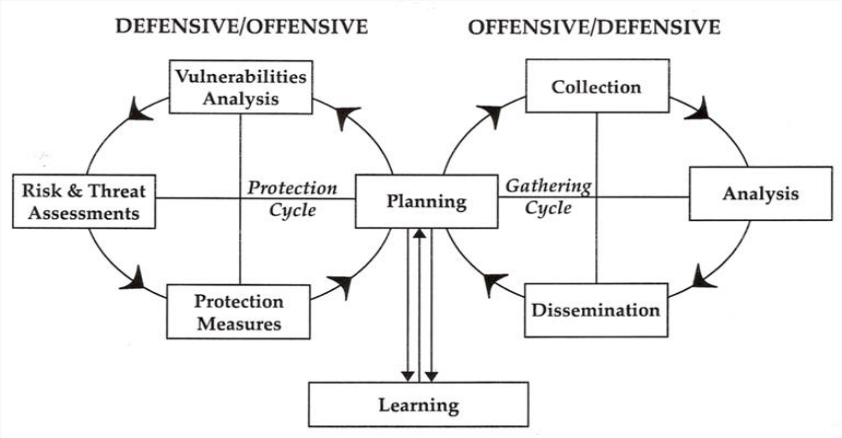

Figure 4: Intelligence Gathering and Protection Intelligence Process (Brouard, 2004)

Such models offer a useful contribution in their conceptual integration of sub-processes and the addition of a risk assessment methodology. Nonetheless, they insufficiently reflect the nature of the defensive and offensive counterintelligence thrusts as described above. They are also not granulated enough to serve either as an aiming point for practical execution or as a sounding board for further academic exploration.

6. A proposed Cyber Counterintelligence Process

This paper proposes a model that combines the respective steps of offensive and defensive CI into a single process. Within this process, the defensive and offensive sub-processes, while for a large part intertwined, also follow distinctive patterns. The paper limits itself to describing in more detail the offensive process. CCI, and to re-emphasize, is executed as part of the broader CI process. The CCI process thus looks, works and is inseparable from the CI process. Graphically, the CI process, with emphasis on CCI, is depicted in Figure 5 on the next page. This proposition builds on and contain extracts from Duvenage & Hough 2011.:

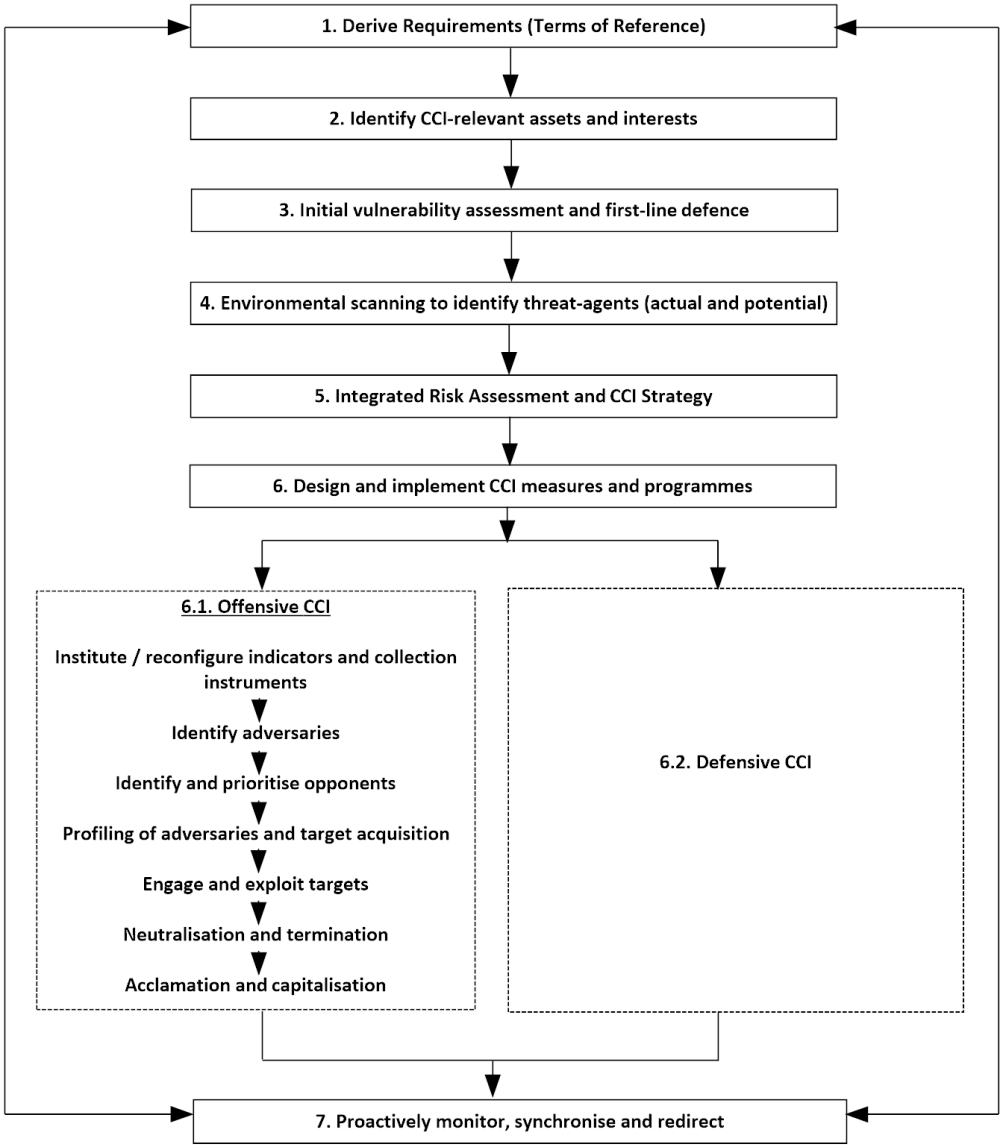

Figure 5: The Cyber Counterintelligence Process (Created by the Authors)

Although Figure 5 shows a linear sequence (i.e. neat finalisation of one step, directly followed by the execution of the subsequent steps), the CCI process is in reality multi-directional with steps being repeated and overlapping. This qualification also applies to the narrative description of the model below.

(1) Derive Requirements (Terms of Reference)

Like CI in general, CCI is not an end in itself. It serves the interest of a particular client – be it a government or business. The client expects from its CI apparatus to not only safeguard its vital interests and objectives, but to actively advance these. Ideally, CCI (as part of the broader CI process) would commence with the client clearly expressing its expectations. These would include: what cyber assets should be protected and what CCI should do to pro-actively promote government or company interests. This is very rarely the case. CI and CCI requirements are mostly derived and not received. They are derived through a meticulous appraisal of the client's objectives, intentions and strategy. Preferably these should be contained in Terms of Reference (ToR) endorsed by the client and within the parameters set by legal jurisdictions.

(2) Identify Assets to be Protected and Interests to be Advanced

Duvenage, P.C., von Solms, S.H. & Corregedor, M. (2015) 'The cyber counterintelligence process – A conceptual overview and theoretical proposition, *Published Proceedings of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, July, pp 42-51.

Resources are finite and CCI can only execute its signature role to defend and neutralise in a highly prioritised and selective manner. The right place to start is to ascertain what assets and interests in the information-cyber sphere are worthy of protection. In the case of nation states (or other sizable role-players) these info-cyber assets and interests – identified on the basis of the ToR - are threefold. Firstly, assets the state possesses which is central for survival and prosperity. Such assets include critical bodies of information, systems and infrastructure. Secondly, assets the state aspires to procure through cyber means (such as the secrets of adversaries). Thirdly, critical interests refer to the conditions the state seeks to realise (for example, the gaining of a competitive edge through obtaining adversarial secrets, adding additional layers to its defences or offensively undermining the C-I-A of adversarial systems).

(3) Initial vulnerability assessment and first-line defence

Although there are exceptions, the CI doctrine requires offensive action to be preceded by solid defence. Applied to CCI, the identification of real and aspirational assets and interests described above, is therefore followed by identifying the vulnerabilities in defensive and cyber-security measures which protect these assets and interest. This process would typically result in remedial action in relation to cyber, information, physical and personal security. It thus also involves CI specialisation fields other than CCI. This sub-process is again performed, but more exhaustively, as part of step 6.2. Care should be taken not to summarily close all 'holes' in the cyber 'fences'. Some of these could be exploited for offensive purposes later on in Step 6.

(4) Environmental scanning to identify threat-agents (actual & potential)

The assessment performed in the previous step mostly considered internal weaknesses and vulnerabilities. Effective CI needs to safeguard against and engage external threats. While opponents (competitors and adversaries) are common threat actors, risks can also be posed by technological and socio-political developments. While all of these are not a CI and CCI concern, they are considered for inferring actual and potential threats agents (of CI relevance). A common pitfall is to identify threat agents mainly on the basis of actors known to be active, adversarial and well-capacitated. The result is a self-feeding, atrophic CCI process with risks posed by previously unknown threat actors going undetected. The importance of innovative environmental scanning, which aims to identify potential threat agents hardly be overemphasised.

(5) Integrated Risk Assessment and Strategy

Considering the external and internal threats as well as vulnerabilities and weaknesses identified in preceding steps, the CCI process proceeds to perform an integrated risk assessment. The risk assessment identifies which CCI measures are obsolete, which require modification, and in which areas they are lacking. Decisions taken on CCI are formulated as part of a broader CI strategy which combines defensive and offensive dimensions. A balance needs to be maintained between, to paraphrase Nolan (1997), defensive CI tasks to 'close holes in the fence', and offensive CI that seeks to exploit the offensive opportunities that vulnerabilities offer.

(6) Design and implement CCI measures and programmes

While offensive and defensive measures are designed and implemented in synergy each sub-process has a unique mission and thus pattern of execution. This paper limits itself to outlining the offensive pattern which consists of the following six steps:

(6.1.1) Institute/reconfigure indicators and collection instruments

Since espionage is both a precursor and end-aim of sophisticated cyber breaches , the offensive sub-process commences with instituting and/or reconfiguring (a) indicators of adversarial cyber espionage and (b) own collection instruments. Whatever form these instruments take (honeynets, tarpits, footholds in on-line communities and sites, etc.), they will be developed and are constantly fine-tuned around most prized assets. In steps 6.1.3 and 6.1.4 these instruments will be further optimised to best collect on and then engage targets.

(6.1.2) Identify and prioritise intelligence opponents

In addition to information obtained through the preceding step, CCI will draw on the broader, all-source CI picture to identify opponents who are and potentially are targeting their own entities though intelligence actions such of espionage, covert action, and so on. Even the well-resourced entities cannot

offensively focus on all known and suspected opponents. Consequently, only prioritized opponents are elevated to actual/potential adversaries and pursued through further offensive action.

(6.1.3) In-depth 'profiling' of adversaries to arrive at targets

These offensive actions firstly entail focused information collection on, and subsequent in-depth profiling of adversaries. The focused collection of information is high-risk and high cost measures and could include cyber espionage. A crucial CCI collection requirement is to ascertain the instrumentalities and proxies adversaries use for intelligence activities. To this end, information procured through other conduits such as HUMINT and other TECHINT are also used. Depending on various factors some of these adversaries, their proxies or campaigns are not suited for offensive exploitation and as such will be channelled to defensive CCI.

(6.1.4) Engagement and exploitation of targets

As is apparent from the above, the acquisition of targets (prioritised adversaries and their proxies) for offensive action is an exhaustive process. In certain respects the acquisition of targets is the most complex part of CCI work. To adopt a Clark (2004) target-centric-type view at the start of the process, would thus clearly be a gross over-simplification which skips over critical segments of the CCI methodology. The engagement and exploitation of targets are at offensive CCI's core. These exploitations can take a myriad of forms and include escalated (more aggressive) collection, deception, manipulation, disinformation as well as the disruption of hostile intelligence activities. The ideal aim of CCI is the degrading and control of the adversary through their own cyber actions. The following observation by Codevilla (1992) rings true also in respect of CCI: "Action against the enemy through the enemy's own intelligence is the very consummation of CI." Usually this is best achieved through combining CCI within other forms of offensive CI. Deception through honeynets and sock puppets could, for example, be supplemented through disinformation fed through a human double agent.

(6.1.5) Neutralisation and termination

While the targets are to a certain level neutralised through exploitation, offensive CCI operations would typically have a 'neutralisation and termination' phase at the end of their 'life-cycle'. Termination can either be opted for (i.e. at own initiative at a pre-determined time) or necessitated by circumstances (such as indications that an operation has been compromised). Whatever the case, termination should be planned for in advance with two purposes. Firstly, delivering the final neutralisation 'blow' to the adversarial campaigns being engaged. Secondly, if executed skilfully, providing the 'seeds' for a subsequent 'generation' of CCI operations.

(6.1.6) Acclamation, reflection and identification of further opportunities

As with CI generally, CCI success ought to be followed by acclamation. There are two kinds of acclamations: Firstly, public acclamation in which aspects of the successful countering of hostile cyber intelligence activities would be cited. In the case of governments, such claiming of success is vital in justifying in the public eye the billions spent on Intelligence, CI and CCI. Moreover, public acclamation can be part of degrading an adversary. Secondly acclamation can be limited on the need-to-know principle. Sometimes entities should "try hard to keep successes secret so that they might be repeated. An oft-quoted CIA saying is, 'The secret of our success is the secret of our success.' "(Hulnick 2007). Whatever acclamation opted for, concluded CCI operations are assessed for lessons learned and to identify opportunities for further exploitation.

(7) Monitor, synchronise and redirect

Although indicated as a separate step in the interest of simplicity, CCI is continuously monitored and synchronised and redirected in accordance with the broader CI and Intelligence effort. The latter in turn, ought to be dovetailed with an entity's Objectives and Strategy. Intelligence and CI of any kind are instruments and not ends in themselves. The intelligence and insights gained through this endeavour influence Objectives, Strategy and thus eventually the ToR of the on-going Intelligence process of which CCI is a part of.

7. Conclusion

This paper moved from the premise that the nature of the current and future cyber threatscape necessitates an integrated cyber security approach with CCI at its core. Sophisticated threats, it was

argued, have intelligence actions (such as espionage) as its essential feature. The paper explained the importance of process models and found existing propositions to be insufficient in explaining the CCI. Nonetheless, the discourse on the intelligence and CI process generally, did provide elements which were useful for the construction of a CCI process model. The paper proceeded with postulating a theoretical framework for the CCI process. This postulation does not purport to offer radically new insights. It is, instead, a tentative proposal intended to stimulate future debate and theory constructions.

References

Bodmer, S. A. *et al* (2012) *Hacking Back: Offensive Cyber Counterintelligence*, McGraw-Hill, New York.

Berkowitz, B. D. & Goodman, A. E. (2000) *Best Truth: Intelligence in the Information Age*. New Haven: Yale University Press.

Brouard, F. (2004) "Business intelligence for Canadian corporations after September 11." *Journal of Competitive Intelligence and Management*, Vol 2, No 1.

Clarke, R. M. (2004) *Intelligence Analysis: A Target-centric Approach*, CQ Press, Washington D.C.

Codevilla, A. (1992) Informing *statecraft – intelligence for a new century*. New York. The Free Press.

Deloitte (2014*a*) "Cyber threat Intelligence: Moving to an Intelligence-driven cybersecurity model'" *Insight* , CIO edition. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/

Deloitte (2014*b*) *Transforming cybersecurity New approaches for an evolving threat landscape*. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/.../ 021114.pdf

Duvenage, P.C. & Hough, M. (2011) "The Conceptual Structuring of the Intelligence and the Counterintelligence Processes", *Strategic Review for Southern Africa*, University of Pretoria, Pretoria.

Duvenage, P. C. & von Solms. S.H. (2014) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol 13, Issue 4 .

Duvenage, P. C. & von Solms. S.H. (2013) "The Case for Cyber Counterintelligence", paper read at *5th International Workshop on ICT Uses In Warfare and the Safeguarding of Peace (IWSP'13)*, Pretoria, Soutyh Africa.

EMC^2 (2014) *Intelligence Driven Threat Detection and Response, (White paper).* Retrieved from http://southafrica.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf.

Firestone, A. (2015) "Shifting Paradigms: The Case for Cyber Counter-Intelligence", *InformationWeek*. Retrieved from http://www.darkreading.com/operations/shifting-paradigms-the-case-for-cyber-counter-intelligence/

Godson, R. (2001) *Dirty tricks or trump cards?* Transaction Publishers, New Brunswick.

Hulnick, A. S. (2007) "What's Wrong with the Intelligence Cycle", in Johnson, L K (ed), *Strategic Intelligence (Vol 4) — The Intelligence Cycle.* Praeger Securities International, Westport.

INSA Intelligence and National Security Alliance (2014*a) Operational Threat Intelligence.* Retrieved on 24 January 2015 from http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2014*b) Strategic Cyber Intelligence*, Retrieved on 24 January 2015 from http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2013) *Operational Levels of Cyber Intelligence*. Retrieved on 07 October 2014 from http://issuu.com/insalliance/docs/ insa_wp_cyberintelligence_pages_hir/16?e= 6126110/4859250

INSA (2011) *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*. Retrieved on 06 October 2014 from http://www.insaonline.org/i/d/a/Resources/Cyber_ Intelligence.aspx

iSightpartners. (2014) *What is Cyber Threat Intelligence?.* Retrieved from *http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief 1.pdf*

KPMG (2013) *Cyber threat intelligence: lessons from law enforcement*. Retrieved from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

Lee, R. M. (2014*a*), "An Introduction to Cyber Intelligence", *Tripwire*, blog series, Part 1, Retrieved 04/01/15 from http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

Lee, R. M. (2014*b*) "Developing Your Cyber Intelligence Analyst Skills", *Tripwire* , blog series, Part 2. Retrieved on 04/01/15 from http://www.tripwire.com/.../developing-cyber-intelligence-analyst-skills/

Lee, R. M. (2014*c*), "Cyber Intelligence Collection Operations", *Tripwire*, blog series, part 3. Retrieved on 04/01/15 from http://www.tripwire.com/.../cyber-intelligence-collection-operations/

Lee, R. M. (2014*d*) "Cyber Counterintelligence: Theory to Practice", *Tripwire* , blog series, part 4. Retrieved on 04/01/15 from http://www.tripwire.com/.../cyber-counterintelligence-from-theory-to-practice/

Lee, R. M. (2014*e)* "Cyber Threat Intelligence", *Tripwire*, blog series, part 5. Retrieved on 04/01/15 from http://www.tripwire.com/.../state-of-security/security-data-protection/cyber-threat-intelligence/

Lowenthal, M.M. (2012) *Intelligence: from Secrets to Policy*, fifth edition, CQ Press, California.

Prunckun, H. (2012) *Counterintelligence: Theory and Practice*. Plymouth, Rowman & Little Publishers.

Sigholm, J & Bang, M "Towards Offensive Cyber Counterintelligence - Adopting a Target-Centric View on Advanced Persistent Threats", paper read at the 2013 European Intelligence and Security Informatics Conference

Sims, J. E. (2009) "Twenty-first-Century Counterintelligence" in Sims, J. E. and Gerber, B. (eds.) *Vaults, Mirrors and Masks – Rediscovering U.S. Counterintelligence*. Georgetown University Press, Washington (D.C.)

United States of America, *Operations Security Intelligence Threat Handbook*, Interagency Operational Security Support Staff, 1996. Retrieved on 02 May 2007 from http:www.fas.org/irp/nsa/ioss/threat96/part03.htm

VeriSign (2012) *Establishing a Formal Cyber Intelligence Capability,* White Paper, retrieved on November 17, 2014 from https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf.