Research Article

EXTENDING THE THEORETICAL STRUCTURE OF INTELLIGENCE TO COUNTERINTELLIGENCE

Henry Prunckun[‡]

This paper consolidates the author's view on his holistic theory of counterintelligence. Based on the author's previously published research, this paper advances a theory that used a "grounded theory" approach. The study's specific purpose was to explore the theoretical base that underscores counterintelligence. Data were collected by means of a survey of the existing intelligence literature and a thematic analysis to develop the theory's propositions. The resulting theory is articulated in three axioms and four principles. The axioms are: surprise, all-source data collection, and universal targeting. The principles are grouped according to defensive counterintelligence (deterrence and detection), and offensive counterintelligence (detection—which is shared with defensive—deception, and neutralisation). The central conclusion is that counterintelligence is not a security function *per se*. Even though counterintelligence incorporates security, it has at its core analysis and acts as the keystone that holds other forms of intelligence work together.

Keywords: counterintelligence theory, counterintelligence doctrine, intelligence theory, counterintelligence

INTRODUCTION

In 2011 Varouhakis argued that there was a theoretical vacuum in the literature relating to intelligence. He pointed out that, "...the large theoretical structure of the field of intelligence does not extend into counterintelligence (Varouhakis, 2011: 495)." In pointing out this theoretical vacuum, he drew on the subject literature that underscored the fact that there were only two studies published in

[‡] Corresponding author: c/o Australian Graduate School of Policing and Security, P.O. Box 168, Manly, New South Wales, Australia, 1655.

the last few decades that attempted to specifically address the issue of counterintelligence theory.

The author agrees with Varouhakis' observations and argues that there needs to be a theoretical base on which counterintelligence (CI) practice can rest. Without a theoretical foundation an efficient and effective counterintelligence service is less likely to be achieved. This paper presents the results of a study conducted by the author that was originally published in *American Intelligence Journal* (Prunckun, 2011) and subsequently circulated in revised form as a chapter in *Counterintelligence Theory and Practice* (Prunckun, 2012). Stemming from this research, the author developed a paper based on these two publications for presentation at the February 2014 conference, *Storage and Use of Information in an Intelligence and Security Context*. This article therefore sums up the author's thinking on the topic of counterintelligence theory to date.

BASIS FOR THE STUDY

Two recent attempts to formulate a theory of counterintelligence are those by Ehrman (2009) and Varouhaskis (2011). The former treatment resulted in not so much a theory but an essay on the importance of developing a theory, and this was acknowledge by that author: "…as a foundation for theoretical work it remains incomplete….(Ehrman, 2009: 18)." The Varouhaskis (2011) treatment was an attempt "…to provide a framework by which CI officers will be able to ultimately understand, explain, and predict the intelligence-gathering behaviours of intelligence agencies domestically and abroad, as well as the employee behaviour at those agencies (Varouhaskis, 2011: 498). " In other words, it was an examination of organisational behaviour with CI as its focus. Having drawn attention to these studies, it does not detract from their importance; on the contrary, these are studies of vital import. In fact, the work these scholars have done underscores the need to developing a theory: "…I hope others will contribute to the development of counterintelligence theory and help further develop what this article attempts to begin (Ehrman, 2009: 18)."

One could argue that there is already a considerable base of evidence within the subject literature that explains such aspects as why intelligence practitioners collect data and how these data are used to support intelligence products. There is no doubt that a rich store of information has evolved on intelligence and intelligence analysis (as an example, see: Clark, 2007; Heuer and Pherson, 2011; Lowenthal, 2009; Prunckun, 2015; Ratcliffe, 2007; and Walsh, 2011).

Likewise, as Wettering (2000) argues, there is ample information on counterintelligence practice and the need for improvement. But what Ehrman (2009) and Varouhaskis (2011) point out is the lack of a systemic presentation of these practices via a theory that explains why they are performed and how each principle relates to the other. Although there have been scholarly attempts that have achieved some levels of success in advancing work toward a theory, unfortunately these have not achieved what could be considered full success (see for instance Van Cleave's 2007 treatment of the issue, which nevertheless is a praiseworthy piece of research). Kahn (2001: 79) underscored this issue when he wrote: "Almost from the start, scholars have called for a theory of intelligence. None has been advanced. Although some authors entitle sections of their work 'theories of intelligence,' to my knowledge no one has proposed concepts that can be tested." Although he wrote of intelligence in general, it applies equally to counterintelligence.

STATEMENT OF GUIDING PURPOSE

There are likely to be tens-of-thousands of personnel practicing the craft of counterintelligence worldwide (in one form or another), so it is reasonable to assume that these partitioners know what to do instinctively—through practice—as there is no theoretical basis reflected in the subject literature. The absence of an articulated theory therefore forms the rationale for this study. Given this situation, the pressing question for CI scholars is: *To guide good practice, what is the theoretical base that underscores counterintelligence?*

BACKGROUND

Individuals, corporations, the military and entire nations owe their safety and wellbeing to counterintelligence. This is because counterintelligence supports the intelligence function in all its manifestations, and in turn, intelligence supports the development of sound, rational policy (Godson, 1995). If espionage were a game, those who practice the craft of counterintelligence could be considered the game's "goal keepers." Without these practitioners the opposition would have *carte blanche* to raid the goal and score endless points. Without counterintelligence, the intelligence goal would be wide-open to such raiders.

Given this analogy, it is not difficult to see why the role of counterintelligence is commonly thought of as *security*. In fact, Johnson (1987 and 2009: 1) pointed this out well over twenty years ago that "People like to confuse counterintelligence with security." The chief reason why counterintelligence's role has been misunderstood is likely to find attribution in the fact that there is little, if any, formally articulated theory of counterintelligence to guide practice (Ehrman, 2009). Yes, there is a great deal of secrecy surrounding counterintelligence's practice and one could argue that because of this, somewhere buried in a classified document in the archives of some intelligence agency is a theory. But if it exists, not even a hint of it has made it to the subject literature. Therefore, practitioners are left to formulate what they do and how they do it based on need and not on an understanding of its theoretical principles. Though there is nothing inherently wrong with on-the-job type training for CI operatives, this kind of necessity-based approach does make for a less efficient, and hence, less effective practice because there is no link with theory.

What makes intelligence work different to the research and analytic functions found in industry and commerce (which includes collecting information) is, arguably, the fact that some aspect of the endeavour is secret (Walsh, 2011: 30–31). Secrecy is therefore a primary objective of counterintelligence. Johnson (1987 and 2009: 2) put it bluntly when he stated: "[counterintelligence] is aimed against intelligence, against active, hostile intelligence, against enemy spies."

There is some confusion between *security* and *counterintelligence*, so it is understandable that this confusion extends to the relationship between counterintelligence and other intelligence functions, such as counterespionage. Duvenage (2013: 130) says:

> ...counterintelligence is often sensationalised and misrepresented in the popular media—it is certainly distorted in fiction. Counterintelligence is portrayed as spies outgunning spies. This is, of course, not the case. [Counterintelligence sometimes] has the more mundane connotations of being principally about computer passwords, restrictions on the use of computing equipment, security guards, access control, guard dogs, and the like. This is also a skewed view.

Duvenage's (2013) argument is perhaps why CI practitioners may have gotten lost in their own *wilderness of mirrors*, as James Angleton had famously put it using TS Eliot's quote (Holzman, 2008: 3). But despite recognising this confusion, Angleton did not himself advance a theory on which counterintelligence could be based when questioned before the Select Committee to Study Governmental Operations with respect to Intelligence Activities (i.e. the Church Committee) (Holzman, 2008: 3). Whether by design or because of the genuine absence of such a theory, Angleton missed an important opportunity to provide a matchless description. The result, at best, are a number of a cobbled-together definitions that, over time, have appeared in various academic journals, professional manuals and military field manuals, as well as in media accounts about what counterintelligence does.

CONTEXT

There are many definitions of counterintelligence and Ehrman (2009) lists a number of these in his study. Without debating the finer points of these and no doubt other definitions, it is reasonable to view CI definitions as being context specific. For instance, the ones cited by Ehrman (2009) appear to treat CI as if it only applies to foreign policy intelligence or national security issues. However, experience has shown that when a nation deals with, for example, a non-state actor or a transnational criminal organisation, there is little demarcation between what might constitute a national security issue and, say, a law enforcement problem. Perpetrators, or targets-of-interest, that fall into these types of categories as "threat-agents" traverse a "radar screens" of number of functional agencies.

So, Johnson's (1987 and 2009: 2) definition of counterintelligence as an activity that is "…aimed against intelligence, against active, hostile intelligence, against enemy spies," is probably as close to the mark as one could get. However, if his definition was truncated to "an activity aimed at protecting an agency's intelligence program against an opposition's intelligence service" it might be closer to being what could be considered a universal definition. This is because the term "agency" could be used to mean any organisation or even a nation state. The term "opposition" could be used to mean any person or group (including a nation state, etc.) with hostile intent. Such a definition could then be applied equally to issues that affect national security, the military, law enforcement, or even corporate and private affairs. This wide approach to defining CI was the approach taken by this study.

APPROACH

Although Bell (2009: 61) stated that "creating theory is an art," it does require structured thinking. It is through structure that transparency and replicability of the methods used to conduct the research can be established. Transparency and replicability are at the core of the scientific method of inquiry (Prunckun, 2015) thus making it not only an art, but a science.

The research method that is widely used for developing theory is that of *grounded theory* (Strauss and Corbin, 1990). Grounded theory usually finds its home with qualitative researchers as it is a method for theorising by *grounding* the theory being developed in observation, or in other words, practice (Babbie, 2001).

Grounded theory method is simple but it is an iterative process. The iterative process requires the identification of themes followed by the use of inductive logic to assign meaning to these themes. (Bell, 2009) The process is equally applicable to primary or secondary data.

As there is no shortage of secondary information that either explains or discusses the counterintelligence, secondary data were deemed an appropriate source for this study. It offered both depth and breadth of information and was a practical way to obtain the required information (i.e. through library research as opposed to the unrealistic approach of trying to arrange personal interviews, surveys, or focus groups). Even more appealing was that these data included practitioners who wrote about their experiences as well as academics who have studied the craft of counterintelligence. In brief, the subject literature ranged from accounts by private investigators and security operatives through to those at the highest levels of national security. The tactical issues covered in these texts ranged from the commonplace (e.g. losing a surveillance tail) to the most complex operational issues to face counterintelligence (e.g. running a double agent, or "walking back the cat" after a leak or penetration by a hostile intelligence service).

Data were therefore collected from secondary sources that were in the public domain; these included scholarly journal articles and text books of various descriptions but mainly pertaining to counterintelligence, intelligence, investigation and security. Military field manuals and training texts that had been used by in-service practitioners were also reviewed as were government reports and publications.

The research process began with the posing of the question "what constitutes the principles of counterintelligence" and then moved to collecting qualitative data from the sources just described. From these data items key themes (or concepts) relating to CI principles were distilled. Then, connections between the themes were hypothesised thus yielding a set of counterintelligence principles—or in other words, the formation of a theory of counterintelligence.

The thematic CI principles were collated and connected using the technique known as *mind mapping* (Buzan, 2002). The themes were then organised into a logical structure, or model, that then formed the theory presented in the findings section below.

In short, the study used a simple step-wise process that was based on the original grounded theory method espoused by Glaser and Strauss (1967):

1) observation—collect data through empirical means;
2) theme notation—through content analysis, then identify and record key themes; and
3) formulate meaning—based on inductive reasoning, assign meaning to the observed themes.

RESULTS

Summary of the Theoretical Model

Prima facie, the principles of counterintelligence are well established but only in practice. In fact, the resulting theory may appear to some to be without surprise because these principles are so ubiquitous. However, they appear to have been overlooked in the same way that one "cannot see the trees for the forest." But by using a grounded theory approach to observe practice, a theory emerges. As with all theories, it can then be tested empirically. Findings of empirical studies—ones based on valid and reliable data—can then guide good practice.

At its core, the theory of counterintelligence states that there are four principles—to deter, detect, deceive and neutralise the opposition's efforts to collect information, regardless of why these data are collected—intelligence, subversion, sabotage, terrorism, weapons proliferation, competitive advantage, and so on.

Because this is a study into a "universal" theory of counterintelligence, these four terms have been adapted. Scholars may find synonyms for these terms in other counterintelligence contexts i.e. military, national security, law enforcement and business. For instance, the term *detection* may equate to *identification*, and so on. The temptation is to resist debate that might draw one down to terminology so that the discussion remains at a high level, focused on the overall theory.

In this sense, intelligence can include planning for any number of purposes—criminal, national security, military, business and private. Subversion can include such acts as rebellion, treason and insurrection. Sabotage is damage, disruption and incapacitation of services and process of a variety of descriptions. Terrorism can include the violent acts themselves and the means by which politically or ideologically motivates groups to express their violent messages. There may be others, but for illustrative purposes this list is sufficiently wide.

These four principles have two foci—passive defense and offensive defense; or stated another way, defensive counterintelligence and offensive counterintelligence. This theory is shown in a logical model in figure 1 but is premised on the three underpinning axioms. These axioms are essentially self-evident propositions on which the theory-dependent principles rest.

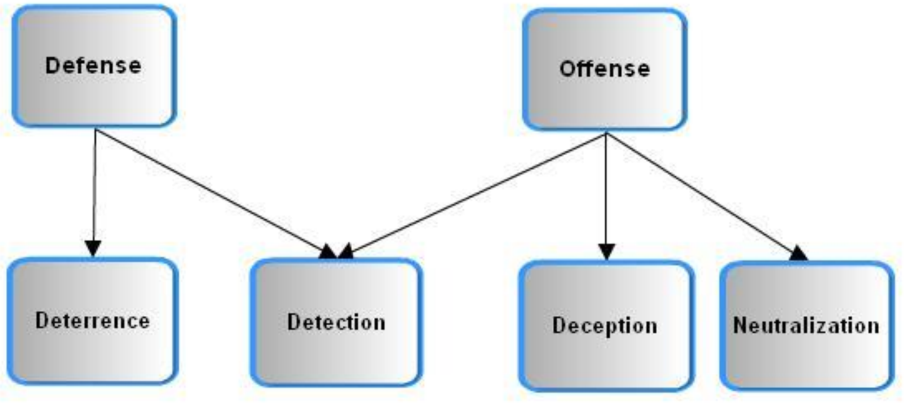

Figure 1 — A logical model of counterintelligence

Axioms

The four CI principles are contingent upon three axioms that are in affect statements of condition—there are deemed to be true and must exist for the theory to stand. (Hospers, 1973)

Axiom of Surprise: The first axiom is that the purpose of counterintelligence is to support other intelligence functions so these functions can achieve operational surprise. It does this by establishing and maintaining secrecy. Surprise may take many forms; in the military sense it might be an attack, or in a national security sense the ability to call the bluff of a foreign leader regarding a geo-political issue. Law enforcers may translate surprise into a scenario where they are able to provide the community with safety by being able to execute search warrants on to gangs for illegal firearms. Businesses may be able to use surprise in developing and launching a new range of services or products ahead of its competitors (Franqu, 2001).

Axiom of Data Collection: The second axiom is that an "opposition" will use various means to collect data on an "agency's operations. (See the discussion of the use of the terms "agency" and "opposition" within this study in the section entitled Context above.) An opposition that does not intend to collect data on the agency *ipso facto* does not warrant a counterintelligence program. This axiom also considers the means employed by an opposition will include *all* available avenues to collect data—ethical and unethical; legal and illegal. (Winks, 1987: 328) By grounding this axiom in the most dangerous possible attack vector the theory allows CI practitioners the ability to formulate a number of possible solutions.

By assuming the worst case, such strategies allow analysts to plan the resources they need to deal with a range of possibilities, from the most minor situation up to and including the catastrophic (Godson, 1995:231). If this reasoning did not form part of this proposition, the possibilities would be limited, thus providing inadequate countermeasures for all risks. By incorporating a worst case premise into this axiom allows analysts to formulate a number of contingency plans. Should the countermeasures be circumvented by the opposition, it also allows for analysts to estimate what resources will be needed to mitigate the effects of a successful attack, and recover from that attack.

Axiom of Targeting: An opposition will direct its data collection efforts toward obtaining information that will lay bare an agency and how it operates (as well as the entities the agency services to protect). That is, the target of a hostile information collection operation will focus on data that will expose an agency's structure (legal/constitutional as well as its chain-of-command and personnel), its sphere of operations and influence (e.g. geographic, economic and political/social), its current capabilities (in all regards) and its future intentions.

Moreover, it will target the factors that limit the agency's operations and its administrative, managerial and functional vulnerabilities.

The reason why these areas are targeted is that it allows an opposition to concentrate its efforts on vectors that will offer surprise, allow it to inflict the most damage (however defined), or allow it to leverage the most advantage in order to neutralise the agency's operations to protect itself and its client(s) (if any).

Principles of Defensive Counterintelligence

Principle of Deterrence: Deterrence is the ability to prevent an opposition from gaining access to information. Deterrence in this context can be both the ability to discourage an opposition from attempting to conduct a penetration operation or by denying an opposition's data collection operation once it has been launched and is underway.

Underlying deterrence are three premises that must be met or else it will fail. The first premise is that of *unacceptable damage*. An organisation must be able to deliver some form of harm upon its opposition in order for that opponent to be deterred. Deterrence in the counterintelligence sense is different to that used in the context of international foreign relations, where it is used to, for instance, contain the aggressive behaviour of an opponent state through the threat of retaliation. In a counterintelligence context, deterrence is simply an agency's ability to persuade its opposing force (OPFOR) that the costs or the risks of mounting an information collection operation outweigh the benefits (in a sense, this could be construed as a form of "retaliation").

The second premise is that the threat has to be *perceived* by an opposition. If an agency wants an opposition to cease unethical or illegal data collection, then the opposition must realise that such a threat has in fact been made; it is of no value if the threat is not communicated.

The third premise is that of *credibility*—the threat must be credible to succeed. Credibility, in turn, comprises two elements, the first that the organisation making the threat is *capable* of delivering the "unacceptable harm," and second that it has the *will* to do so.

Deterrence forms the bulk of what comprises defensive counterintelligence and, in the main, this takes the form of physical security, information security, personnel security and communications security (*information security* should not be confused with *computer security*. Information security is used here in its widest form; that is, documents and papers, electronic data, software, knowledge, and artefacts). Security is the bedrock on which this principle relies. Although security does not act as an absolute deterrent, it is the keystone.

Principle of Detection: Detection is the act of noticing that an event has taken place and that the event is somehow associated with a breach or potential breach of confidential information. There are five premises that comprise the principle of detection and these are:

1. Identifying an event of concern;
2. Identifying of the person(s) who were involved in the event;
3. Identifying the organisational association of the person(s) of interest;
4. Identifying the current location of the person(s) of interest; and
5. Gathering the facts that indicate that the person(s) committed the event.

An *event of concern* is used here as a generic term that could be anything that could be at the center of a hostile information collection operation. For instance, it could be the temporarily removal of documents from an office for copying. It could be the passing of information from an employee to an opposition organization, or it could be the unauthorised observation of classified information. The examples could be endless, but suffice to say that the event of concern is, in law enforcement terms, the "alleged breach." With regard to counterintelligence, it is the event that has given rise for concern.

To be able to identifying such events, a counterintelligence officer needs to have in place systems that will bring these events to their attention. Systems might include the observations of a person in the office who has been trained to report issues of this nature; or it might be technical systems, like alarms or digital image recordings of people's activities within the office. Regardless, without systems in place detection is diminished and the event may go unnoticed, which is after all what the hostile information collection operation is anticipating.

If an event is detected, then the perpetrator(s) needs to also be identified. Without this, the ability of assessing the damage caused by the breach is lessened. For example, a counterintelligence officer could not conclude with confidence who was interested in the data, how it was to be used and what ramification this "lost" information could result in for the agency. CI officers could nonetheless estimate the damage and the intended purpose, but this would not be as valuable as knowing the identity of the person and the details surrounding the breach.

Closely associated with detecting the person involved is identifying the person's association with any organisation (opposition or otherwise). It would be hard to envision an individual acting solely on their own without any association with anyone else or with any other organisation. Spies collect data and in the normal course of their employ, pass it onto intelligence analysts in a headquarters setting who then synthesise this information and produce intelligence reports. Even in the case of small operations in, say the business community, where a competitor is seeking insight into another firm's service or product, the data is handed from the information collector to someone who will (formally or informally) process this information and use it for planning.

Unless the case involves a private individual who has unilaterally embarked on a personal mission to, for instance, "expose" some dealings of the agency (or its client), then it is hard to conceive a situation where no one else in involved. Even in a situation of such a "man-on-a-mission" case, they would presumably hand-over the information they collect to some legal authority or the news media as a way of exposing the disagreeable behaviour at the core of their mental disquiet (e.g. Fowler, 2011).

Regardless, it is important that the person's association with others is identified as it not only allows for the counterintelligence officer to understand what needs to be done in terms of damage control, but it also helps detection and evidence gathering—motivation is key to many a successful counterintelligence investigation. Knowing who one is looking for, by name and other identifying traits, makes locating that person feasible.

Finally, the ability to gathering facts that directly or indirectly indicate a person's complicity in an event of concern concludes the principle of detection. With the facts of the events in hand, the counterintelligence officer has the full picture of the event—what, when, who, how, why. Generally, termed *criminalistics* or *forensics* this includes the use of science and scientifically-based techniques to locate, collect and preserve evidence of the event. However, unlike a pure criminal investigation, the end purpose of collecting evidence in a counterintelligence investigation may not be prosecution in a court of law, but instead to mount a counter-operation (i.e. see offensive counterintelligence below) in order to obscure, confuse or deceive the opposition.

So, with any event of concern, the ability to detect and identify the perpetrators would cause an opposition to be less inclined to attempt a hostile operation to target an agency's information. If it does not, and the opposition is still inclined, it forces them to become far more sophisticated, which may place them beyond their technical capability, or it places them at such risk that the consequences out-weigh the benefits. If the opposition does carry-out a more sophisticated operation, then it makes the counterintelligence officer's job harder, but paradoxically, the counterintelligence officer can deduce the likely identity of the perpetrator, and by doing so contribute to the first principle of counterintelligence theory—deterrence.

Principles of Offensive Counterintelligence

Principle of Deception: Deception involves misleading an opposition's decision makers about some aspect of the agency's operations, capabilities or intentions (or those of its client). The end state is to have the opposition form a view that makes them take action (or not act) so that these actions prove futile. Or, deception operations may be aimed at causing confusion thus delaying an opposition's ability to react effectively, or to project a false understanding that sends the opposition down a path that wastes its time and resources, thus placing the agency in a far stronger position than before. Double agent operations are classic in regards to the latter. (Winks, 1987: 342–343)

Renowned examples of counterintelligence deception were the various operations carried-out in the lead-up to the Allied invasion of Nazi-occupied Europe during World War Two. One was Operation Bodyguard. This operation was designed to convince German leadership and decision makers into believing that the Allies invasion would be timed later than it actually was, and that the invasion would be at locations other than the true objective of Normandy. For instance, Allied forces were well aware that the Nazis were collecting information on the preparations they were making for invasion with the view to determine the landing sites (Stevenson, 1976). With such intelligence, the Nazis could have mounted a formidable defense that repelled the attack, as they did in 1940 when British, French and Belgian troops were forced to evacuate Europe from a beachhead at Dunkirk, France (i.e. Operation Dynamo) (Gardner, 2000).

Principle of Neutralisation: Blocking of an opposition's intelligence collection operation can be done though the method of *neutralisation*. This principle is based on the concept of "defeat"—that is, collapse, failure, rout, or ruin.

The ability of an opposition to be successful with its intelligence collection operation is predicated upon the premise it will be successful. This counterintelligence principle suggests that hostile operations can be thwarted by either destruction or paralysis. It can also be occur by causing a loss of interest or enthusiasm to carry-out the operation (or continuing to carry-out an operation), or by inflicting a loss of confidence on an opposition that will be unable to achieve its objective (in whole or part).

Destruction in the military sense is easy to visualize—for instance, the destruction of forward observation posts, whether they are manned or electronic, or the killing of reconnaissance forces sent forward to reconnoiter. However, in other intelligence operations it might be the arrest of a spy cell or the transfer of a suspected spy to a remote office or location where they have no access to classified data (e.g. where not all the elements of *detection* have been established).

Although neutralisation by paralysis is not as dramatic as destruction it can be as effective. With paralysis an agency must be able to cause an opposition to halt any actions that might lead it to gain access to classified information (or further access if already underway). Unlike destruction where "demolition" of the operation is the goal, paralysis is concerned only with inflecting a temporary disruption of, say, a key process, or a temporary disruption to communications so that direction, leadership, coordination or command is lost, thus dooming the operation to failure. The intent is to cause the abandonment of the operation and the dismantling of, perhaps a spy ring, by the opposition to avoid detection. Paralysis can be actions that are initiated by an agency as a pre-emptive measure to flush-out an opposition operative or as part of a counterintelligence investigation.

Destruction and paralysis could be argued to be defensive counterintelligence strategies; whereas loss of interest and loss of confidence could be classified as offensive. For instance, loss of interest is predicated on the notion that if an agency can project the belief that the financial, political or other costs of collecting the information are greater than collecting the information by legal or ethical means, it will cause an opposition to lose interest in the operation. Another approach to causing a loss of interest is if the agency can project the belief that the value of the information is so low that it is not worth collecting, or by presenting a more tempting alternative, which might also form part of a deception strategy.

Causing a loss of confidence is a more esoteric method. It involves an organisation being able to inflict upon an opposition's operative an event or set of events that cause that operative (or his master controller) to become dysfunctional to the point that he is either detected or is paralysed to the point that he is ineffective. Take for example two business competitors that aggressively vying for the same market. If an agency can erode the opposition's faith in their operative's ability to succeed, defeat will occur.

Methods for neutralised are numerous but the stand-out is the one made classic in the fictional spy genre of counterespionage. Counterespionage "…calls for the engineering of complex strategies that deliberately put one's agent(s) in contact with an adversary's intelligence personnel. This is done so that an adversary can be fed with disinformation which will hopefully lead to confusion, thus disrupting the adversary and allowing the perpetrator to prosper (Prunckun, 2010: 10)." "Counterespionage is like putting a virus into the bloodstream of the enemy (Winks, 1987: 422)."

DISSCUSSION AND CONCLUSIONS

If we return to the analogy of financial investment one could argue that anyone promoting the notion of a low risk but high yield investment is akin to the alchemist peddling the idea he can turn lead into gold. Extending the financial analogy to intelligence work, one would be hard-pressed to argue that running an intelligence operation, or conducting a secret research project, could be performed without the need to mitigate risk.

In order to provide utility to the support of sound CI practices, this study sought to formulate a theory of counterintelligence that was grounded in empirical observation. The study used secondary data from the subject literature as the basis for its observations.

What can be concluded from these findings? The first and foremost is that counterintelligence is more than a security function. It has, at its core, analysis and because of this, acts as the keystone that holds other forms of intelligence work together—for instance, tactical, operational, warning, and strategic intelligence. It is argued that the craft of counterintelligence could not function efficiently or effectively without producing policy options that are based on fact and reason. Reasoned argument is, in essence, analysis. So, counterintelligence practice needs to be based on analytic output. This may in turn join together with the research function of positive intelligence, and perhaps it should as a matter of course as the two could work hand-in-glove to achieve the same overall objective.

As for the practice aspects that CI analytics informs, these too are more than traditional security. The theory states that defensive measures constitutes only half of the practice—deterrence and detection. However, these principles of counterintelligence are also more than simply "blunting the opposition's ability to…" as the saying goes. These defensive functions need to dovetail with the offensive side of the craft—to deceive and to neutralise.

With regard to offensive counterintelligence, the theory highlights the active role it plays in misleading an opposition's decision makers through deception and to destroy or paralyse the opposition's ability to continue with its intelligence operation. Both of these functions cannot be effectively performed without considering the defensive functions interaction. Without such a theoretical understanding, a successful agency counterintelligence program would be hamstrung.

Nevertheless, by viewing counterintelligence according to the two foci put forward here—defense and offense—we see that defensive counterintelligence gathers together those activities that contribute to deterrence and detection, whereas offensive counterintelligence are those activities that contribute to deception and neutralisation. Having said that, detection may also be included as part of offensive counterintelligence. The reason detection could be included in both categories is because its role can be to provide a means that secures information and the facilities that holds these data, as well as "hunting" those who have breached those controls.

In summation, this theory of counterintelligence is not one that could be described as being conceptually dense, but nonetheless it is one that clearly articulates the four principles that explain why counterintelligence practice is performed as it is, or as it should be… It also presents the three axioms that lay the conditions on which these principles rely. Therefore, an understanding of the relationship between theory and practice can be used not only to improve a CI program's performance but help avoid catastrophic security failures (or penetrations).

Theory can do this by providing scholars with the ability to formulate hypotheses that can be tested: for example, *a purely defensive approach to protecting information is less effective than one that incorporates offensive* *measures*. Because this is a universal theory of counterintelligence, it allows the context to be varied so it too can be tested: for instance, *a purely defensive approach to protecting national security information is less effective than one that incorporates offensive measures, but in a business context, incorporating an offensive role will be counterproductive*. Using such hypotheses, scholars can then define variables and operationalise them. Take the first hypothesis above as an example: *offensive measures* could be operationalised into, say, double-agents, agent provocateurs, sleepers, walk-ins, or any number of other manifestations of the concept offensive measures.

Finally, having a basis to explain why and how CI practitioners carry-out their craft in a testable form also gives rise to the possibility of exploring metrics that could be used to measure CI outputs as well as outcomes.

Prunckun (2010: 2) stated: "intelligence is…not a form of clairvoyance used to predict the future but an exact science based on sound quantitative and qualitative research methods. Intelligence enables analysts to present solutions or options to decision makers based on defensible conclusions." The same is true for counterintelligence. With this paper, and the previously mentioned published research on the topic (Prunckun 2011 and 2012), it is hoped that the profession is in a position to accept that there is now a theory that underpins the craft. With the passage of time it is anticipated that other intelligence scholars will build on this theory so that solutions to CI problems, based on defensible conclusions, can be implemented.

REFERENCES

Babbie, Earl (2001). *The Practice of Social Research, Ninth Edition*. Belmont, California: Wadsworth.

Buzan, Tony (2002). *How to Mind Map*. London: Thorsons.

Clark, Robert M. (2007). *Intelligence Analysis: A Target-Centric Approach, Second Edition*. Washington, D.C.: CQ Press.

Duvenage, Petrus C. (2013). "Counterintelligence," in Prunckun, Hank (ed.), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*. Springfield, IL: Charles C Thomas Publisher Ltd.

Ehrman, John (2009). "Toward a Theory of Counterintelligence: What are We Talking About When We Talk About Counterintelligence?" in *Studies in Intelligence,* Vol. 53, No. 2.

Franqu, Alain (2001). “The Use of Counterintelligence, Security and Countermeasures,” in Craig Fleisher, David Blenkhorn, editors *Managing Frontiers in Competitive Intelligence*. Westport CT: Greenwood Publishing Group Inc.

Fowler, Andrew (2011). *The Most Dangerous Man in the World: How One Hacker Ended Corporate and Government Secrecy Forever*. New York: Skyhorse Publishing.

Gardner, WJR (ed) (2000). *The Evacuation from Dunkirk: 'Operation Dynamo,' 26 May–4 June 1940*. London: Frank Cass Publishers.

Glaser, Barney, and Strauss, Anselm (1967). *The Discovery of Grounded Theory*. Chicago: Aldine.

Godson, Roy (1995). *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*. Washington, D.C.: Brassey’s.

Heuer, Richards J., Jr., and Pherson, Randolph H. (2011). *Structured Analytic Techniques for Intelligence Analysis*. Washington, DC: CQ Press.

Holzman, Michael (2008). *James Jesus Angleton, the CIA, and the Craft of Counterintelligence*. Amherst: University of Massachusetts Press.

Hospers, John (1973). *An Introduction to Philosophical Analysis*, second edition. London: Routledge and Kegan Paul.

Johnson, William R (1987). *Thwarting Enemies at Home and Abroad: How to be a Counterintelligence Officer*. Bethesda, Maryland: Stone Trail Press.

Johnson, William R (2009). *Thwarting Enemies at Home and Abroad: How to be a Counterintelligence Officer*. Washington, DC: Georgetown University Press.

Kahn, David (2001). “An Historical Theory of Intelligence,” in *Intelligence and National Security*, Vol. 16, No. 3.

Lowenthal, Mark M. (2009). *Intelligence: From Secrets to Policy, Fourth Edition*. Washington, D.C.: CQ Press.

Prunckun, Hank (2010). *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*. Lanham, Maryland: Scarecrow Press.

Prunckun, Hank (2011). "A Grounded Theory of Counterintelligence." *American Intelligence Journal*. Vol. 29, Number 2, December 2011, pp.6-15.

Prunckun, Hank (2012). *Counterintelligence Theory and Practice*. Lanham, Maryland: Rowman & Littlefield.

Prunckun, Hank (2015). *Scientific Methods of Inquiry for Intelligence Analysis, Second Edition*. Lanham, Maryland: Rowman & Littlefield.

Ratcliffe, Jerry H. (ed.) 2007. *Strategic Thinking in Criminal Intelligence*. Sydney: The Federation Press.

Stevenson, William (1976). *A Man Called Intrepid: The Secret War 1939–1945.* London: Book Club Associates.

Strauss, Anselm, and Corbin, Juliet (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage.

Van Cleave, Michelle K (2007). *Counterintelligence and National Security*. Washington, D.C.: National Defense University Press.

Varouhakis, Miron (2011). "An Institutional-Level Theoretical Approach for Counterintelligence," in *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 3.

Walsh, Patrick F (2011). *Intelligence and Intelligence Analysis*. New York: Routledge.

Wettering, Frederick L. (2000). "Counterintelligence: The Broken Triad," in *International Journal of Intelligence and Counterintelligence, Vol 13, No.* 3.

Winks, Robin W (1987). *Cloak and Gown: Scholars in the Secret War*. New York: William Morrow and Company.

ACKNOWLEDGEMENT

The author would like to thank the referees for their helpful comments.

ABOUT THE AUTHOR

Dr Henry (Hank) Prunckun is Associate Professor of Intelligence Analysis at the Australian Graduate School of Policing and Security. He specialises in the study of transnational crime—espionage, terrorism, drugs and arms trafficking, as well as cyber-crime. He is the author of numerous reviews, articles, chapters, and books. He is the winner of two literature awards and a professional service award from the International Association of Law Enforcement Intelligence Analysts. He has served in a number of strategic research and tactical intelligence capacities within the criminal justice system during his twenty-eight year operational career, including almost five years as a senior counterterrorism policy analyst during the Global War on Terror. In addition, he has held a number of operational postings in investigation and security.

- o O o -