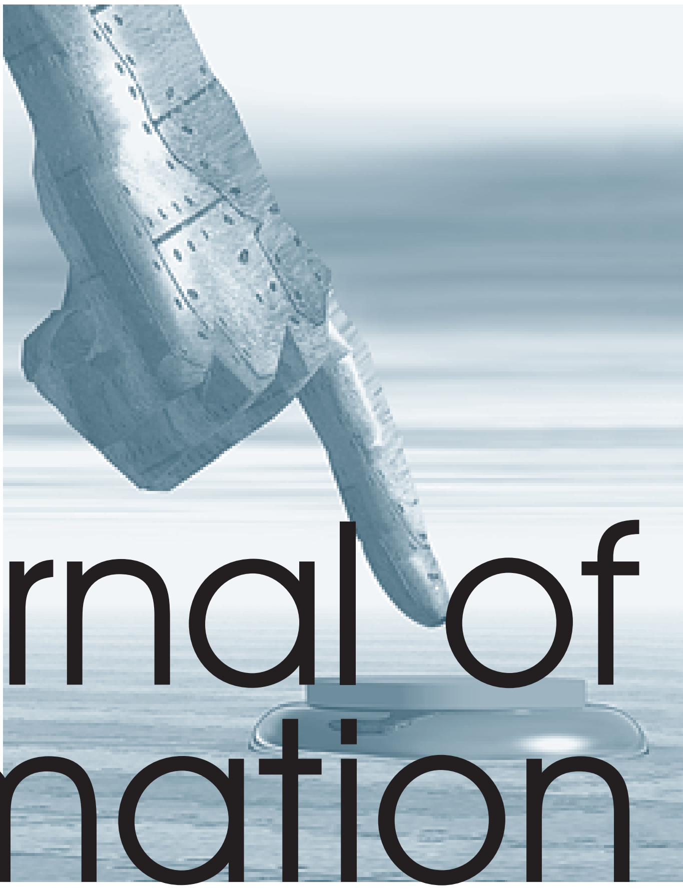
Volume 13, Issue 4, January 2015

ISSN 1445-3312 (Printed Journal)

ISSN 1445-3347 (On Line Journal)



Journal of Information Warfare

These attacks can range from
service to the deliberate
Disrupt or destroy data: this is similar to the
above, but disruption can be caused to the
system collecting and storing the data or
that part of the system, which disseminates
Destruction of the data can occur by physical
destruction of the storage medium, or
data itself, so it becomes irrecoverable
needed to make it useful

Journal of Information Warfare

Volume 13, Issue 4

Contents

Cyber Counterintelligence: Back to the Future

PC Duvenage, SH von Solms

Centre for Cyber Security
Academy of Computer Science and Software Engineering
University of Johannesburg, South Africa
E-mail: duvenage@live.co.za;basievs@uj.ac.za

Abstract: *It is generally accepted that conventional cyber security generally has failed. As such, Cyber Counterintelligence (CCI) is fast gaining traction as a practicable approach to secure and advance our own interests effectively. To be successful, CCI should be an integral part of multi-disciplinary Counterintelligence (CI)–conceptually and in practice. With a view to informing sound CCI practice, this paper conceptualises CCI as a part of CI. It proceeds with going back to some time-tested CI constructs and applies these to the cyber realm. In so doing, this paper aims to offer a few building blocks toward a future of sound CCI theory and practice.*

Keywords: *Counterintelligence, Cyber Security, Cyber Counterintelligence*

Introduction

What was seen as a paradigmatic shift in thinking at the turn of this decade is now commonly accepted–that conventional cyber security which we have been relying on is deteriorating on all fronts (Lües 2012). As a result, cyber space is now probably more insecure than it has ever been (Bodmer *et al*. 2012). It is also likely to be the most secure than it is going to be for the foreseeable future. It is, simply put, going to get much worse. In this regard, the World Economic Forum's (WEF) 2014 Global Risk Report warned of "digital disintegration" when it stated: "The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce" (WEF 2014). The report continues by identifying the foremost "technological risks" for the immediate future as the breakdown of critical informational infrastructure and networks, an escalation of large scale cyber-attacks, and incidents of data fraud continue on an unprecedented scale (WEF 2014). Even early on in 2014, these were no longer risks but manifesting trends. Attesting to this concern is the continuing prominence in mass-media media reporting on the escalating detrimental impact of cyber criminals, hacktivists, and other role-players. Simultaneously, nation states' cyber surveillance by the intelligence apparatuses of not only the United States (US) and United Kingdom (UK), but also the People's Republic of China (PRC) and Russia continue to make headlines.

With the awareness of conventional cyber security's faltering, both state and non-state actors have been intensifying their quests for ways to more effectively protect and advance their cyber interests and, in the case of service providers and vendors, those of their clients. As could be expected, solutions offered in the marketplace vary considerably. Buzzwords and marketing slogans currently gaining favour include: counter exploitation, threat intelligence, offensive measures, hacking back, threatscape, and intelligence software analytics (IBM 2013; Helton 2013). Common to most of these solutions advocated is recognition of the imperative of intelligence on threat actors and the need to engage threats pro-actively/offensively. There is a sense of taking the fight to adversaries. The use of such notions and phrases would have been encouraging if it was indicative of more organisations "moving towards intelligence-driven risk management and decision-making models" (Helton 2013). As it currently stands, however, the use of these terms is disturbing for three interrelated reasons. First, the terms are used vaguely and without the proper context from the statutory intelligence practice from which they are often derived. In marketing jargon 'intelligence' is used interchangeably with 'data and information'. Consequently, solutions offered under the rubrics of 'intelligence' may not solve the problems for which they purport to be the fix. In a similar vein, opting for quick-fix offensive actions, not dovetailed with an appropriately configured defensive posture, is inviting disaster. Equally disconcerting is the fact that solutions and terms are sometimes thrown around without due and categorical stipulations that some aspects of cyber defence and offense are the exclusive prerogative of the state apparatus in most countries. These functions ought not to be 'out-sourced' to other entities. Secondly, solutions being offered are essentially technical and tactical in nature. As important as they are, technical and tactical measures on their own are insufficient to confront the sophisticated threat actors about whom we are most concerned. Social engineering, to cite one example, "played a part in nearly every major hack or breach in 2013 yet it still stays in the background when we consider security controls. This is something that needs to change as we move forward" ([ISC]^2 2013). Thirdly, these solutions are presented as neat 'add-ons' or 'plugins' to be used as a layer additional to existing cyber security measures. 'Add-ons' seldom have, and certainly will not in the future offer adequate protection against advanced adversaries. For sizable institutions with significant digital and information interests to face up to such adversaries, cyber security needs to be a coherent part of their DNA and not mere feel-good plasters offering little real protection.

There is a way in which such synergy can be achieved and the tables turned on cyber adversaries. This paper posits cyber counterintelligence (CCI) as a practicable approach to effectively securing and advancing cyber interests. From this perspective, malicious cyber actions are not all bad news. The good news is that we can exploit malicious cyber actions to our advantage and to the detriment of the adversarial instigators. There is, however, a precondition: there can be no half measures. To be effective, CCI needs to be properly conceptualised and implemented. If not, it is likely to be self-defeating and could even end in self-destruction. For a substantial part, this conceptualisation entails the application of time-tested counterintelligence (CI) notions to the cyber sphere. It is a case of going back to counterintelligence fundamentals in order to enable our wellbeing in the cyber sphere today and in the future. It is thus a case, as suggested by the paper's title, of going back in order to successfully move to a more secure cyber future.

This paper's primary aim is to provide a conceptual baseline that could help stimulate the academic discourse on CCI. Consequently, it begins with a cursory overview of the status of CCI in the public and academic discourse on cyber security. An academic self-awareness of CCI's under-theorised status is, after all, a first step in addressing this near void. The paper proceeds with advancing CI and CCI constructs hopefully useful to this discourse. Rather than aiming to advocate radically new concepts, the emphasis is on presenting existing knowledge in a manner conducive to further academic debate. Such conceptual 'building blocks' include a definition and delineation of the CI as a CCI sub-discipline, a taxonomy for CCI methods and means, as well as a CCI matrix for configuring an offensive-defensive posture. It concludes with some views on CCI's future by suggesting areas for further academic enquiry.

As noted above, the following section reflects on CCI under-theorised status, since such awareness is an important first step in make progress with the academic discourse.

Cyber Counterintelligence's under-Theorised Status

In one form or the other, cyber counterintelligence has been practised as part of the statutory counterintelligence functions in various intelligence communities for well over two decades. CCI has also been offered as a service provided by a few niche companies for well over a decade. Until very recently, however, CCI has not really gained traction outside the statutory security structures and the small batch of clients the niche companies served. Despite the key it holds to secure cyber interests for state and non-state actors, CCI entered the second decade of the 21st century underappreciated and underexplored in policies and in the literature in the public domain. The overwhelming majority of governments' cyber security policies do not make any references to counterintelligence. And, in the few instances that the concept is cited, counterintelligence is hardly at the centre.

Anecdotal indications are that CCI has fast been gaining traction during the last two years. The 2013 proceedings of the 12th European on Cyber Warfare and Security (ECCWS), for example, consist of 44 papers and are 406 pages long (Kuusisto & Kurkinen 2013). Not one of these papers makes mention of CCI. There is, in fact, only one sentence in the whole of the proceedings that makes cursory reference to the general concept of counterintelligence (Kuusisto & Kurkinen, 2013). A mere one year later, and ECCWS 2014 featured a dedicated mini-track to Cyber Intelligence/Counterintelligence. While this certainly reflected an increased awareness of CCI, contributions remain scarce. Only one paper presented at ECCWS 2014 had CCI as its focus or had 'counterintelligence' in its title.

While a few commendable books have been published on the subject, these are minuscule in comparison with the proliferating material on cyber security in general. The shift in emphasis towards CCI is nonetheless also apparent here. An outstanding work by Bodmer *et al.* was first published in 2012 with the title *Reverse Deception – Organized Cyber Threat Counter-Exploitation* (Bodmer *et al*. 2012). The edition due for release in 2014 which, as far as could be surmised from pre-launch advertising, retains the core of the 2012 edition–and is more aptly called *Hacking Back: Offensive Cyber Counterintelligence* (Bodmer *et al*. 2014).

Although CCI is poised to gain prominence, the participation in and agenda of this discourse will inevitably be influenced by the relative obscurity of CI in general. CCI will be demonstrated in further sections as a sub-set of the broader, multi-faceted CI discipline. It thus follows that contributions to CCI would need to be preceded by some grounding in CI. CI, however, (and herein lies the glitch), is in itself academically obscure and underappreciated. This obscurity is as old as its inception as a formalised discipline in the run up to World War II. Some would argue that this can be ascribed to the fact that a large part of CI work relies for its effectiveness on secrecy. Yet, we do not need to reveal secrets to talk seriously about matters of Intelligence and Counterintelligence (Meyer 1987). A more likely reason for CI's obscurity in the academic debate is to be found in the fact that it is arguably the most complex and least understood of all Intelligence disciplines (Godson 2001). The following statement by a U.S. CI veteran in the midst of the Cold War has lost none of its relevance: "It is not easy, nor can one feel confident, to re-enter this world where, it has been said, the tortuous logic of counterintelligence prevails...Unfortunately, there seems to be no easy way to explain counterintelligence...Because effective counterintelligence is a combination of so many aspects" (Miller 1980). Even among policy makers, scholars, and 'national security practitioners' in foremost intelligence communities such as those of the U.S., "the role of counterintelligence remains little known or understood" up to this day (Van Cleave 2007).

Since the role, functions, and importance of CI is opaque within statutory intelligence circles, the reluctance of 'techies' to apply this concept to the cyber sphere is understandable. In a similar vein, those skilled and experienced in more conventional counterintelligence do not necessarily have a sound working knowledge of technical cyber. If we are not clear on a conceptual level, we can hardly make progress in the academic discourse, thereby eventually affecting our ability to implement sound solutions. In the conceptual difficulties of CI also lie the opportunity. If we can understand and explain CI, we can explain CCI and then we can unlock the latter's potential as a force multiplier.

This section illustrated the need for contributions to the budding CCI field to be clearly rooted in CI. In line with this contention, the next section provides a conceptual primer of CI.

A Primer on Counterintelligence

Counterintelligence has been practised and described for millennia. Some enduring principles were penned in 500 B.C. by the much-quoted Sun Tzu in a specific chapter in his *The Art of War* devoted to the use of spies and counter-spies (Giles 2002). The term in its contemporary connotations entered the English lexicon in the mid-1930s (Dictionary.com 2014). For some, counterintelligence is all about spies outgunning adversarial spies. For others, it invokes mundane security measures such as computer passwords, restrictions on the use of computing equipment, security guards, access control, and the like. Counterintelligence is all of these things, and so much more (Duvenage & von Solms 2013).

Delineating Counterintelligence

Counterintelligence can be defined as the collective of measures undertaken to identify, deter, exploit, degrade, neutralise, and protect against adversarial intelligence activities deemed as detrimental or potentially detrimental to one's own interests (Duvenage 2010). The term 'counterintelligence' is thus an abbreviated form for the countering of hostile intelligence activities. Adversaries engaging in hostile intelligence actions include nation states, corporate entities, criminals, activists, individuals, and any combination of these.

Adversarial intelligence activities include espionage, deception (disinformation), influencing, and some other forms of covert action that can have disruptive and destructive outcomes. Of these different intelligence activities, espionage is the most central. Espionage to obtain protected information in order to gain a competitive advantage can be an end in itself; or such information can be used to further other malicious ends such as data manipulation, disinformation, and disruption. Sophisticated adversaries execute their intelligence actions through the exploitation of humans (HUMINT) and technical means (TECHINT). The latter, in turn, comprise Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), and Cyber Intelligence (CYBINT). These conduits and their relation to adversarial intelligence ends are graphically depicted in **Figure 1**, below:

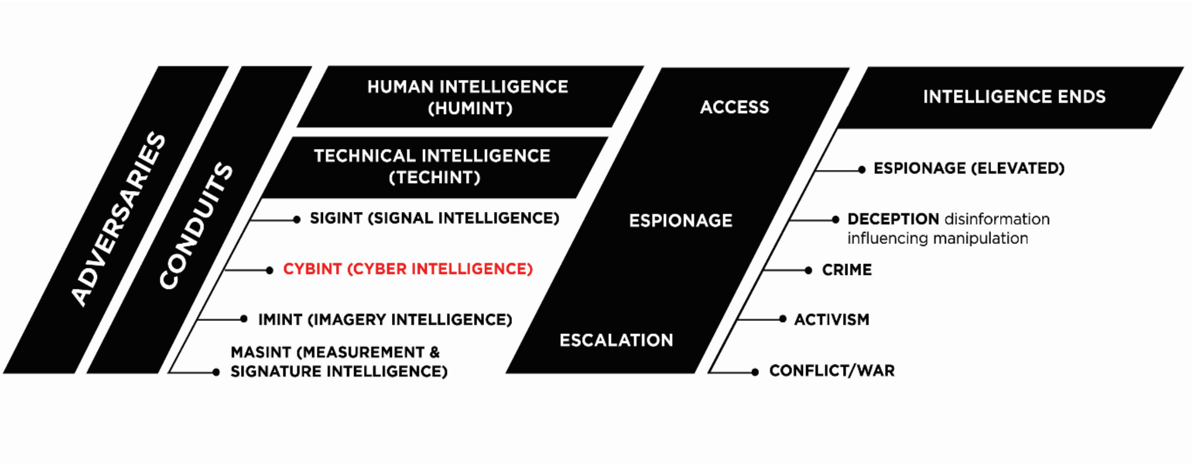

ADVERSARIES
CONDUITS
HUMAN INTELLIGENCE (HUMINT)
TECHNICAL INTELLIGENCE (TECHINT)
SIGINT (SIGNAL INTELLIGENCE)
CYBINT (CYBER INTELLIGENCE)
IMINT (IMAGERY INTELLIGENCE)
MASINT (MEASUREMENT & SIGNATURE INTELLIGENCE)
ACCESS
ESPIONAGE
ESCALATION
INTELLIGENCE ENDS
ESPIONAGE (ELEVATED)
DECEPTION disinformation influencing manipulation
CRIME
ACTIVISM
CONFLICT/WAR

Figure 1: Adversarial Intelligence: Conduits and Ends

Several revelations by the whistle-blower Edward Snowden provide a practical illustration of the above. During September 2013, for example, *The Guardian* newspaper revealed that the British and U.S. Agencies run HUMINT operations to “help secure an insider advantage” (Ball, Borger & Greenwald 2013). To this end the British Government Communications Headquarters (GCHQ) established a HUMINT Operations Team (HOT) "responsible for identifying, recruiting and running covert agents in the global telecommunications industry" (Ball, Borger & Greenwald 2013). These operations enabled the Agency to “tackle some of its most challenging targets", specifically, in as far as the breaking of encryption was concerned (Ball, Borger & Greenwald 2013). In this instance, success in the field of CYBINT thus depended on the effectiveness of HUMINT operations. The reverse is of course also true. Given the high and growing digital dependence, CYBINT is often a critical enabler in the HUMINT sphere. To be effective, CI needs to counter all types of adversarial intelligence activities and, in the case of high-end adversaries, it has to do so in more than one of or in all of the conduits.

Counterintelligence: Measures, Means, and Modes

In order to execute its mission, CI relies on measures and means that vary from passive-defensive to active-offensive ones. At the one end of the spectrum, passive-defensive measures strive to deny adversaries access to protected information assets. They aim to reduce vulnerabilities through a combination of policies, procedures, and practices–sometimes referred to on a lighter note as “gates, guards, guns, and dogs” (Francq 2001). Apart from denying opponents access, properly instituted passive-defences measures are like caste walls. In addition to preventing common intrusions, their presence discourages intrusion attempts and consequently serves a deterrence function. Examples of passive-defensive measures are access and movement control, perimeter security, alarm systems, safes and vaults, fire prevention measures, key control, and the control of the removal and transfer of information from facilities where valued information is located. At the other ends of the spectrum, offensive counterintelligence aims to neutralise a competitor’s intelligence efforts through measures ranging from deception and manipulation to the neutralisation of adversarial intelligence activities and systems. Deception takes various forms and can be achieved through numerous means. Skilfully executed, deception attains a primary counterintelligence aim, which is the manipulation and control of an adversary. This is aptly encapsulated by Codevilla (1992) when he states “Action against the enemy through the enemy’s own intelligence is the very consummation of CI”. There are of course also aggressive CI measures that CI shares with its sister-discipline, Covert Action. Under certain conditions, assassinations and even extraordinary rendition can be classified as active-offensive CI neutralisation measures (Duvenage 2010).

Between passive-defensive and active-offensive lie a wide array of other measures, such as: pre-employment personnel security; in-service personnel security; technical surveillance countermeasures (TSCM); encryption; surveillance (physical, static, mobile, and electronic); double agents; agents; and continued monitoring. In most instances, these measures can serve defensive or/and offensive purposes. Defensive counterintelligence tactics and strategies provide information and act as triggers to alert the offensive side of the practice. Similarly, offensive operations (for example a source reporting on an adversary's intentions and capabilities) inform the proactive configuration of defences. It will also be noted that several of these are highly useful in the collection of information of internal vulnerabilities (such as organisational weaknesses and insider threats), the external environment, as well as actual and potential adversaries. It goes without saying that, without such information being analysed, CI would be blind and unable to execute the defensive-offensive interplay. The following matrix, depicted in **Figure 2**, below, is somewhat of an over-simplification, but is nonetheless useful in conveying the nuanced nature of the offensive-defensive interplay as well as the importance of collection:

Defensive Mode **Denies adversaries access to and generates information about adversaries**	
Passive Defence Denies the adversary access to information through physical security measures and security systems.	**Active Defence** The active collection of information on the adversary to determine its sponsor, modus operandi, network, and targets. Methods include physical and electronic surveillance, dangles, double agents, moles, and electronic tapping.
Offensive Mode **Aims to manipulate, degrade, control, and neutralise adversaries**	
Passive Offensive Reveals to the adversary what you want them to see. This could range from selective exposure of actual information to decoys and dummies. The adversary is thus left to draw its own inferences and interpretations.	**Active Offensive** The adversary is fed with disinformation and its interpretation thereof manipulated. Disinformation can be channelled through, for example, double agents and 'moles'. Active-offensive CI could include some forms of covert action. Covert action, in its use here, denotes the targeting of an adversary through the influencing of events, conditions, individuals, groups, or institutions to the benefit of a sponsor in a manner not attributable to the sponsor or by offering plausible deniability. Influencing is achieved through measures that vary from paramilitary and political actions to propaganda and intelligence assistance.

Figure 2: A Four-Sector Counterintelligence Matrix (Compiled by the authors on the basis of narratives in Prunckun 2012; Sims 2009; Odom 2003; Godson 2001)

Counterintelligence Process

The preceding matrix and discussion above demonstrate that CI is an intricate and exhaustive discipline. It is not only about defences, but is also about the concrete advancement of one's own interest vis-à-vis adversaries' interests. It could be surmised from the above that, no matter how well-resourced, the CI endeavour cannot protect all assets or advance all interests all the time. The bodies of information that justify CI protection as well as the systems, processes, institutions, and individuals in which such information resides must be identified and prioritised (Prunckun 2012). Since offensive action carries even higher risks and costs, CI should be crystal clear on it role in this regard. Such clarity in turn presupposes CI to be in synergy with Intelligence and at the centre of a government's or business' strategy. These are the critical roots of the CI premise.

While few would dispute CI's premise, opinions are divided on the structuring of the CI process. This paper favours a process model that differs fundamentally from the traditional (positive) intelligence cycle and Clarke's target-centric process (Clarke 2004). This process model comprises the following steps (Duvenage & Hough 2011; Duvenage 2013):

1. Identify information and assets that warrant the expending of counterintelligence resources.
2. Assess vulnerabilities that increase the risk of information being compromised.
3. Scan the environment and identify actual or potential threat-agents.
4. Collect information on threat-agents and appraise the risks.
5. Re-assess own vulnerabilities and review defences.
6. Develop sets of counterintelligence measures and projects (offensive and defensive).
7. Implement the recommended countermeasures and projects.
8. Continually assess and adapt the implemented countermeasures to compute the changing environment.

The apparent simplicity of this model in certain respects masks some intricacies of the counterintelligence process. In the case of offensive counterintelligence, for example, espionage adversaries will be engaged through a pattern of activities interwoven within the broader counterintelligence processes. Offensive counterintelligence, in other words, will be performed as a sub-process of step 6 outlined above. This sub-process draws an important distinction between an 'espionage adversary' and an 'espionage target'. An 'espionage adversary' is the ultimate sponsor of an intelligence effort, while the counterespionage target is the instrument with which intelligence activities are conducted. This instrument is targeted by an opposing entity's counterespionage structure–hence the phrasing 'counterespionage target'. A nation state and its intelligence service would, for example, be espionage adversaries and the proxies for conducting the actual espionage would be the counterespionage targets. Such proxies could be recruited agents or third entities (for example, front companies). Employing this distinction, the offensive counterespionage process–which is executed per step 6 of the process model above–will typically have the following sub-steps (Duvenage & Hough 2011):

6.1 Identification of espionage adversaries.
6.2 Prioritisation of espionage adversaries.
6.3 Investigation of espionage adversaries.
6.4 Engagement of counterespionage targets.
6.5 Exploitation of counterespionage targets.
6.6 Neutralisation of targets and termination of operation

This section provided a primer that demarcated CI, explained CI measures and modes, and offered changes to the CI process. Building on this overview of CI, the paper proceeds with conceptualising CCI.

Conceptualising Cyber Counterintelligence

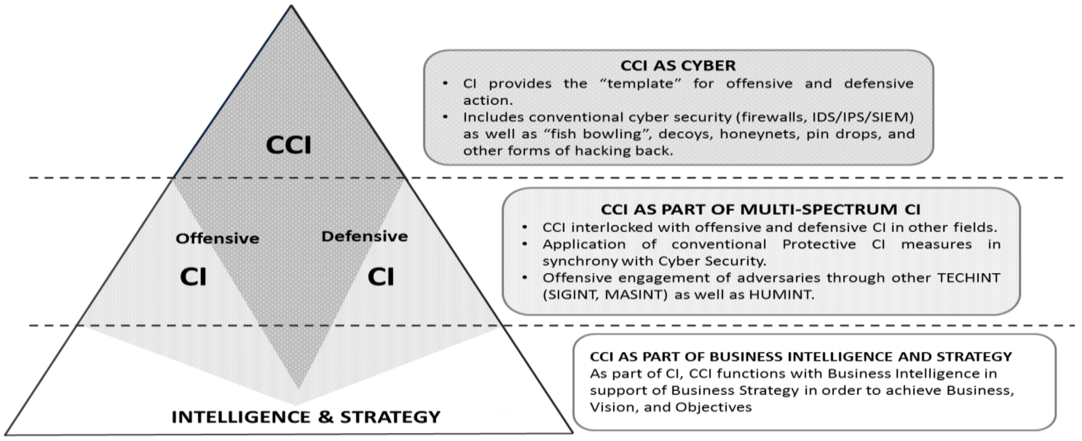
This section provides a provisional definition of CCI, advances a model for integrating CCI with CI and Intelligence, and outlines some CCI methods, means, and modes.

Defining and Delineating Cyber Counterintelligence

While various definitions for CCI have been advanced, none of these specifically explicate the relationship between CCI and CI (for example, Carrol 2009; Bodmer *et al*. 2012; Farchi 2012). In keeping with the paper's central contention, CCI is defined as that subset of multi-disciplinary CI aimed at deterring, preventing, degrading, exploiting, and neutralising adversarial attempts to collect, alter or in any other way to breach the Confidentiality, Integrity and Availability (CIA) of valued information assets through cyber means. Expanding on this definition, it is postulated that CI delineates CCI on the following three tiers (Duvenage & von Solms 2013):

- Applied to the cyber context, CI theory and practice provides a conceptual template for modelling CCI actions in the safeguarding and advancing of cyber interests. Mirroring CI, CCI has offensive and defensive missions that are distinguishable but not separable.
- To be effective, cyber counterintelligence needs to be interlocked with all-field counterintelligence–defensively and offensively. In this sense, CI cements an integrated approach to securing the cyber space. CCI is thus about both the modelling of cyber actions on CI and the integration of these offensive and defensive actions with conventional CI.
- Effective CI protects and promotes the intelligence endeavour and business strategy. Since CCI is part of CI, it is also integrated in business strategy and intelligence.

Figure 3 depicts this three-tiered relationship graphically.



CCI AS CYBER

- CI provides the "template" for offensive and defensive action.
- Includes conventional cyber security (firewalls, IDS/IPS/SIEM) as well as "fish bowling", decoys, honeynets, pin drops, and other forms of hacking back.

CCI AS PART OF MULTI-SPECTRUM CI

- CCI interlocked with offensive and defensive CI in other fields.
- Application of conventional Protective CI measures in synchrony with Cyber Security.
- Offensive engagement of adversaries through other TECHINT (SIGINT, MASINT) as well as HUMINT.

CCI AS PART OF BUSINESS INTELLIGENCE AND STRATEGY
As part of CI, CCI functions with Business Intelligence in support of Business Strategy in order to achieve Business, Vision, and Objectives

Figure 3: The Cyber Counterintelligence Pyramid

The postulation, per the narrative and **Figure 3**, above, is admittedly cursory and does not purport to conform to the criteria of a conceptual model. However, it could provide a useful premise for further research and for the development of a conceptual model for implementation in the cyber domain.

Overview of Cyber Counterintelligence Methods, Means, and Modes

The section above discussed defensive and offensive CCI actions. Mirroring CI in general, CCI methods and means can be deployed in offensive and defensive modes, but defy categorisation in watertight compartments. At the very ends of this spectrum there are a few methods and means that could be designated clearly as active-offensive (notably cyber weapons with a destructive purpose, such as Stuxnet) or passive-defensive (for example, access control and validation directives). In the main, however, offense-defensive and active-passive are not neat compartments, but rather the manner in and end towards which methods and means are deployed (Duvenage & von Solms 2013). This is illustrated in the following matrix, **Figure 4**, below, which depicts the four cyber-counterintelligence modes (postures) an entity could assume:

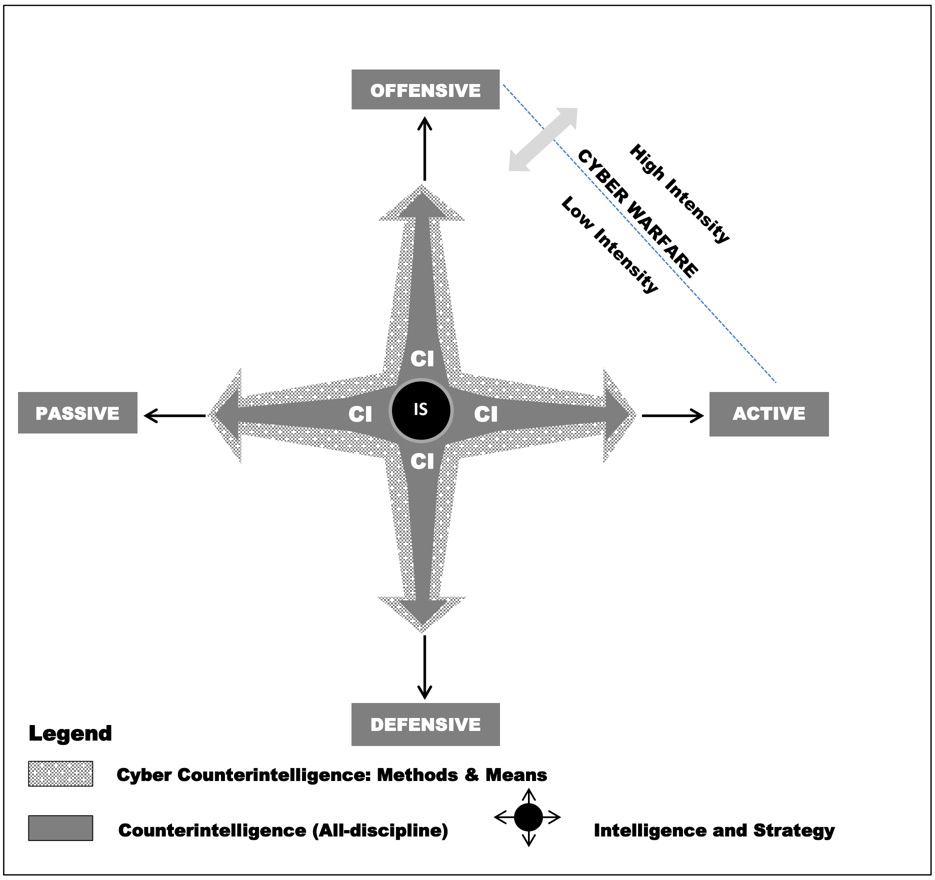

OFFENSIVE
High Intensity
CYBER WARFARE
Low Intensity
PASSIVE
CI
CI
IS
CI
CI
ACTIVE
DEFENSIVE
Legend
Cyber Counterintelligence: Methods & Means
Counterintelligence (All-discipline)
Intelligence and Strategy

Figure 4: Cyber Counterintelligence Matrix

The CCI matrix per **Figure 4** is more than a notional construct and can be applied practically by entities (with sizable cyber interest and assets) in the plotting of CCI methods and means. The matrix ensures that a presence is maintained or, at the very least, that contingency planning is done with respect to all four quadrants. It furthermore facilitates innovation and creativity in the application of methods and means–within legal parameters, of course. Contrary to a misconception, for example, an Intrusion Prevention System can be configured with surprising positive results in executing aims in the other three quadrants. Consequently, the construction of a tabulated taxonomy of CCI methods and means could very well be an oversimplification. Even more so should the taxonomy endeavour to point to parallels that exist between CCI measures and those in CI generally. Nonetheless, at this early stage of conceptualising CCI, such a simplification can serve as a jumping off point for further debate. With this caveat, a cursory taxonomy of CCI methods and means is provided in **Table 1**, below:

Table 1: Taxonomy of Cyber Counterintelligence Methods and Means (Duvenage & von Solms 2013)

<table>
<tr><th colspan="4">DEFENSIVE MODE</th></tr>
<tr><td colspan="4"><b><i>Passive</i></b> → <b><i>Active</i></b></td></tr>
<tr><td colspan="4"><b><i>Deny</i></b> &gt;&gt; <b><i>Detect</i></b> &gt;&gt; <b><i>Collect</i></b></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.
• <i>In loco</i> theft of data, hardware.
• Introduction of malware through physical access to systems.
• Physical destruction.
• Unauthorised reading (acoustic, visual, 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.

<u>Remark</u>: Within the area of Physical Security, there is an extensive and strong convergence between CCI and conventional CI. In keep with the article’s central contention that CCI ought be seamlessly integrated with CI, the sub-category ‘Physical Defensive’ is included in this taxonomy. Note is taken of the fact that with other classification criteria some of the measures listed above may be excluded from CCI, per se.</td>
<td>Consists of aspects such as
• IT and user personnel <b>vetting</b>, re-vetting, and confidentiality agreements.
• Personnel security measures, <b>BYOD</b> user parameters, or exclusions.
• <b>User programmes</b> in cyber security which cover policy and procedures for the handling of security incidents and malfunctions.
• Overlapping with system defences, the use of <b>software decoys</b> to mitigate the insider threat.
• <b>Investigations</b> focused 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, 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 and honeynets.
✓ Overlapping with the latter, are <b>IDS</b> and <b>IPS.</b> Depending on its configuration, a honeynet can be defensive or offensive in type/mode. The term fish bowling denotes the defensive configuration. (Remark: See http://ids.cs.columbia.edu/content/ publications.html for extensive work that has been done on IDS/IPS).
• Processes (such as supply-chain management, product verification, and <b>testing</b>) are also, in part, system defences.
• <b>Vulnerability assessments</b> and <b>penetration testing</b>.
• Incident <b>investigation</b> and response. A <b>CERT</b> is, by definition, defensive–although it might contain offensive elements in its responsive action.
• <b>BYOD</b> regulation in as far as network interfacing is concerned (also part of Personnel Defenses).</td>
</tr>
<tr><td rowspan="2"></td><td colspan="3">• The use of <b>honeynets and software decoys to mitigate the insider threat</b> creates an overlap between personnel and system defensive measures. They are mostly active CCI means.</td></tr>
<tr><td colspan="2">• <b>Investigations</b> focused on <b>internal</b> cyber security incidents involving personnel. May include digital forensic investigations.</td><td>• <b>Investigations of external cyber intrusions</b> could be part passive and part active system defence.</td></tr>
<tr><th colspan="4">OFFENSIVE MODE</th></tr>
<tr><td colspan="4"><b><i>Passive</i></b> → <b><i>Active</i></b></td></tr>
<tr><td colspan="4"><b><i>Collect</i></b> &gt;&gt; <b><i>Disrupt</i></b> &gt;&gt; <b><i>Exploit</i></b> &gt;&gt; <b><i>Destroy</i></b></td></tr>
</table>

- **Collection** of information on and the monitoring 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., which 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) and data mining. - The recruitment and handling of **virtual agents** on underground forums (under true or false flag) that can serve the purpose of collection and/or exploitation. (Under certain circumstances virtual agents can also develop into HUMINT assets).	Measures taken to **exploit** and to **neutralise** adversaries' activities in the cyber sphere: - **System and honeynet** can be **configured offensively** with the aim of 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.	**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 should allow utilisation without, or in conjunction with, kinetic war. Nevertheless, a top class civilian CCI outfit will need to have the authority and the capacity to very selectively conduct operations that have cyber warfare characteristics. Such cyber CCI operations will share characteristics with covert action. (Covert action aims to influence role-players, conditions, and events without revealing the sponsor's identity.) Within business, the use of offensive measures will be determined by the legal and regulatory framework within which the entity operates.
- **Cyberespionage** on adversaries. Distinguishable from own-system collection (IPS, IDS, honeynets) on the basis that adversarial networks are actively targeted and exploited in accordance with strategic and operational objectives.		

Table 1 samples only some of the possible CCI methods and means. Moreover, and given the length constraints of an article, only a very few of these are further elaborated upon, namely honeypots and decoys, cyber profiling, and cyber-agent operations.

In the means cited above, honeynets feature prominently in the active and passive as well as the defensive and offensive modes. Honeynets have been in use for more than two decades with the principle objective to detect, to monitor, and to gain intelligence on adversarial intrusion on a network (Bodmer *et al*. 2012). In recent years, the purposes of honeynets broadened from their original mostly defensive use to include also a much more active and/or offensive role. Concurrently, the different types of honeypots and configurations are sharply increasing. In as far as architecture goes, and depending on specific needs and situations, honeynets can be centralised, distributed, federated, and confederated (Bodmer *et al.* 2012). The diversifying aims of honeynets now include one or a combination of deception, disinformation, and the draining of adversarial resources through labyrinths and "rabbit holes" (Nakashima 2013; Duvenage & von Solms 2013). In a similar vein, decoys are highly useful in disrupting external intrusion and/or mitigating the insider threat (Voris *et al*. 2013). The more resourced and sophisticated the adversary, the greater the imperative to attune the staging of honeynets and the content filling of honeypots, honeyfiles, and honeytokens in accordance with the opposition's interests and modus operandi (Duvenage & von Solms 2013).

Counter-action with matching sophistication, in turn, requires sound analysis of high-grade information on the environment and on adversaries. Unsurprisingly, cyber profiling, which involves the application of criminal and intelligence profiling methods to the cyber realm, is fast gaining field as a CCI specialisation area (Bodmer *et al*. 2012). In order to procure information on actual and potential adversaries, as well as to keep tabs on hacking communities of all sorts, CCI outfits maintain a layered presence on nets and forums. This presence varies from the deployment of soft and hardware instrumentalities to the cyber equivalent of HUMINT counterespionage, namely the recruiting, turning, and handling of witting/unwitting agents (Duvenage & von Solms 2013).

Cyber Counterintelligence as a Multi-Disciplinary Subset of Counterintelligence

In line with the theoretical outline of the relationship between CCI and CCI (**Figure 3** and **Figure 4**), the practical safeguarding and advancement of cyber interests is a multi-disciplinary endeavour. CCI is thus not only multidisciplinary in itself but is overlaid upon multi-disciplinary counterintelligence. This multi-disciplinary mind set is especially relevant in the face of sophisticated threats. As part of the Edward Snowden revelations, it was reported, for example, that the USA and UK Intelligence communities rely on the recruitment and running of HUMINT sources networks in the global telecommunications industry to "tackle" some of their "most challenging targets"--*inter alia* in the cryptology field (Ball, Borger & Greenwald 2013). In keeping with such multi-dimensional threats, a CI operation in the cyber field could entail a multi-disciplinary team comprised of cyber security specialists, strategic analysts, tactical and technical analysts, HUMINT specialists (such as agent handlers and intelligence psychologists), cyber defense technical experts, language experts, ethical hackers, sociologists, and religious experts (Bardin 2011). While a sharp edge on the offense, humans are also the weakest and possibly the most ruinous chink in the defensive armour. Powell, Wick & Fergus (2013) assert "an organization's insiders" are "primary threats to cybersecurity … [which are] ….the most difficult to mitigate". Complementary to technical defences, CI personnel fidelity measures and HUMINT counterespionage practices are thus critical. This is being highlighted by unfolding detail around the Edward Snowdon breach.

The convergence of cyber and HUMINT counterintelligence was furthermore demonstrated by a recent re-evaluation of the Aurora attacks. This re-evaluation suggests the Aurora attacks were not, as was initially thought, a People's Republic of China (PRC) operation which targeted human rights activists. It was in fact a Chinese counterintelligence operation to determine whether PRC intelligence operations and agents had been compromised by USA intelligence (Corbin 2013). Duvenage & von Solms (2013) cite as a further example of "an integrated CI initiative, a disinformation campaign as part of which the staging and content filling of a honeynet is harmonised with disinformation fed to an adversary through a HUMINT asset (e.g. double agent)".

Cyber Counterintelligence and Counterintelligence–An Integral Part of Intelligence and Strategy

To re-state the paper's recurring theme, CCI forms part of and is guided by the integrated CI endeavour. Consequently, CCI follows the CI processes discussed in Section 3.3. The CI processes, in turn, ought to function in synergy with positive intelligence. CI not only safeguards intelligence operations, but also renders inside information on competitors highly useful to executives. In addition, deception, disinformation, and other such projects support a company in achieving its business objectives. This is thus a more a practical illustration of the theoretical postulations per **Figures 3** and **4** which put business objectives and strategy as the pivot around which CI and CCI evolve.

Conclusion

This paper forms part of a still spare yet fast-growing body of academic literature which views CCI as a practicable approach for governments, businesses, and other sizable entities for securing and for advancing cyber interests. Proliferating threats and trends affecting cyber security are not all bad. Contradictory as it may appear, the more extensive adversarial cyber action the greater the potential opportunity could be for counter-exploitation. The call for cyber CCI should not be misconstrued as a call for a free-for-all cyber Wild West. Performed haphazardly and in a silo, CCI could be self-destructive.

There are several pre-conditions for effective CCI. To be effective, CCI should be an integral part of multi-disciplinary CI– conceptually and in practice. In academic literature, however, such conceptualisation is lacking. For the most part researchers have endeavoured to progress with CCI theory construction, without a sound foundational explication of CI. Theory so formulated and models so constructed could hold serious negative repercussions on a practical level. Within counterintelligence, the price for bad theory is eventually costly failure. As pointed out in an earlier contribution: "Conceptual models are not mere theoretical, academic constructs. Models condition our thinking and our approach to practice. What we therefore need is a sound overarching CCI model that can synergistically bind developing theory" (Duvenage & von Solms 2013).

Therefore, this paper aimed to put the counterintelligence in cyber counterintelligence. This was done through conceptualising CCI as part of multi-disciplinary CI and the applications of time-tested CI constructs to the cyber sphere. Secondly, the article offered a few conceptual constructs as the beginning of the construction of such a model. In so doing, it demonstrated the degree to which conventional, time-tested CI constructs can guide CCI's conceptualisation. The actual construction of a credible model, however, will require extensive in-depth, multi-disciplinary research and debate.

References

Ball, J, Borger, J & Greenwald G 2013, 'Revealed: How US and UK spy agencies defeat Internet privacy and security', *The Guardian*, viewed 30 Sept. 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/>.

Bardin, J 2011, 'Ten commandments of cyber counterintelligence', as adapted from Olsen, J *'Ten Commandments of Counterintelligence'*, viewed 9 Jan. 2013, <http://www.csoonline.com/article/2136458/identity-management/ten-commandments-of-cyber-counterintelligence---adapted-from-james-m--olson.html>.

Clarke, R 2004. *Intelligence analysis: A target-centric approach*, CQ Press, Washington, D.C.

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

--- 2014. *Hacking back: Offensive cyber counterintelligence*, McGraw-Hill, New York.

Carrol, J 2009, 'Cyber counter intelligence', *Defense Tech*, viewed 03 Dec. 2012, <http://defensetech.org/2009/03/09/counter-cyber-intelligence/>.

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

Corbin, K 2013,''Aurora' cyber attackers were really running counter-intelligence', *CIO*, viewed 1 May 2013, <http://www.cio.com/article/732122/_ Aurora_Cyber_ Attackers_Were_Really_Running_Counter_Intelligence?page=1&taxonomyId=3133>.

Dictionary.com, 2014 '*counterintelligence'*, viewed 13 Jan. 2014, <http://dictionary.reference.com/browse/ counterintelligence>.

Duvenage, P 2010, ‘Open-source environmental scanning and risk assessment in the statutory counterespionage milieu’, Ph.D. dissertation, University of Pretoria.

--- 2013, ‘Counterintelligence’, ed. H Prunckun,. *Intelligence and private investigation: Developing sophisticated methods for conducting inquiries,* Charles C. Thomas, Springfield IL.

--- & Hough, M 2011, ‘The conceptual structuring of the intelligence and the counterintelligence processes: Enduring holy grails or crumbling axioms–*quo vadis*?’ *Strategic Review for Southern Africa*, University of Pretoria, Pretoria.

--- & von Solms, SH (2013). “The case for cyber counterintelligence”, *5TH Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, IWSP'13, Pretoria.

Francq, A 2001, ‘The use of counterintelligence, security, and countermeasures’, eds. F Fleisher & D Blenkhorn, *Managing Frontiers in Competitive Intelligence*, Quorum Books, Westport.

Farchi, J 2012, ‘Offensive counter-intelligence and cyberwarfare—a paradigm shift in information security’, *ISACA*, viewed 11 Nov. 2012, <http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d% 2D9997%2 D4b62%2D96a4%2Da36fb7e 171af&ID=261>.

Giles, L 2002. *Sun Tzu–The Art of War,* (Translation), Dover Publications, New York.

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

Helton, D 2013, ‘Human threat and cyber counterintelligence–An agent’s perspective’, *Speartip*, viewed 4 Jan. 2014, <http//www.speartip.com/ >.

IBM 2013, *IBM protects clients from security attacks with new cloud solution,* viewed 22 Nov. 2013, <http://www-03.ibm.com/press/us/en/pressrelease/42269.wss>.

(ISC)^2 Michigan Chapter 2013, *Events Diary,* 8 Nov. 2013, viewed 2 Jan. 2014,
< http://isc2chapter-westmi.org/category/events/>.

Kuusisto, R & Kurkinen, E (eds.), 2013, *Proceedings of the12th European Conference on Information Warfare and Security, Jyväskylä (Finland),* Academic Conferences and Publishing International Limited, Reading.

Lües, J 2012, ‘IT security has failed–Once effective, ITsecurity is now deteriorating on all fronts’, *iWeek*, no. 225.

Meyer, H 1987. *Real world intelligence*, Weidenfeld & Nicolson, New York.

Miller, N 1980, ‘What is counterintelligence–Discussants’, ed. R Godson *Intelligence requirements for the 1980’s: Counterintelligence,* National Strategic Information Center, Washington, D.C.

Nakashima, E 2013, ‘To thwart hackers, firms salting their servers with fake data’, *The Washington Post*, 3 Jan. 2013.

Odom, W 2003. *Fixing intelligence for a more secure America*, Yale University Press, New Haven, CT.

Powell, D, Wick, A & Fergus, D 2013, ‘Protecting against cyber threats’, *Security Management*, viewed 11 May 2013, <http://www.securitymanagement.com.>.

Prunckun, H 2012. *Counterintelligence: Theory and practice*, Rowman & Littlefield Publishers, Plymouth, UK.

Sims, J 2009, 'Twenty-first century counterintelligence', eds. J Sims & B Gerber, *Vaults, mirrors and masks–Rediscovering U.S. counterintelligence*, Georgetown University Press, Washington, D.C.

Van Cleave, M 2007, *Counterintelligence and national strategy*, School for National Security Executive Education, Washington, D.C., National Defense University Press, viewed 02 July 2010, <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471485>.

Voris, J, Jermyn, J, Keromytis, A & Stofolso S 2013. *Bait and snitch--Defending computer systems with decoys*, Columbia University, New York.

WEF 2014, *Insight report--Global risks 2014*, viewed 11 Feb. 2014,
<http://www.weforum.org/globalrisks2013>.