Research Article

FIRST PRINCIPLES OF INTELLIGENCE ANALYSIS: THEORISING A MODEL FOR SECRET RESEARCH

Henry Prunckun[‡]

Leveraging off of the author's previously published research, this paper advances a set of *first principles* for a paradigm on intelligence analysis. The study used a grounded theory approach to explain a theoretical framework about "secret research." Data were collected by means of a survey of the subject literature on intelligence, and thematic analysis was used to develop the theory's propositions from these unstructured (i.e. qualitative) data. The resulting theory is a system of propositions that is *coexistent* rather than being *sequential*. The theory's six propositions state that intelligence research is: 1) conducted in secret, 2) identified within the intelligence cycle process so that data collection and analysis can be problem focused. In this regard, intelligence analysis can be 3) offensive as well as 4) defensive, but 5) it must be timely, and 6) its findings need to be defensible. The proposition of defensibility comprises seven research methodological axioms: 1) data must be valid and 2) reliable, and when possible, the research methods employed should use: 3) randomness, 4) experimental design; 5) pre- and post-tests, 6) inferential statistical tests, and 7) multiple measures of observing the data.

Keywords: Intelligence theory, analytic theory, theory development, first principles, theorising, secret research, intelligence research

BACKGROUND

One could start the discussion of first principles by posing the question, "Why should we be concerned with intelligence?" The answer is simple—because intelligence enables individuals and organisations who seek to exercise control over particular situations. In this sense, control equates to power. As Marrin (2007: 828) states, there needs only be two factors for intelligence to

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

exist: "power and competition." Cohen (1975: 41–42) in his classic treatment of the study of power writes:

> Power is sought because without power the security and even the ability of [one] to continue to exist is generally decreased. Without power, [one] has no ability to deter another . . . from actions whose consequences threaten the vital interests of the former. Without power [one] cannot cause another . . . to do that which the former desires but which the latter desires not to do. Power is sought because the more power that [one] has, the greater is the number of [his or her] available options. The more options available to [one], the greater [his or her] security. The greater [his or her] security, the better off [he or she is]. [He or she is] more secure in [his or her] life and in the enjoyment of [his or her] private property.

Intelligence is, therefore, not a form of clairvoyance used to predict the future but a science based on sound quantitative and qualitative research methods adapted largely from the social and behavioral sciences (as well as the humanities and other academic disciplines). But as Lowenthal (2009: 6) points out: "Intelligence is not about truth. If something were known to be true, states would not need intelligence agencies to collect the information or analyse it. . . . [So,] we should think of intelligence as a proximate reality . . . [Intelligence agencies] can rarely be assured that even their best and most considered analysis is true. Their goals are intelligence products that are reliable, unbiased, and honest (that is, free from politicisation)." In this regard, intelligence enables the analyst to present solutions or options to decision makers based on defensible conclusions.

But at this juncture it should be noted that such conclusions are not absolute, and there will always be some level of probability or uncertainty involved with presenting intelligence findings (i.e. proximate reality). Nevertheless, uncertainty can be reduced and conclusion limits further defined so decision makers understand the boundaries. This must be contrasted with making decisions based on "a hunch," "instinct," "luck," "gut feel," "belief," "faith," "trust," or "hope." So, conducting intelligence research is like shining of a light into a dark place.

Having said that, the word *intelligence* conjures up assorted notions of spying and espionage, secrets, and the world of exotic gadgetry. Yet to others, the word *intelligence* is closely associated with the Orwellian concept of Big Brother—a world of hardball politics and an uncompromising quest for influence. To some degree, intelligence work is associated with these concepts. But here the study of intelligence is approached from the focus of the analytic methods that turn information into intelligence. This process is based on methods used in applied research rather than the James Bond-like devices used by cinema heroes or in the authoritarian oppression exercised by some of the world's police states.

RATIONALE

First Principles

In the post–September 11, 2001 world, analysts have searched for scholarly material to help them develop their analytic skills as well as assist them understand the theoretical base on which the craft of intelligence research is founded. This paper advances a theory of secret research—intelligence analysis—which is founded on what is argued to be the discipline's *first principles*.

First principles refers to the fundamental concepts on which a theory rests. This theory can be applied to the various types of intelligence practice: national security, military, law enforcement, business, and private sector intelligence (i.e. that is, intelligence activities practiced by operatives/organisations other than law enforcement, national security, or the military).

This paper expands the results of my previous study of the issue which were published in *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition* (Prunckun, 2015: 2–15). This paper extends those findings by constructing a more integrated theory of intelligence analysis. It demonstrates how observations of the various disciplines associated with intelligence analytics can be unified into a single broad theoretical framework. This theoretical model contributes to the debate by putting forward a consolidated view of secret research in the form of a set of *first principles*.

PROBLEM IN CONTEXT

It has been argued that that information is the unrefined, raw material used to produce finished, focused intelligence. Without information, intelligence could not exist. But trying to define information is difficult but not impossible. Information is like gravity and electricity, as it cannot be defined by tangible examples. Nevertheless, its properties can be observed and described, thus enabling improvement in the analytic methods that produce intelligence. The problem hard sciences face in trying to define gravity and electricity has never prevented engineers from designing and building applications that involve these phenomena. Therefore, a lack of a physical variable does not prevent analysts from producing intelligence from what we call *information*.

It is safe to say that every facet of our lives, whether central or incidental, is in some way related to information. We rely on an alarm clock to wake us in the morning, the newspaper to tell us what is happening in the world beyond the end of our street, the radio to alert us if rain is expected, an array of indicator lights and meters on our car's dashboard to tell us about the car's performance as we drive to work, traffic lights and signs to alert us to road conditions, and on we could go until the clock tells us it's time to lay our work aside and to go off to sleep.

Individuals, organisations, and indeed whole societies owe their survival to information. The concept of community is only possible because of our ability to collect, store, retrieve, and transfer information from one person or body corporate to another. The more complex our society, the more it necessitates the conversion of information into intelligence.

VARIABLES DEFINED

There are many definitions of *intelligence* and this appears to have given rise to some scholars asserting that there is no agreed position on what it means. This is simply not the case. Although there may be as many definitions as there are intelligence scholars, the differences amount to mere word smithing. This is because the various definitions in circulation have commonality that can be narrowed to four meanings.

Dictionaries use what is referred to as an "order of definitions" in cases where there are multiple definitions. They order the definitions by synchronic semantic analysis to clarify the different meanings. Taking this approach for the many uses of the term *intelligence* that appear in the subject literature can be deduced to mean:

1. Actions or processes used to produce knowledge (Prunckun, 2015);
2. The body of knowledge thereby produced (Schroeder, 1983);

3. Organisations that deal in knowledge, e.g., an intelligence agency (Walsh, 2011); and
4. The reports and briefings produced for decision makers in the process or by such organisations (Andrew, et al., 2009: 1).

However, it is axiomatic that these four meanings take place in the context of secrecy. Otherwise, these definitions could apply to other forms of research. Moreover, in this paper, intelligence as a process (i.e. definition 1 above) is categorised by the different functions it performs. *Knowledge* in the context of intelligence equates to *insight*, or viewed another way, the ability to *reduce uncertainty*. Insight (in other words, *advantage*), and therefore, certainty, offers mankind the ability to make decisions that enable civilizations to take better control over the "unknown." But it should be noted that insights are not produced through mystic rituals; insights are produced through processes based on sound quantitative and qualitative research methods that culminate in *defensible conclusions*. In this sense insights relate to *probability* and/or *prediction*. Expressed as an equation, intelligence could be shown as:

$$\textit{(secrecy (information + analysis = intelligence} \therefore \textit{insight} \Rightarrow \textit{reduces uncertainty))}$$

The elements of this equation will be discussed shortly in relation to the grounded theory of intelligence.

INTELLIGENCE AS A PROCESS

The intelligence process is a series of procedures or steps, forming what has been traditionally termed the *intelligence cycle*. In recent years the term *intelligence process* has gain popularity over intelligence cycle as it has been recognised that it is not really a cycle *per se*, but a process. Nonetheless, this cycle, or process, is initiated by a decision maker who poses a question or requests advice. This is termed an *intelligence requirement* (in some intelligence agencies, such as the military, this is referred to as *essential elements of intelligence*—EEI). The intelligence requirements are forwarded to an intelligence agency and the cycle begins.

I argue that the intelligence process consists of seven steps (see figure 1). Some scholars may contend that this process could be defined in few steps (by consolidating some), or more steps (by expanding particular steps). Nevertheless, my view is that the seven I outline accurately describe the process without abbreviating what is entailed, or unnecessarily increasing the phases by adding further detail. The first five steps focus on converting raw data[1] into intelligence:

1. Direction setting (i.e., problem formulation and planning);
2. Information collection;
3. Data collation;
4. Data manipulation and processing; and
5. Data analysis.

This resulting intelligence is then treated with two further steps:

6. Report writing; and
7. Dissemination to decision makers (which would include provision for feedback).

Depending upon the initial intelligence requirements (e.g., the research objective), a single "loop" may be sufficient to complete the intelligence research project and provide the decision maker with the insight sought. However, in practice, further data may need to be collected with the cycle beginning again, or the cycle may have two or more tasks being performed at once and may double back before advancing again. For instance, once the research question has been formulated and the data collection plan devised, an outline of the report may begin, and as the more readily available pieces of information flow in, a database or spreadsheet may have been constructed and the data collated.

Furthermore, even before all the data are received, some preliminary analysis may be carried out, and depending upon the results (e.g. at the collation stage which some analysts view as low grade analysis), further information may be requested (e.g., if by chance these results show the data would be inadequate to answer the research question or a serious limitation noted). This would mean that the data collection plan is revised and field operatives called on to gather more or different data, and so on.

As long as a specific intelligence operation is being conducted, the analytic process will be continuous—forming a cycle. As new information is being collected and collated, other data will be manipulated and analysed. The resulting outcomes will be disseminated for either immediate use and/or used to set new collection goals.

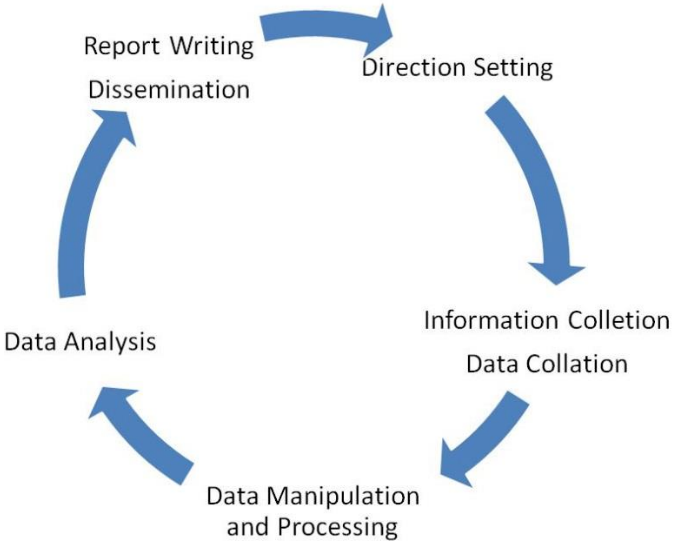

Figure 1—The intelligence process.

The dissemination of the intelligence product can take a variety of forms. Take for instance the case of business intelligence—it could be a background history on a company or one of its executives, a diagram of a company's office layout, identification of new projects being researched, a prediction on the intended release of a new product, staff salaries, the classification and number of personnel on a company's payroll, and the like.

The intelligence cycle is not unique to intelligence research but has parallels with research cycles in academic disciplines—*open research* (Prunckun, 1996: 70–72). For instance, the research cycle that is used in applied social research shares the same pattern:

- Establish a plan for information collection and carry out initial field work;
- Observe, discuss and collect data;
- Analyse the data and write the report; and

- Distribute the report and gather feedback that can be used to formulate further disseminate strategies.

INTELLIGENCE ANALYSIS THEORY

Why should we know about the theory of intelligence analysis if we can define it, and once defined, recognise intelligence in any of its fours meanings? Because theory offers both scholars and practitioners the ability to understand how and why intelligence is what it is, and does what it does. Without a theory it is difficult to posit a view about an intelligence related phenomenon and then test that hypothesis through empirical observations to see if the results support the hypothesis, or reject it.

Although scholars have called for a theory of intelligence for decades, unfortunately until 2009 the literature was, I would argue, largely devoid of such theorising. Gill, Marrin and Phythian (2009) published an anthology of papers that addressed this "missing" intelligence theory issue to some extent, as did Marrin's (2007) paper on a general theory of analytic responsibilities. Amongst the collection of essays by Gill, Marrin and Phythian (2009) were treatments by key opinion leaders such as professors David Kahn, Michael Warner, and Jennifer Sims. Although there are other scholars who have discussed the issue elsewhere in the subject literature (Walsh, 2011: 295–298), these researchers were, arguably, at the time of this writing in the forefront of the debate. However, surveying the theories advanced in Gill, Marrin and Phythian (2009) edited volume, it is evident that there is little consensus between the papers and nothing I would call an integrated theory of intelligence analysis. Nonetheless, these scholars are to be commended for progressing the debate by contributing to the discourse.

Given this situation, I responded to Walsh's (2011: 295) call to build theory so that it might "...contribute further to developing the discipline of intelligence." I saw this as an opportunity to provide an integrated theoretical framework that consolidates empirical findings and well-understood insights from the subject literature. This paper suggests such a theory; and like Marrin's (2007) "general theory" of analytic responsibilities, one that is not military- or national security-centric. This is because the world of intelligence is no longer able to operate in such a neatly defined parameter. The post-9/11 world is vastly different to the siloed operations that were hallmarks of the Cold War. Present intelligence research projects can stride several categories of intelligence work—

for instance, law enforcement issues may impact on national security or military issues in the form of, say, espionage, terrorism, or the trafficking in arms, drugs and people, or a range of cyber-crimes. These issue may also impact on business (business intelligence) and private sector organisations (e.g. NGOs operating in developing countries).

GROUNDED THEORY OF INTELLIGENCE RESEARCH

A *grounded theory* methodology, which I used to develop a complementary theory of counterintelligence,[2] was applied to observations made by surveying the intelligence subject literature. Grounded theory is an inductive process that examines data and constructs theory from the ideas and concepts that are collated into categories (Bell, 2009; Charmaz, 2009). The analysis of these data (i.e. the survey of the subject literature) formed the basis for the resulting theory of intelligence analysis.

My theory of intelligence analysis has its roots in the four definitions that were put at the beginning of this paper. There may be many other definitions of intelligence due to the fact that some scholars disagree with certain semantic constructions of “this-or-that” definition, it was, nonetheless, still possible to extract the core meaning from these various definitions in the subject literature. The results was the four unencumbered definitions presented above. These “conditions” therefore become the foundation on which I rested the theory. Reiterating these definitions, they are:

1. Actions or processes used to produce knowledge;
2. The body of knowledge thereby produced;
3. Organisations that deal in knowledge;
4. The reports and briefings produced for decision makers in the process or by such organisations; and
5. The fifth condition is that is required in order for intelligence research to occur in any or all of the four preceding definitions is that there needs to be some incorporation of secrecy.

Theoretical Framework

Having surveyed the subject literature and collated various research concepts and ideas into categories, it became apparent that there were six propositions that explained the various definitions of intelligence. This forms a system of propositional units—a theory. These propositions consistent and integrated, and state that intelligence is driven by decision-makers' priorities so that they can respond to the need to project power in the face of competition/adversity (Marrin, 2007: 831). Each of the propositional units relates to the others in a relationship that is *coexistent* as opposed to being a set of *sequential* units. This means that all propositions need to be present for intelligence research to exist, but one proposition does not need to follow the other (they simply need to be present): 1) intelligence requirements need to be identified within the intelligence cycle process so that data collection and analysis is problem focused. This intelligence research can be either 2) defensive *or* it can be 3) offensive, and that intelligence needs to be 4) timely, as well as it needs to be 5) defensible. In terms of the last proposition, it comprises seven research methodological axioms—i.e. premises that are evident and accepted on face value.

Proposition 1—Secrecy is Provided via Counterintelligence

If the fifth condition discussed in the section above is not present, *intelligence research* then becomes *open research*. This is because the *knowledge* that is produced in either enterprise—intelligence or research—results in knowledge. It could be argued that knowledge leads to insight, and insight results in reducing uncertainty in decision making, but unless secrecy is involved, it is merely research. Having said that, secrecy will be context driven—what is secret for one agency may not be for another, or it may not be in a certain situation. The equation expressed earlier in this paper presents a logical model for the theory of intelligence:

$$\textit{(secrecy (information + analysis = intelligence} \therefore \textit{insight} \Rightarrow \textit{reduces uncertainty))}$$

Expressed in narrative form intelligence theory might go something like this: Under the veil of secrecy—provided through the counterintelligence function[3] (Prunckun, 2012)—analysts obtain information and analyse it. This process results in intelligence (knowledge) and therefore provides insight to decision makers (reports and/or briefings), which in turn reduces uncertainty. This takes place within an organisation (or unit within an organisation, etc.) that's role is to engage in intelligence (secret research).

If the requirement for secrecy is removed from the model, we can see how it transforms intelligence into research. By way of example, take the case of an open research project being conducted by, say, clinicians and researchers who are exploring treatments for some of the more common forms of arthritis. Using the intelligence model just discussed, it can be seen that all the principles apply—analysts (researchers) obtain information and analyse it. This results in knowledge and therefore provides insights to decision makers (in this case, the development of a suitable drug), which in turn reduces uncertainly (that is, it gives certainty to manufacturing or other processes involved in the drug's effectiveness and/or production). But what is different is the use of counterintelligence to provide secrecy. This makes research *open research*—anyone could, potentially, access this information (or at least in a limited form of circulation as per, perhaps, a "private policy," if conducted under the auspices of some organisation, but certainly not in a classified way as per intelligence). Open research (or as it is sometimes termed, *open science*, which includes social and behavioural sciences as well as the humanities) makes data, methods, and research findings accessible to the inquiring public.

In contrast, if some level of counterintelligence (secrecy) is applied, the research now becomes intelligence—in this example, *business intelligence*, to place it in the correct typological classification. Not all aspects need to be secrets, but the literature suggests at least one. Comparing this supposed case of drug research to military analysts who might be researching a question about the development of a new weapons system by an unfriendly nation. In the course of their inquiries they may access open source information—say, the *curricula vitae* of certain academics in that nation who are known to be experts in the particular technology needed to develop such a weapons system. Cleary, these data are freely available via the universities websites that employ them; but the fact that the research project is secret, the methods of analysis are classified, and other aspects of the endeavour are undisclosed, makes this *intelligence*.

Proposition 2—Intelligence Requirements, Data Collection and Analysis

The literature suggests that defining intelligence requirements (or essential elements of intelligence) is driven by decision-makers, yet some scholars posit that analysts must not be reactive and should drive the process of identifying topics, issues or problems that need examining (Marrin, 2007: 831). This theory of intelligence analysis puts forward the view that it cannot be one or the other; intelligence analysis must be flexible enough to accommodate both. For example, in a private intelligence setting where an organisation's concerns are narrowly focused, the decision-maker model may be valid. Whereas in a national security or law enforcement context, a hybrid model where decision-makers set priorities is combined with analysts who advance questions that might need addressing. By perusing a flexible model for setting intelligence requirements (whether they are strategic, operational or tactical), subsequent data collection and analysis will be problem focused.

Proposition 3—Defensive Intelligence

Defensive intelligence is concerned with providing decision makers with insights into how to deal with threats, vulnerabilities, and risks. Defensive intelligence is applicable to five typological classifications discussed earlier—national security, military, law enforcement, business, and private sector intelligence. Defensive intelligence can be concerned with several related aspects of defense—for example these might include: prevention, preparation, mitigation, damage control/response, and recovery (and perhaps other areas).

Proposition 4—Offensive Intelligence

If intelligence research is not used defensively, it can be used in an offensive capacity. Intelligence can be used to assist decision makers plan offensive missions. A simple example is that of targeting in the military. Targeting analysts use intelligence to task military assets so they can damage or destroy enemy capabilities; provide advice for immediate fire or manoeuvre; or to support of deep offensive operations. Examples of the application of offensive intelligence to other intelligence typological classifications are conceivable. Offensive intelligence might include estimative or strategic intelligence because these categories of research projects concern themselves with outmanoeuvring emerging threats.[4]

Proposition 5—Timely

In order for intelligence to be useful, it must be provide in a timely fashion. If an intelligence report or briefing is not provided to decision makers on time, it is *prima facie* that the insights cannot be used. *Timely* may also include the notion of *continuous*—which is applicable in cases where an event is unfolding and updated intelligence is needed on a regular basic.

Proposition 6—Defensible Conclusions

Defensibility takes into account several factors. These include the need for the analytic process that produces intelligence to be transparent and replicable. Transparency means transparent to those who are within the defined circle of trust, not transparent to anyone outside that circle.

The reason for transparency is to allow those reading the reports, or receiving the briefings, to understand the methodological thinking. In academia this is known as reproducibility of results. But to do so would be most unusual, nevertheless what is likely is that a process of assessment will be carried out in the same vein when an academic research report is peer-reviewed for methodological soundness. Reproducibility underscores the fact that intelligence is based on the same research first principles as other types of applied research (barring the element of secrecy)—that is, the use of the scientific method of inquiry, which is based on sound quantitative and qualitative research methods (Prunckun, 2015).

Some scholars refer to this as *auditable*. But regardless of whatever term is used, replication means that, say, the reader of an intelligence report can understand the collection methods, collation and analysis techniques used (and understand why these were selected), and be able to derive similar conclusions as the analyst did from the study's findings. It is not to say that the next time the intelligence cycle is repeated that the same findings will be produced—it means that if the same data and methods used to arrive at the position articulated in the report were employed, it would be reasonable to expect similar results.

Even though the environment in which intelligence operates is dynamic, it does not stand in the way of the concept of replication. Applied social research is analogously the same—rarely does an issue under investigation remain static. There are numerous independent variables in any research question that can be added, removed, or changed. This applies to intelligence research too.

If transparency and the ability to replicate an intelligence study are present, then the findings are able to be "defended." Integrity tied to this factor are the concepts of relevancy and accuracy—these are concepts often discussed in relation to intelligence research reports. The argument concerning these concepts is that if the proposition of defensible is maintained, by default, these two factors are also catered for, but it requires a set of axioms to help explain the reasoning behind it.

To achieve relevancy and accuracy in intelligence research output, a metaphoric potpourri of related research design considerations needs to be adhered to. These axioms suggest superior methodological design, and with these comes a more robust defence. Not all of the following axioms may apply to every intelligence research project, but as axioms they provide superior methodological design (Thyer, 1989):

*Axiom 1—D*ata must show a high degree of internal validity;

Axiom 2—Assessment methods for dependant variables must show a high degree of reliability;

Axiom 3—Random sampling will prove better to more error prone sampling techniques;

Axiom 4—Experimental designs should be used when possible;

Axiom 5—Pre- *and* post-test are better than post-test only studies;

Axiom 6—Use of inferential statistical tests are superior to qualitative assessments/impressions only; and

Axiom 7—Multiple measures for observing the issue under investigation are more desirable to single measure approaches.

DISCUSSION

Why does it matter that we have a theory of intelligence research? Because theory allows us to test propositions—questions about, say, the efficacy of certain intelligence approaches, or operational methods, or procedural practices, as well as other issues facing the profession. For instance, it allows us to test the effectiveness of intelligence concerns in terms of outcomes, outputs, and processes. As Walsh (2011: 295–297) put it, it allows the development of the discipline of intelligence.

So what would intelligence scholars and practitioners test with such a theory? Well, prominent amongst the list of possible responses is the so-called phenomena of *intelligence failures*. For example, research questions that evaluate how intelligence agencies prioritise, task, and/or resource research into developing issues (strategic problems) versus current issues (tactical targets), and how these tensions might result in an "intelligence failure." Take for instance the now ill-famed example of weapons of mass destruction where, "[President] Bush turned to [CIA Director] Tenet. 'I've been told all this intelligence about

WMD and this is the best we've got?' . . . Tenet rose up, threw his arms in the air. 'It's a slam dunk case!'."[5]

Using this theory, other research questions can be formulated and tested. Findings of such empirical studies—ones based on valid and reliable data—can then guide good research practice. In sum, this theory of secret research could not be described as being conceptually dense, but nevertheless it is one that articulates the six coexistent propositions that explain why intelligence research is performed as it is, or where it is not, as it should be.

Perhaps other intelligence scholars will refine this theory so that the theoretical framework that underpins the craft of secret research is even better understood. "All being well, one would anticipate that, in the fullness of time, this and other yet to be articulated [intelligence research] theories will spawn better policy options. These policy options will therefore be based on defensible conclusions that are grounded in empirical research." (Prunckun, 2012: 48)

NOTES

1. *Raw information* is sometimes referred to as *unassessed intelligence*.

2. In 2011–2012 I advanced a theory of counterintelligence. I saw it as a way to fill the void in the subject literature that had existed for decades. My paper on this issue, along with the method I used, was published in progressively revised versions in the following publications: *American Intelligence Journal* (Volume 29, Number 2, December 2011, pp. 6–15), Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2012), and Henry Prunckun, "Extending the Theoretical Structure of Intelligence to Counterintelligence," *Salus Journal,* Vol. 2, No. 2, June 2014, 31—49.

3. Space in this paper limits my discussion of counterintelligence. I suggest that scholars who are interested in this intelligence function see Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2012) for a more detailed discussion.

4. Acknowledging that counterintelligence can also have an offensive focus and therefore could be included in this discussion (see Prunckun, 2012).

5. Former CIA Director George Tenet's reported reply to then-President George W. Bush regarding his question about the threat posed by Iraq. Quote as cited in Woodward (2004: 249).

REFERENCES

Andrew, Christopher; Aldrich, Richard; and Wark, Wesley (2009). *Secret Intelligence: A Reader*. London: Routledge.

Bell, David C. (2009). *Constructing Social Theory*. Lanham, MD: Rowman & Littlefield.

Charmaz, Kathy (2009). *Constructing Grounded Theory*. Los Angeles; Sage.

Cohen, Ira S. (1975). *Realpolitik: Theory and Practice*. Encino, CA: Dickenson Publishing.

Gill, Peter; Marrin, Stephen; and Phythian, Mark, editors (2009). *Intelligence Theory: Key Questions and Debates*. New York: Routledge.

Lowenthal, Mark M. (2009). *Intelligence: From Secrets to Policy*, fourth edition. Washington, DC: CQ Press.

Merrin, Stephen (2007). “Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities,” in *Intelligence and National Security*, Vol. 22, No. 1.

Morris, William, editor (1971). *The American Heritage Dictionary for the English Language*. Boston: American Heritage Publishing Co. and Houghton Mifflin Company.

Prunckun, Henry (1996). “The Intelligence Analyst as Social Scientist: A Comparison of Research Methods.” *Police Studies*, Vol. 19, No. 3.

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

Prunckun, Hank (2015). *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition*. Lanham, MD: Rowman & Littlefield.

Schroeder, Terry L. (1983). *Intelligence Specialist 3 & 2, vol. 1*. Washington, DC: Naval Education and Training Program Development Center.

Thyer, Bruce (1989). “First Principles of Practice Research.” *British Journal of Social Work*, Vol. 19.

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

Woodward, Bob (2004). *Plan of Attack*. London: Simon & Schuster

ACKNOWLEDGMENT

I would like to thank the three reviewers for their comments and advice.

ABOUT THE AUTHOR

Dr Henry Prunckun, BSc, MSocSc, PhD, is Associate Professor of Applied Research 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, including, *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition* (Rowman & Littlefield, 2015), *How to Undertake Surveillance and Reconnaissance* (Pen & Sword Books, 2015), *Intelligence and Private Investigation* (Charles C. Thomas, 2013), and *Counterintelligence Theory and Practice* (Rowman & Littlefield, 2012). 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.

- o O o -