Proceedings of the 15th European Conference on Cyber Warfare and Security

Bundeswehr University
Munich, Germany
7-8 July 2016

Edited by
Gabi Rodosek and Robert Koch

A conference managed by ACPI, UK

Conceptualising Cyber Counterintelligence – Two Tentative Building Blocks

Petrus Duvenage[1], Victor Jaquire[2], Sebastian von Solms[1]
[1] Centre for Cyber Security, University of Johannesburg, South Africa
[2] Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa.

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

Several escalating trends are affirming the centrality of Cyber Counterintelligence (CCI) in effectively addressing advanced cyber threats of today and tomorrow. Yet, in comparison with the burgeoning academic and commercial literature on the related field of Cyber Threat Intelligence (CTI), CCI remains vastly unexplored. Outside the circles of governments' security apparatus, some large corporates and niche vendors that offer such specialised services, CCI is still obscure. While interest is gradually growing in CCI, this academic discipline is very young and largely uncharted. Leveraging off previous research by the aforementioned authors, this paper advances two further building blocks to contribute towards constructing this emerging discipline.

Building block 1 comprises a distinction between CCI and CTI. Such a distinction is necessary for clarity and has the advantages of allowing CCI to benefit from the extensive research work done in the CTI field.

Building block 2 consists of a multi-layered framework that explicates the different levels on which CCI functions, namely the strategic, operational and tactical functional levels. This framework progresses building block 1. While these functional levels have been described extensively in CTI literature, no such CCI-specific application could be found in literature within the public domain. Since it expounds CCI on the various levels that it functions, the framework contributes to a more nuanced academic conceptualisation of this discipline of CCI. On a practical level, the framework could serve as a notional guide for performing actual CCI work more effectively. The article concludes by reiterating the importance of CCI in addressing advanced threats and suggesting areas for further research.

Keywords: cyber counterintelligence, cyber threat intelligence, offensive cybersecurity, cyber counterintelligence levels, cyber counterintelligence maturity.

1. Introduction

In what has become a recurring theme in recent years, industry threat reports for 2015 to 2016 highlighted the escalating damage caused and threats posed by cyber actors of increasing sophistication (Kaspersky 2015, McAfee 2015, Crowdstrike 2016). This trend is accelerating despite a continuing increase in global spend on cyber security. In recent years, vendors have been pushing particularly Cyber Threat Intelligence (CTI) as a critical part of the 'solution' and it has evolved to one of the fastest growing cyber security sectors. The $1, 02 billion global spend on CTI in 2015, for example, represents a 129% increase compared to 2011 (Statista 2016, Info-security Magazine 2015). Further attesting to threat intelligence's rising prominence is the escalation in Google search results from a mere 18 700 in 2011 to 381 000 in February 2016 (Chismon & Ruks 2015, Google 2016).

As matters currently stand, the CTI market buzz and spending of resources have not by any measure translated in a corresponding mitigation of advanced threats – nor is it likely to do so in the near future. There are various reasons for this rather gloomy prognosis of which two will be highlighted in this paper.

The first reason is that a significant portion of products and services and that are marketed as CTI is not intelligence at all. They are mere re-labelled data feeds or anti-virus packages. Of course products of this nature have a role, but they are wholly insufficient against higher-end threats. It can rightly be argued that sound CTI as part of an effective cyber-security approach would be effective in addressing advanced threats. This is indeed the case, but only partially. CTI employed as part of an effective cyber-security approach will address a substantial portion of cyber threats. It will, however, not be effective against those high-end threats that should top our concern. For CTI to be effective against these threats, it needs to be embedded in counterintelligence (CI).

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June, pp 93-103

The second reason for CTI not delivering on expectations is that CI is simply not being embraced. Organisations with significant cyber assets are too slow to realise that we are faced with CI challenges rather than cyber security problems. Perhaps, we are still too attached to outdated, neat tables linking specific cyber actor types to certain methods and aims. In reality, the distinction between what was conventionally labelled as state-sponsored Advanced Persistent Threats (APTs) and the actions of other actors is blurring fast. In its 2015 Global Threat Report, Crowdstrike (2016) states, for example, that "the primary motivation behind global cyber activity has now shifted from disparate activities carried out by individuals, groups and criminal gangs pursuing short-term financial gain, to skilled adversaries driven by broader agendas." The cyber criminals' aim, asserts PwC (2016), currently "goes beyond targeting financial information to include a company's 'crown jewels' – customer data and intellectual property information, the loss of which can bring down an entire business." Various types of threat actors can and do cooperate (INSA 2011). The tradecraft, activities and even aims of various classes of threat actors in cyber space are often difficult to separate and reflect high skill levels in intelligence and counterintelligence (Moyo 2015). For state and non-state actors (such as criminal groups, some corporate entities) multi-vectored espionage (e.g. human and technical means) has become a precursor to extensive breaches. The addressing of such threats is CCI's signature role.

While CI/CCI awareness within board rooms appears to be growing, these concepts are far less known than CTI (cf. SpearTip 2015, The Economist 2015). Moreover, the symbiotic relationship that should exist between CCI and CTI is seldom addressed. Therefore academia has a crucial role in conceptualising CCI clearly. This paper proposes two further building blocks that could aid in conceptualising this discipline. Firstly, CCI is distinguished from CTI and the relationship between these constructs examined. Secondly, a multi-layered framework is submitted to explicate the different levels on which CCI functions. Notionally and practically, this multi-levelled examination provides clarity on what CCI is, what it does and what its relation with CTI is.

It needs to be emphasised that this paper builds on previous articles that defined various CCI concepts, positioned CCI as part of multi-disciplinary CI, detailed CCI's defensive-offensive modes and advanced a process model (Duvenage & von Solms 2015; Duvenage, von Solms & Corregedor 2015). While some aspects of previous work are concisely recapitulated (per Section 2.2), the latter is highly selective and could not address all aspect necessary for context.

The foregoing introduction highlighted the importance of CCI in addressing current and future cyber threats. Subsequently, the need to further conceptualise CCI was underlined. The next section delineates CCI and CTI by offering definitions and discussing the relationship between the constructs.

2. Conceptual clarification – what are 'Threat Intelligence' and 'Cyber Counterintelligence'

As suggested above, CTI and CCI are interrelated yet distinct concepts. Delineating these two constructs is important, since each has a unique and complementary role in ensuring cyber security. Moreover, a clear differentiation would enable CCI to draw on extensive CTI literature in a manner that is academically credible and responsible.

2.1 Defining 'Cyber Threat Intelligence'

The rapid market growth in the market of CTI products and services has been accompanied by a proliferation in terms and definitions. "Threat intelligence", "cyber intelligence", "cyber threat intelligence" are sometimes used interchangeably and sometimes with different connotations (Deloitte 2014, Schoeman 2015, EMC^2 2014, INSA 2013, INSA 2014*a-b*, Lee 2014*a-b*.). A dissection of all these terms will distract from the paper's main focus and be more confusing than helpful. In the interest of simplicity CTI is henceforth employed in the paper as the umbrella term. Schoeman (2015) rightly states that CTI has evolved in a "catchall term for a vast array of different technologies, methodologies and ideas." Products and services sold under this banner can vary extensively in scope, usability, aims and contents (Chismon & Ruks, 2015). At the one end of the spectrum CTI can be just anti-virus signatures at a much higher cost; while at the other end, it can mean an overarching approach central to an organisation's strategy (Schoeman 2015, Riley 2015).

The term 'threat intelligence' has its roots in the concept 'intelligence' as used with state security apparatus and Intelligence Studies. Depending on context, 'Intelligence' can have several meanings within Intelligence Studies. Intelligence can denote the overarching discipline that comprises Positive Intelligence, Counterintelligence and Covert Action. Sometimes Intelligence is often employed as a shortened reference to Positive Intelligence. The term Intelligence could furthermore refer to the outcome of a process that delivers actionable, analysed information. These meanings and applications thereof in the cyber realm were explored in an earlier article (Duvenage, von Solms & Corregedor, 2015). Suffice it to note here that 'intelligence' used in 'cyber threat intelligence' – and as henceforth applied in this paper – means actionable, assessed information on a cyber-related hazard to an entity. This is in line with Gartner's defining of threat intelligence as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" (Schoeman 2015). Deriving intelligence from information and data requires analysis performed by humans. Tools and data feeds cannot by themselves provide threat intelligence (Schoeman 2015). In this regard Lee (2014*a*) states "Intelligence of any type requires analysis. Analysis is performed by humans. Automation, analytics and various tools can drastically increase the effectiveness of analysts but there must always be analysts involved in the process." In summary it can thus be said that data is processed and refined to produce information. Information is in turn analysed and presented in a format that is actionable and constitutes intelligence. In the case of CTI, this is intelligence produced on cyber-related hazards.

Ideally CTI should provide intelligence on a full spectrum of adversarial action in the cyber sphere from decision to execution. INSA (2013) provides the following breakdown of these actions and what cyber threat analysis should consider:

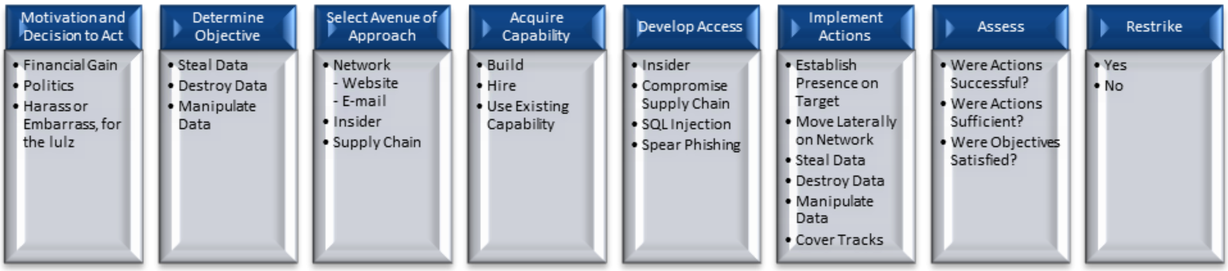

Figure 1: Adversarial Pathway to an Attack as aid for Cyber Intelligence Analysts (INSA 2013).

CTI is thus not a "collection discipline" but more of an "analytical discipline" that informs "decision makers on issues pertaining to all levels in the cyber domain", namely the strategic, operational and tactical (Mattern et al 2014). On a strategic level, CTI should identify the intent, capability and opportunity that actual and potential malicious actors could have (Lee 2014*a*). On a tactical level, CTI identifies network threats and informs responses. Bridging the mostly non-technical strategic and narrow technical/tactical layers, the operational level is focussed on an organisation's immediate operating environment (INSA, 2014*a*).

Moving from the conceptualisation of CTI in the preceding paragraphs, the notion of CCI and its relation with CTI are now examined.

2.2 Delineating Cyber Counterintelligence and its relation with Cyber Threat Intelligence

What then is CCI, how does it differ from CTI and what is the relation between these fields? As will be shown in this subsection, CCI's focus is paradoxically narrower and broader than that of CTI. CCI is narrower in that its external dimension is directed against a very specific category of "cyber hazards", namely that of hostile intelligence actions playing out in the cyber sphere. However, CCI is also broader than CTI in several respects. CCI is for one not limited to the producing and disseminating of intelligence. It also engages internal and external threats through a wide array of offensive and defensive measures. These measures are executed in synergy in accordance with the principles of traditional, multi-disciplinary CI.

2.2.1 Demarcating Counterintelligence

Therefore, CCI and its relation with CTI, can only be understood and definitively defined within the context of CI generally. CI has been discussed in some detail in earlier contributions (Duvenage & von

Solms 2015; Duvenage, von Solms & Corregedor 2015). Since familiarity with the concept CI is essential for further unpacking of CCI and for contextualising the CCI framework, a brief recapitulation is provided here.

As suggested by its composite terms ‘counter’ and ‘intelligence’, counterintelligence is essentially about the countering of hostile intelligence actions. Of these hostile intelligence actions, espionage (i.e. secret intelligence gathering) is perhaps the best known example. In addition to espionage, hostile intelligence activities also can include covert action (e.g. non-attributable influencing and deception). These hostile intelligence actions target valuable bodies of information as well as the people, processes, technologies and repositories wherein it resides. Hostile intelligence actors typically execute their actions through a combination of human (‘spies’) and technical means. The exploitation of the cyber sphere to realise intelligence ends is part of such technical means.

The CI mission is to safeguard, but also to advance organisational strategy and assets actively. In order to execute its mission, CI has three main thrusts namely an offensive focus, a defensive focus and an intelligence function. These three dimensions constitute the CI trident. In execution of these three dimensions, CI relies on an extensive array of means, measures and methods. In traditional CI, this ranges from defensive information security measures to the offensive running of a mole or double agent. These thrusts and their relation with means, measures and methods are explained in more detail as part of the discussion on CCI.

To summarise CI can be defined as the activities conducted to “identify, deter, exploit, degrade, neutralise and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to the own interests” (Duvenage, von Solms, Corregedor 2015). Effective CI takes on, and guard against, hostile intelligence on a human (HUMINT) and technical (TECHINT) level. This technical level includes the cyber sphere as one of its conduits.

2.2.2 Defining Cyber Counterintelligence and its relation with Cyber Threat Intelligence

Building on the preceding outline, CCI can be “described as that 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” (Duvenage & von Solms 2015; Duvenage, von Solms, Corregedor 2015). As is clear from this definition, CCI shares CI’s defensive and offensive missions (Bardin 2011). Defensive CCI seeks to deny an opponent the access it seeks, to guard the organisation against insider threats and vulnerability (Bodmer et al 2012). Offensive CCI’s signature role is engaging and exploiting adversarial cyber actions to own advantage. It aims to neutralise a competitor’s intelligence efforts through measures ranging from deception and manipulation to the degrading of adversarial cyber intelligence activities and systems (Farchi 2012, Lee 2014*b*). This exploitation can take the form of deception, disinformation and degrading. The ultimate aim of offensive CCI should be the control and exploitation of an adversary through the manipulation of its cyber intelligence action.

Effective defensive and offensive CCI cannot be executed blindly but is guided by intelligence. Similar to CTI, analysis is necessary to generate intelligence from information and data collected. Since CCI is about the outmanoeuvring of intelligence adversaries, high-quality analysis is imperative. In this regard Godson (2001) states: “Perhaps the queen of the counterintelligence chessboard is analysis – both offensive and defensive.” CCI requires this high-grade intelligence on own cyber-relevant vulnerabilities (weaknesses of people, processes, facilities and technologies) actual and potential adversaries as well as on a strategic level, the macro-environment.

CCI executes it offensive-offensive missions and the collection of data and information through a wide array of measures (Bardin 2011). It must be emphasised that care should be taken not to categorise a CCI measure or methods rigidly as defensive or offensive. In numerous instances a measure can be of service to both the defensive and offensive missions. In addition, several of the offensive-defensive measures collect data or information of relevance to the CCI intelligence mission. These measures and the multi-purposes they serve are shown in the taxonomy provided in Table 1 (next page).

Table 1: A taxonomy of CCI Means, Methods and Measures (updated and adapted from Duvenage & von Solms, 2015)

<table>
<tr><th colspan="4">Defensive Mode</th></tr>
<tr><td colspan="2">*Passive* ⟷</td><td colspan="2">*Active*</td></tr>
<tr><td>*Deny*</td><td>*Detect*</td><td colspan="2">*Collect*</td></tr>
<tr><td>Physical Defensive</td><td>Personnel/User Defensive</td><td colspan="2">System Defensive</td></tr>
<tr><td>Protects against:
• Unauthorised access to facilities and systems
• *In loco* theft of data, hardware
• Introduction of malware through physical access to systems
• Unauthorised altering or destruction of data
• Physical destruction or access denial
• Unauthorised reading (acoustic, visual, radiation, analogue, signals)
• While not conventionally seen as a Physical Defence, **supply-chain management** has a physical defensive function. It is also part of System Defences as an enabler.</td><td>Consists of aspects such as:
• IT and user personnel **vetting**, re-vetting, confidentiality agreements and monitoring
• Personnel security measures, **BYOD** user parameters or exclusions
• **User programmes** in cyber security that cover policy and procedures for the handling of security-related incidents, malfunctions and recovery.
• Overlapping with system defences, the use of **software decoys and traps** to mitigate the insider threat
• **Investigations** focussed on cyber security incidents involving personnel. Could also include digital forensic investigations.</td><td colspan="2">Comprises a combination of:
• Hardware and software such as:
✓Network perimeter-based security (filters, certain firewalls, **IDS** and **IPS** etc.) Malware scanners.
✓Integrated automated systems/tools (that collect and evaluate information about devices connected to a network, activities thereon – inclusive of intrusions). Examples of such tools, discussed further on in the table, are decoys, honeypots and behavioural analyses toolsets.
✓Overlapping with the latter, depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration.
• Processes (such as supply-chain management are also in part system defences).
• **Vulnerability assessments**, **penetration testing and verification testing** (on products, systems, software and secure code).
• Incident and threat monitoring, identification, **investigation** and response. A **CERT** is per definition defensive – although it might contain offensive elements in its responsive action.
• **Port level security and BYOD** regulation in as far as network interfacing is concerned (Also part of Personnel Defences).</td></tr>
<tr><td></td><td colspan="3">• Commercial Cyber Threat Intelligence products, services and platforms.</td></tr>
<tr><td rowspan="2"></td><td colspan="3">• The use of **software decoys to mitigate the insider threat** is an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
<tr><td colspan="2">• **Investigations** focussed on **internal** cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• **Investigations of external cyber intrusions** could be part passive and part active system defence.</td></tr>
<tr><th colspan="4">Offensive Mode</th></tr>
<tr><td colspan="2">*Passive* ⟷</td><td colspan="2">*Active*</td></tr>
<tr><td>*Collect*</td><td>*Disrupt*</td><td>*Exploit*</td><td>*Destroy*</td></tr>
<tr><td colspan="2">• **Collection** of information on and the monitoring/surveillance of the cyber sphere to detect cyber adversaries and their exploitation of the cyber sphere in a manner that is not own-network restricted – (i.e. requires more than deployment of systems described under defensive mode). Could, depending on configuration also include IDS/IPS, honey-client applications (as opposed to host-based honeypots), luring and some forms of data mining.
• The recruitment and handling of **virtual agents** on underground forums (under true or false flag) that can serve the purpose of enticement, collection and/or exploitation. (Under certain circumstances virtual agents can also develop into HUMINT assets).</td><td>Measures taken to **exploit and neutralise** adversaries activities in the cyber sphere:
• **System and honeynet configured offensively** with the aim of enticing, exploiting and deceiving adversaries. False information is displayed to adversarial reconnaissance tools, network scanners and listeners, etc. This has as one of its aims to lead adversaries in the direction of your own preference.
• Utilisation of **virtual agents** for offensive purposes.</td><td rowspan="2">**Cyber warfare**, in the full extent of the term, is typically excluded from the mandate of civilian intelligence communities. A cyber warfare capability should be flexible and allow utilisation without, or in conjunction with, kinetic war.

Nevertheless, a top class civilian CCI outfit will need to have the authority and capacity to very selectively conduct operations that have cyber warfare characteristics, utilising cyberwarfare- related techniques. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions and events without revealing the sponsors identity.)

Within business, the use of offensive measures will be determined by the legislative and regulatory framework within which the entity operates.</td></tr>
<tr><td colspan="3">• **Cyberespionage** on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets etc) on the basis that adversarial networks are targeted actively and exploited in accordance with strategic and operational objectives.</td></tr>
</table>

The preceding discussion and table show that CCI, in contrast to CTI, is not only about the delivery of intelligence products. It includes active and passive measures instituted as part of an integrated approach. Moreover, the intelligence that CCI generates covers a scope significantly wider than the actor-centric intelligence associated with CTI. From both these perspectives, CTI can thus be posited as a constituent part of CCI (cf Lee 2014*b*). Figure 2 – that should be read with the qualification on the term 'intelligence in subsection 2.2 – depicts this relationship graphically.

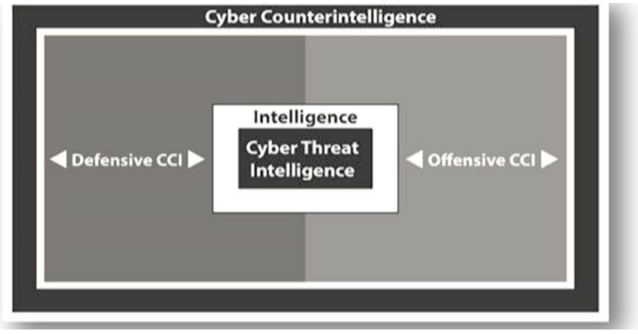

Figure 2: The relationship between Cyber Counterintelligence and Cyber Threat Intelligence (authors)

This section showed CCI as a multi-faceted CI sub-discipline that participates in, but extends beyond conventional cyber security. CCI was concluded to include CTI but to be much wider in respect of scope and nature of measures undertaken.

3. Towards a multi-layered CCI framework

Effective CCI is not only multi-facetted, but also stratified. To be optimal CCI needs to involve all organisational layers from the C-suite to line-functionaries. The levels conventionally ascribed to statutory intelligence –namely strategic, operational and tactical – provide a useful approach for explaining CCI. Although these levels are described in literature dealing with CTI, no postulation could be found in open-source literature on a multi-layered framework for CCI. Works of note in the CTI field include those by Mattern (et al 2014), Friedman & Bouchard (2015), Chismon & Ruks (2015) as well as a series of papers compiled by the Intelligence and National Security Alliance (INSA 2011, 2013, 2014a, 2014b, 2015). The cited works were foundational to the framework provided in Table 2 and were also applied for the subsequent narrative description of the CCI levels.

Table 2: A multi-layered CCI framework

	Strategic	Operational	Tactical/Technical
CI mission	• Advance and protect organisational interests through defence against, and the offensive engagement of, adversarial intelligence activities. This is achieved through the following functions: detect, deny, deter, deceive, degrade, and/or disrupt.		
CCI mission	• As above, when the adversary uses cyber as a conduit or a cyber asset is a target.		
Leadership	• C-level	• Senior & Middle Management	• Line and team leaders
Interface with CI	• Organisational, Intelligence and CI Strategies • All-source CI feed	• Multi-disciplinary programmes and operations	• Multi-disciplinary projects and continuous line-functional interaction
Referent objects	• Organisation's 'crown jewels' • Critical information and cyber-assets sought (e.g. adversary's 'crown jewels') • Conditions (competitive advantage)	• People, processes, systems, procedures (personal security, ICT architecture, supply-chain management) • Own intelligence programmes	• Systems, networks, and devices • Network Security Operations • C-I-A (confidentiality, integrity and availability)
Interrogatives	• Who, why?	• Who, Where, When, How?	• What, How?
Adversarial progression (Impact chain)	• Motivation, intent and decision, objective	• Objective • Avenue of Approach • Capability or perceived capability, develop access	• Develop network access, implement, assess, restrike • Payloads and payload delivery mechanisms
Level of adversarial role-player focussed	• Sponsors, opponents, Intelligence capacity	• Intelligence structures, groups, campaigns	• Individuals, TTPs, incidents, actions (on-the-network)

	Strategic	Operational	Tactical/Technical
Indicators of targeting and compromise	• Geo-political, sector/industry 'flags' • Analogous events • Adversarial strategy and business decisions	• Operational disruption • Organisational and/or revenue decline • Information leakage	• Breach in the CIA of cyber and / or information security milieu • Identification of malicious code, intrusion, threat exploitation
Analysis output	• High-level, strategic appraisals • Strategic warning and advisories	• Operational reports (CCI operations, threat, damage and vulnerability assessments, alerts, warnings) • Trend analyses	• Tactical and technical information reports • Alerts and warnings
Consumers of CCI products	• C-Level and operational management (selectively)	• Line-functional managers, CI analysts and CCI specialists.	• CCI analysts • CCI technical personnel
Means, methods and measures (Offensive, defensive and collection)	• Multi-discipline CI • Strategic direction of means, methods and measures in Table 1.	• As in Table 1 • Interlocked with operational and tactical CI.	
Cyber threat intelligence (Sourced)	• White papers, commissioned and non-commissioned research.	• Platforms.	• Data feeds.
Skillsets required (Line-functional)	• Sound knowledge of business and industry • Specialised knowledge and skills in Intelligence, multi-disciplinary CI and CCI • Strategic analysis and management	• Multi-disciplinary CI • CCI operational and/or technical specialisation • Operational management • Elements of both strategic and tactical	• ICT, information security • Systems, software development,programming, scripting, • Ethical hacking. • CI and CCI tactical /technical specialisation (also HUMINT) • Technical cyber defence and collection • Social sciences, languages • Engineering and Reverse Engineering

Within the confines of a conference paper, the framework above cannot be discussed in detail. Not even each of the vectors can be narratively explicated. The subsequent sub-sections thus do not rigidly mirror the table, but rather aim to provide a bird's eye view of the different levels on which CCI is executed.

3.1 Cyber counterintelligence on the strategic level

In his benchmark work, Prunckun 2012 rightly asserts "executive responsibility" as CI's "first and highest tenant". For CCI to be successful, the organisation's executive management (C-suite) need to understand and sanction CCI's mission to advance and protect organisational interests through defence against and the exploitation of adversarial, cyber-related intelligence activities (cf INSA 2014*b*, Chismon & Ruks 2015). Practically, the C-level executive assigned with leading the CI aspect will be responsible for also directing the CCI effort. The executive's responsibilities include obtaining the collective executive management's approval of CCI strategy, priorities and resourcing. In some instances, the executive would selectively also seek endorsement – normally from the CEO – for high-risk and high-cost programmes. The actual CCI work on a strategic level is performed by a team consisting of seasoned CCI specialists, multi-disciplinary CI specialists, strategic analysts (business and CI) and various other experts relevant to the organisation's core business.

CCI informs the C-suite mainly through high-level products and presentations that include estimates, threat and risk assessments as well as advisories. These products are informed by appraisal all-source CI operational reports as well as an extensive all-source scanning of the macro-environment for CCI-relevant trends and drivers that could affect the organisation (INSA 2014*b*). External CTI products sourced would mainly be white papers as well as commissioned and non-commissioned research papers (Chismon & Ruks 2015). A thorough knowledge of organisational strategy and planning is imperative, as is a clear grasp of the organisation's information-related assets critical for it to exist and prosper – commonly referred to as the 'crown jewels' (INSA 2014*b*). It is these assets that CCI protects from adversarial intelligence activities and it is the organisational strategy that CCI should advance through the exploitation of adversaries in the cyber sphere.

Strategic CCI differs from that in the operational and tactical level in that it takes a wider view of the macro-environment and a longer term view on the actual or potential emergence of threats (Bodmer et al 2012, Mattern et al 2014). Strategic CCI would for instance identify intelligence principals/sponsors who have plausible motive, intent and capacity to target the own organisation through cyber means. (See Table 2 – "Adversarial Progression") These principals or sponsors will not necessarily execute the actual intelligence activities but are they are the ultimate benefactors (such as a nation state). The actual implementers of hostile cyber as well as associated tactics are those that carry out the task of operational and tactical CCI. While the implementers will determine the operational and tactical avenue of approach, the strategic decisions (e.g. to pursue objectives via human and/or technical means) in this regard will be taken by the Intelligence principal. The pathway of adversarial progression guiding CCI therefore differs from that of CTI (compare Figure 1).

Strategic CCI is furthermore tasked with detecting high-level indicators that the organisation is being targeted or has been compromised. Similarly, strategic CCI should identify drivers and trends suggesting a rise in the risk of internal compromise (insider threat). Equally important is the detection that organisational strategy and decision-making are being unduly influenced by deceptive, adversarial cyber operations. Strategic CCI will advise on countermeasures to best exploit adversarial cyber activities. To be successful cyber counter-deception and exploitation have to be fully synchronised with such actions in other CI fields (such as agent and double agent operations). Therefore, it is imperative for CCI to ensure that countermeasures are aligned with CI and organisational strategy. The design and filling of honeypots on the operational and tactical levels, for example, will ultimately be informed by strategic CCI's direction on counter-deception (cf Bodmer et al 2012).

3.2 Cyber Counterintelligence on the operational level

As on the strategic level, CCI on the operational level strictly pursues the CCI's central mission of defensively and offensively advancing CI-relevant interests in the cyber sphere. Adherence to the mission at all three levels CCI ensures a coherent approach and an optimised CCI effort.

Operational CCI is driven by senior and middle management as well as specialists in the field of CCI operations and analysis. It functions as conduit and advisory to C-Level leadership in matters such as CCI strategic objectives, financials, financial projections and other resource requirements, projects, statistics and reporting.

Operational leadership is responsible, among other, for the following main functions (INSA 2014*a*, Mattern et al 2014): (i) operationalise the CCI strategy as set jointly by the executive management, operational management and CCI experts, (ii) develop and implement CCI structures and acquire resources, (iii) develop and implement operational plans and identify focus areas and (iv)drive daily operations and performance.

Operational CCI is responsible for safeguarding the people, processes, procedures and systems in which the organisation's critical cyber-related assets reside. Consequently, it includes a wide spectrum of organisational functions such as personal security, physical security, procurement, supply chain management, ICT-user management and much more. In addition to conducting CCI operations against adversaries (discussed below), it safeguards the organisation's own information and cyber intelligence operations. It provides operational cyber counterintelligence reports on operations, cyber threats and threat actors, damage and vulnerabilities (as identified through assessments), alerts, warnings and trends to the strategic CCI, line-functional managers, analysts and CCI specialist (Riley 2015). It also self-analyses the reports' output with a view to driving reports' outcomes to action (INSA 2013, 2014*a*).

Operational CCI interfaces with the larger CI function through multi-disciplinary programmes and operations, specifically focussing on the cyber part of CI. Its main concern is whom the adversaries are, their location, capabilities (such as the ability to utilise or develop malware), intentions (either pronounced or unpronounced) and modus operandi (Chismon & Ruks 2015). Together with this, it is concerned with the adversaries' intelligence structures and their intelligence campaigns (either planned or existing).

With regard to a traditional defensive approach, CCI similarly has a dual proactive-reactive focus to identify indicators of cyber targeting and compromise. Such indicators include a disruption in the organisational operations, tell-tale declines in organisational functionalities and/or information leakage. From a reactive perspective, CCI seeks to counter such instances by identifying its origin and addressing the compromise (through either defensive or offensive means). From a proactive approach, it identifies such possible capabilities and campaigns and addresses threats (by either defensive or offensive means)(Bardin 2011).

Operational CCI is persistently seeking exploitable opportunities presented by adversarial cyber campaigns, operations and actions. Through counter-operations these opportunities are pursued either pro-actively or re-actively – depending on the circumstances.

The skillsets required to capacitate operational CCI are multi-disciplinary and include elements such as general management, advanced operational management, CCI analysis, cyber security, cyber defence and offensive CCI techniques and other fields of technical expertise (Bodmer et al 2012).

3.3 Cyber counterintelligence on the tactical and technical levels

The aim of tactical and technical CCI is to achieve the organisations CCI mission though tactical and technical means. It is driven and executed by line-functional leadership as well as team leaders, role leaders, CCI technical and tactical experts, security analysts and other technical personnel. It has an advisory responsibility to both the operational and executive management that includes matters such as CCI threats and opportunities, defensive and offensive measures, systems and toolsets, CCI analyses and financials (Riley 2015; INSA 2013, 2015). This advisory responsibility is usually fulfilled through submitting tactical products to the operational and in some instances directly to the strategic CCI level. Prior to submission to the executive, tactical CCI inputs are normally contextualised at the operational and strategic levels.

Tactical CCI is responsible, among others, for the following main functions (cf INSA 2015): (i) concretise operational direction into action; (ii) identify, design and implement systems, toolsets and reporting mechanisms (both defensive and offensive), (iii) carry out tactical taskings through combined technical and HUMINT measures and (iv) identify, analyse and action CCI threats and opportunities.

Tactical CCI performs the daily management, configuration (including identification and/or compromise in the case of offensive measure implementation) of both defensive and offensive systems, networks, devices, network operations and security operations (INSA 2015). It is responsible for ensuring the C-I-A of the organisation's cyber and information security environment, as a defensive tactic and measure. In the case of an offensive or exploit tactic (that must be congruent with operational objectives and the organisational strategy) tactical CCI further strives to degrade the C-I-A of an adversary's cyber and information security. Tactical CCI interfaces with the larger CI function through multi-disciplinary projects and continuous line-functional interaction. Tactical and operational CCI has a shared focus on on-the-network threats and/or opportunities, threat actors' capabilities or possible capabilities as well as the deployment of and expansion of capabilities. Tactical CCI is concerned with engaging individual groups or individuals, their specific network actions, TTPs and specific technical issues such as malware signatures (Chismon & Ruks 2015).

Tactical and technical CCI processes feed into information reports and focus on specific issues such as breaches, the identification and/or creation of malicious code, intrusion, threat and exploitation. The process leads to the compilation of tactical and technical reports, alerts, warnings, defensive and offensive solution and action reports, campaign proposals, etc. These are provided to CCI analysts, tactical leadership, operational leadership and the executive in the manner described above (Friedman & Bouchard 2015).

The skillsets required for tactical and technical CCI are, as is the case with strategic and operational CCI, multi-disciplinary. They include elements of tactical and line-functional management, ICT security, development of systems and software, programming, scripting, developing offensive and defensive toolsets, CCI technical specialisation, HUMINT and intelligence collection, as well as language and social science expertise (used in for example penetration of hacking forums), ethical hacking, technical defensive and offensive measures as well as reverse engineering (Bodmer et al 2012).

4. Conclusion

This paper emphasised the centrality of CCI to engage morphing high-end cyber threats effectively. Although only well-resourced entities can afford a fully-fledged capacity in this field, a CCI mindset and approach could benefit smaller organisations. Within the context of CCI's infancy as an academic discipline, the paper sets out to contribute two further conceptual building blocks, namely a CCI–CTI differentiation and a multi-layered framework. Constructs such as these are important since they condition our approach to the practice. Since considerable further research is required, both constructs presented are qualified as tentative soundboards intended to stimulate future debate.

There is no consensus on definitions of CCI and CTI and this paper's differentiation is inevitably contestable. It nonetheless offers a start. The framework explicated activities on different organisational levels. As it stands, it provides more clarity on what CCI is and what it is supposed to do. With further research this framework can be developed to a scalable template for the practical execution of CCI on all organisational levels.

Acknowledgment

The research presented in this paper forms part of a project at the Centre for Cyber Security (Academy for Computer Science and Software Engineering, University of Johannesburg) aimed at formalising CCI as a multi-disciplinary field of academic inquiry in the South African context. Those interested are invited to contact the authors and/or view more detail at http://adam.uj.ac.za/csi/CyberCounterintelligence.html.

References

Bardin, J. (2011) "Ten commandments of cyber counterintelligence", *CSO* [online], http://www.csoonline.com/article/2136458/

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

Chismon, D. and Ruks, M. (2015), *Threat Intelligence: Collecting, Analysing, Evaluating*, MWR Infosecurity, UK Cert, United Kingdom.

CrowdStrike (2016) *Global Threat Report 2015* [online] www.crowdstrike.com/global-threat-report-2015/

Deloitte (2014) "Cyber threat Intelligence: Moving to an Intelligence-driven cybersecurity model." *Insight* , CIO edition, [online] http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-threat-intelligence-cybersecurity-29102014.pdf

Duvenage, P. C. and von Solms. S.H. (2015) "Cyber Counterintelligence: Back to the Future", *Journal of Information Warfare*, Vol. 13, Nr 1.

Duvenage, P.C, von Solms, S.H. and Corregedor, M (2015) "The Cyber Counterintelligence Process - a conceptual overview and theoretical proposition", Paper read at the 14th ECCWS, Hatfield, United Kingdom, July.

Duvenage, P. C. and von Solms. S.H. (2013) "The Case for Cyber Counterintelligence", Paper read at the 5TH Workshop on ICT Uses In Warfare and the Safeguarding of Peace, Pretoria, South Africa, November.

EMC^2 (2014) *Intelligence Driven Threat Detection and Response (White paper)*, [online], https://www.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf

Friedman, J. and Bouchard,M. (2015) Definitive Guide to Cyber Threat Intelligence, [online], https://cryptome.org/2015/09/cti-guide.pdf

Godson, R. (2001) *Dirty tricks or trump cards - U.S. covert action and counterintelligence*. Transaction Publishers, New Brunswick.

Google (2016), Search "threat+intelligence", (2016-02-16)

Info-security Magazine (2015) "Global threat intelligence services spending is projected to rise", [online], **http://www.infosecurity-magazine.com/news/cybersecurity-spending-to-hit/**

INSA -Intelligence and National Security Alliance (2015*a)*, *Tactical Cyber Intelligence*, online, http://www.insaonline.org/i/d/a/b/TacticalCyber.aspx

INSA(2014 *a)*, *Operational Cyber Intelligence,* [online] www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx

INSA (2014 *b) Strategic Cyber Intelligence*, [online] www.insaonline.org/i/d/a/b/StrategicCyberWP.aspx

INSA (2013) *Operational Levels of Cyber Intelligence*, [online], 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*, [online] www.oss-institute.org/storage/.../insa_cyber_intelligence_2011.pdf

iSightpartners (2014) *What is Cyber Threat Intelligence and why do I need it?* [online], http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief 1.pdf

Kaspersky (2015) *Global IT Security Risks Survey 2015: The current state of play* [online] http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf

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

Lee, R. M. (2014a) "Cyber Threat Intelligence". *Tripwire* ,blog series, part 5. Retrieved on 04 January 2015 from http://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence/

Lee, R. M. (2014b), "Cyber Counterintelligence: From Theory to Practice". *Tripwire*, blog series, part 4. Retrieved on 04 January 2015 from http://www.tripwire.com/state-of-security/.../cyber-counterintelligence-from-theory-to-practice/

Mattern, T. et al (2014) "Operational Levels of Cyber Intelligence"*, International Journal of Intelligence and Counterintelligence*, vol. 27, no. 4.

McAfee Labs (2015) 2016 Threats Predictions http://www.mcafee.com/us/resources/reports/....predictions-2016.pdf

Moyo, A. (2015) "Syndicates wreak havoc in cyber space", *ITWeb*, [online] http://www.itweb.co.za/index.php?option =com_content&view=article&id=143480:Syndicates-wreak-havoc-in-cyber-space&catid=234

PwC (2016) *Global Economic Crime Survey 2016: The UK*, [online], http://www.pwc.co.uk/gecs

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

Riley, S. (2015) Insights *to Modern Threat Intelligence*, online, https://www.linkedin.com/pulse/insights-modern-cyber-threat-intelligence-shawn-riley?articleId=7011683228767036224

Schoeman, A. (2015)"Demystifying Threat Intelligence", *Infosecurity Magazine*, [online], http://www.infosecurity-magazine.com/opinions/demystifying-threat-intelligence/

SpearTip (2015) Cyber *Hunt Team Operations and Counterintelligence*, [online] http://www.iopw.com/Article/9461/Business--Professional-Services/Cyber-Hunt-Team-Operations-and-Counterintelligence?gPage=60

Statista (2016) *Threat Intelligence Services Worldwide*, [online], www.statista.com/statistics/417588/threat-intelligence-spending/...../

The Economist (2015) "*Counter-intelligence techniques may help firms protect themselves against cyber-attacks", [online],* http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protectthemselves

VeriSign (2012) *Establishing a Formal Cyber Intelligence Capability,* (White Paper), [online], https://www.verisigninc.com/assets/whitepaper-idefense-cyber-intel.pdf.

Duvenage, P.C., Jaquire, V.J. & von Solms, S.H. (2016) 'Conceptualising cyber counterintelligence – Two tentative building blocks' in *Published Proceedings of the 15th European Conference on Cyber Warfare and Security*, Munich, Germany, June, pp 93-103