Issue 2, Number 2
2014

Salus Journal

A peer-reviewed, open access e-journal for topics concerning law enforcement, national security, and emergency services

Special Issue on the Storage and Use of Information in an Intelligence and Security Context–Beyond 2014

Published by

Charles Sturt University

ISSN 2202-5677

Issue 2, Number 2

Charles Sturt University

Issue 2, Number 2, 2014

www.salusjournal.com

Published by

Charles Sturt University
Sydney, New South Wales, Australia

ISSN 2202-5677

Salus Journal

Issue 2, Number 2

2014

Special Issue

Contents

Licensing

Editorial

STORAGE AND USE OF INFORMATION IN AN INTELLIGENCE AND SECURITY CONTEXT–BEYOND 2014

Associate Professor Felix Patrikeef, University of Adelaide

Special Edition Editor

Between 12 and 13 February 2014, Kathleen Lumley College, University of Adelaide, hosted a conference with the theme, *Storage and Use of Information in an Intelligence and Security Context—Beyond 2014*. The aim of the conference was to examine the nature of information and intelligence retention in the Asia–Pacific region, as well as the issues concerning how these data might be shared.

I am grateful to my co-organisers for their assistance in making this event reality: Mr Jason Sargent, Mr Simon Hall, Ms Allyson Sandham, and Mr Mark Robinson. My thanks also go to the scholars who presented: there were speakers from Australia, Asia, and Europe who discussed issues on topics that covered both the historical and contemporary importance of intelligence in preserving global political stability.

Although Asia–Pacific intelligence is often seen as being associated with dealing with crime syndicates and the spread of radical Islamic terrorism, the papers presented went beyond these topics and explored the question, “Who retains information in the Asia-Pacific region, and how should it be shared and protected?”

I would like to go into detail about the presentations and authors, but because the conference was by invitation, it meant that the papers, although not classified, were presented under Chatham House Rules. Suffice to say, the three papers published in this special edition of *Salus Journal* characterise the insights provided by those authors who were not able to get publication clearance from their agencies for their manuscripts. I commend these papers to you and in doing so I convey my appreciation to the associate editors of the journal’s Editorial Board who kindly donated their time to the peer-review process.

- o O o -

Analytical Essay

NORTH KOREA—STILL AN INTELLIGENCE PROBLEM

Stephan Blancke[*]

A few years after Kim Jong Un came into office, North Korea is still attracting controversy in the headlines, and political sanctions are still in operation. Despite the harsh measures in place to isolate Pyongyang from sources of money and luxury, the rulers are able to get what they want using front companies or the help of other states. The reasons for this are deeply rooted in the North Korean political structure. A network of high ranking officials, their children, and political minions are grappling for power and wealth. Beside the powerful Kim clan there exist other families in North Korea whose loyalty must be secured with bribes. If the loyalty of the influential families is eroded, the power base of Kim Jong Un is likely to soon diminish. As a result, the North Korean government is searching for sources of money. Illicit drugs may be one solution the ruling regime find attractive to this problem, but there appears to be a twist: struggling ordinary citizens are showing signs that they too are taking part in this illegal enterprise. This is manifested by their willingness to become involved in crime in the same way as the corrupt regime.

Keywords: Bongwhajo, North Korean intelligence, Chinese intelligence, drug trade, organised crime, Princelings, clan structures, intelligence cooperation in East Asia

INTRODUCTION

For several decades, North Korea has been accused of a range of violations regarding international legal norms. In addition to the violations relating to human rights, which are not the subject of this discussion, there are the issues of: drug trafficking, counterfeiting of drugs as well as currency, laundering of money, trafficking of arms, the trade in endangered species, insurance fraud,

[*] Corresponding author: stephan@blancke.de

people smuggling, and prostitution. However, there is a distinction that needs to be drawn between crimes committed by the state and those committed by non-state actors. For instance, prison camps, forced starvation, and executions undoubtedly constitute a crime by the state and those responsible for their commission should be tried in the International Criminal Court in The Hague.

Nonetheless, the crimes described in this analytical essay are seen from a different perspective: these are typically developments within the country where only a few who can be classed as privileged because of their position with the regime are able to attain luxury and power. Corruption and nepotism are common features of this system and parallel political orders that have existed in other totalitarian systems, such as the former Soviet Union. In North Korea, one can observe an increasing separation between the corrupt elite and the ordinary people who are forced to go without. In order to survive under this state enforced austerity, ordinary people are also engaging in these corrupt activities. Based on this situation, the conclusion that presents itself is that the population of North Korea is taking a very big risk in operating on the black market, stealing "public property," and smuggling illicit drugs into China (as well as consuming these drugs themselves).

One cannot describe all of the North Korean elite as corrupt or criminal, but the political system produces conditions that are favourable to the growth of corruption, which in turn distances individuals from the "normal" socio-political process that has the hallmarks of a society which embraces high ethical standards. Due to the strict international sanctions imposed on North Korea, it appears to have become a state that has to search for alternative ways to obtain goods and currencies. There is evidence that the ruling elite in North Korea has demonstrated a great desire for luxury goods—so, the use of bribes paves the way for a lifestyle beyond what could normally be afforded while sanctions are in place. Bribes also secure the “loyalty” of other influential families within the country, drawing them together into what could be seen as a “corrupt collective.”

In order to maintain their hold on power, the North Korean elite needs a large bureaucratic and military apparatus—North Korea has one of the largest armies in the world—and this organisation needs to be funded. Given the dire financial situation in North Korea, financing a military is not always possible. To cope, the various ministries and government entities are trying to use alternative means within their control to generate profits in order to procure sanctioned goods. By way of example, there are various sanctions which cover nearly every relevant part of North Korean activities related to their security apparatus, the military, and the lifestyle of the elite. Many aspects are listed by the United Nations, such as the ban on export and import of certain goods and technologies, luxury goods, the embargo on arms and related material, or the freezing of economic resources, funds and financial transfers. These sanctions have not stopped the ruling elite from acquiring luxury goods—this is due to the expanding trade between North Korea and China (see figure 1).

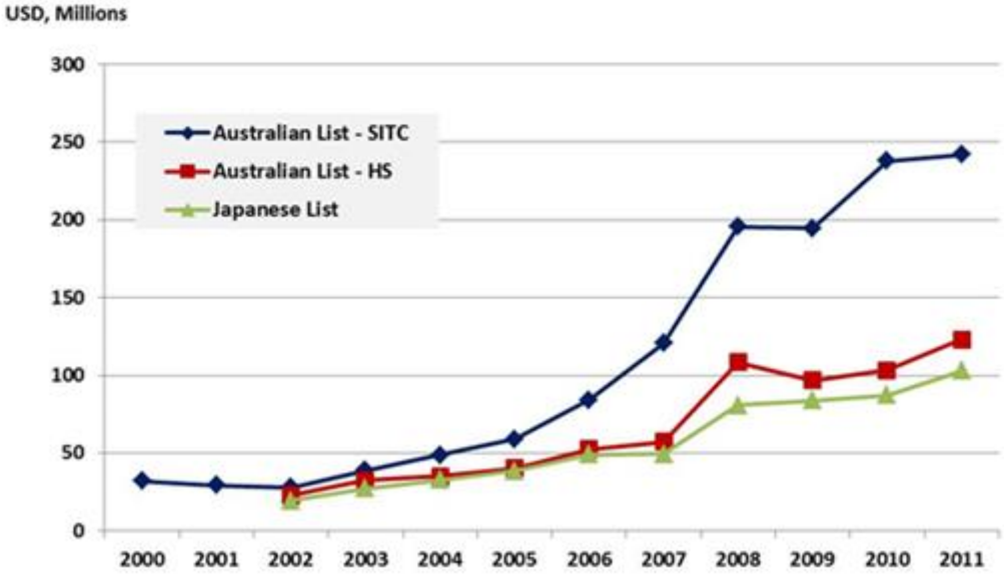


Figure 1 — Chinese Luxury Goods Exported to DPRK (Source UN Comtrade, KOTRA, 2006)

Compared to the luxury trade with the European Union or Russia, one can see in figure 1 that the delivery of luxury goods from China could be considered stable: they can be described as a compensation for the loss in other parts of the world. A recent analysis of the Li Fang Wie (Karl Lee) case shows the system of Chinese front companies that are dealing with North Korea—but only as long as the money flows. So to achieve this "flow," the North Koreans have resorted to illegal activities because legal methods have been blocked by the international sanctions. The necessary financial transactions cannot be performed without problems because, for instance, opening a bank account on behalf of a North Korea entity is problematic. Thus, the North Korean government has been forced to find alternative ways to transfer funds and to invest.

Kang (2013) writes about the ineffectiveness of sanctions: "However, sanctions are also unlikely to achieve their stated goal of changing North Korean behaviour." In this analytic essay the success or failure of the sanctions is not discussed, but suffice to say that sanctions are coming under increased criticism. In the main, this is because any transaction between North Korea and China regarding luxury goods are not affected.

The key areas that present problems to the international community will be discussed. These issues underscore the need for a new form of cooperation between intelligence agencies. Although it may not always look outward, Western intelligence, as well as some of the most important agencies of East Asia, have a fundamental interest in getting control over the trade in illicit drugs, sensitive technologies, and certain types of intellectual expertise. The tracking of people or materials across borders should no longer be the hurdle that it has been. For example, the lack of surveillance of charter flights across Asia could be a reason for the “seeping” of weapons and ammunition into crisis regions of the world. Even traditional political reservations may not dampen the cooperation of individual North Korean officials. Such discrete guided discussions need further development and the pressure placed on influential members of the elite might yield positive results should they be increased.

CURRENT ISSUES

Two aspects of currency issues will be discussed here—namely the counterfeiting of currencies, and the trade in illicit drugs. The US Secret Service has accused North Korea of being actively engaged in the counterfeiting of high-quality US currency—the so-called *Supernotes*. Different numbers have been cited over the years, but they are rather irrelevant in an international comparison of currency counterfeiting. For instance, the number of investigations carried out in relation to counterfeit currencies in South America are much higher than those that reportedly coming from North Korea. An employee of the US Secret Service said in a statement before the Senate: "During the same timeframe as that of the Supernote investigation, our investigation into counterfeit currency produced in Colombia yielded seizures in excess of $380 million. The amount seized is also low when compared to the large volume of genuine US currency in circulation worldwide." (Merritt, 2006: 2)

Several states have pointed out that the United States would not provide any evidence for their accusations, which echoes its past claims that were directed against Hezbollah. In this situation, the main accuser has been a North Korean defector who alleged he had been involved in various frauds. However, in general, the testimony of defectors must be taken cautiously (DeForest and Chanoff, 1990) because until a full counterintelligence evaluation is undertaken, it is difficult to assess the veracity of their stories (Prunckun, 2012).

> The Swiss Federal Criminal Police in its *Falschgeld Lagebericht* (Counterfeit currency report) 2004–2005 described accusations of counterfeit currency production as largely unverifiable on technical grounds. According to anonymous intelligence sources who spoke to IHS Jane´s, North Korea has also not yet managed to acquire the technology needed to produce high-quality counterfeit currency. (Blancke, 2104)

Although in the past North Korean officials with counterfeit currency have been repeatedly observed while operating abroad, this could be explained by the fact that North Korean officials are often not sufficiently paid and therefore tend to do business in a legal gray zone in order to increase their income. Moreover, there appears to be some expectation on them to send funds and gifts to the ruling family in North Korea.

Nevertheless, it could be argued that it is a criminal act without mitigation because of the difference that lies between private actors who commit such an act and those done by and for the state under some form of duress. For intelligence agencies and security police, this presents a special problem: North Korean criminal activity can be protected by that nation’s global security apparatus (Blancke, 2009). As an example, state resources, such as vessels or aircraft can be used, or perpetrators can smuggle currency inside diplomatic bags. Evidence is sketchy, but if more complex intelligence analysis was carried out, a clearer picture of the extent of these covert activities might emerge. Nonetheless, forged currency is not the central issue—the transfer of funds and their uncontrollable disappearance in the global financial system is an bigger area of concern.

Even though it is difficult to prevent the transfer of monies internationally, it is nevertheless important to intelligence operations to be able to understand the logistics that support these activities—Who is involved in the transferred money and where does it end up? Do these funds contribute to political benefits and for whom? Can it lead to political destabilisation?

To date penalties and warnings by various world governments have not discourage these large monetary transfers by North Korea. These alternative options appear to allow North Korea to transfer funds, to speculate with it on world markets, and to invest and re-invest. Pontell, Fang, and Geis (2014) said:

> The PRC government has banned state workers from traveling to Macau in an effort to prevent potential embezzlement and squandering of public funds. In 2007, the mainland government reiterated its ban, calling gambling by officials 'malpractice' and declaring that 'swift action and severe punishment' would be taken against malefactors. Despite such government warnings, one researcher at Beijing University estimates that officials gamble up to 600 bilion Yuan in public money every year in Hong Kong, Vietnam, Laos and North Korea as well as Macau.

In addition, the transfer of funds can be carried out anonymously, and techniques for obfuscation can also be used by the North Koreans. (Kim Jong-un´s, 2013) It is possible, for example, to make a money transfer via mobile telephone (cell phone) across multiple middlemen to North Korea. (Plaza, 2011) However, other possibilities exist for the North Korean government to participate in the international financial market. Companies can be established in China that profitably sell North Korean products abroad. Likewise, there are several Chinese firms, or networks of Chinese firms, that are said to be active in North Korea—there finances remain largely closed to Western intelligence agencies. (The 88 Queensway, 2009)

DRUG TRAFFICKING

Another important issue that is relevant to the regional security situation between China and North Korea is the illicit drug trade across their common border. For years the problem of North Korea drug trafficking has reflected the changing demands in the region. In particular, the drugs seized at by China at it border suggests a sizable demand for illicit pharmaceuticals in that country. In addition, there are reports that suggest that precursor chemicals are stopped at the border as well as very pure synthetic drugs.

According to the finding of previous studies, the source of these drugs appear to originate from North Korean pharmaceutical laboratories, however finding hard evidence of this direct link is difficult because of the secrecy surrounding the trade. A recent case has highlighted the global dimensions that demonstrate the drug connection to North Korea. It involves the smuggling of methamphetamine that was more than 99% purity, produced in North Korea, and smuggled internationally by different actors who were from various countries. Drug production is not unknown in North Korea, but presently it is particularly difficult to establish whether the individuals within the general criminal population are behind the production of these drugs, or if it is state, or some combination of both in collusion.

One such defendant who was detained in connection to a case of drug smuggling responded to a question by an undercover agent of the DEA, if they could visit the labs in North Korea:

> No, we can´t get go to North Korea . . . We take it out. If we don´t talk Korean language, they´ll have suspicions. And the NK government already burned all the labs. Only our labs are not closed . . . To show Americans that they are not selling it any more, they burned it. Then they transfer to another base. (US Indictment, 2013)

Although a simple statement by this defendant, the inferences show a complex case—beside North Korea there is the involvement of many other parties in drug trafficking, including a Triad from Hong Kong, an Outlaw Motorcycle Gang in Thailand, and various assassins in the form of former military snipers from various countries. (Manhattan US Attorney, November 2013)

DISCUSSION

So it may not be surprising that Western and even Asian intelligence agencies are confronted with different developments:

1. Ordinary people of North Korea are producing drugs and trafficking them in order to provide a somewhat better standard of living. This, in turn, encourages corruption.

2. For the same reason, some elements of North Korean state entities are involved in the trade. This also favours corruption.

3. Drug trafficking is highly likely to be protected by North Korean security authorities, and this is being done through professional criminal enterprises. This state-based protection allows this criminal activity to enjoy safety afforded by North Korean counterintelligence operations.

4. Parts of the North Korean elite are most likely involved in the drug trade and it is almost certain that they are involved in other criminal activities. With the profits they earn they can establish a luxurious life, buy

proliferation-sensitive goods and bribe influential family clans in North Korea to secure their loyalty.

4. Drugs from North Korea are sold abroad, which brings all of the well established negative societal effects of drug abuse, especially in parts of the region that borders China.

5 In addition to individuals, organised crime organisations are most certainly involved in the drug trade. Groups from Hong Kong, China, Japan, South Korea, Eastern Europe, the Golden Triangle, and probably from the Balkans as well as South America have substantial human, financial and logistical resources. In the future—especially after the much speculated collapse of North Korea—there could be a global struggle for domination of this profitable illicit market.

These factors call for improved cooperation between Western and Asian intelligence agencies and counterintelligence police (see Walsh, 2011). A political solution seems hardly possible in the current situation. Individual South American governments are seeking dialogue with drug cartels. This could be seen as a capitulation of power to organised crime.

There is little doubt that these cartels will continue seek the profits of the past, and therefore any political solution would seem to be a contradiction in goals. North Korean officials and networks are not likely to give up their sources of revenue because that would mean a loss of wealth and as a consequence, a decline in power. The future of illicit wealth for North Korean elites will be realised only in cooperation with other international actors—who in turn are operating in parallel with the legitimate global economy. In the context of drug trafficking, this provides a challenge for the Western world. (US Department of Justice, 2007)

It is suggested that it is the job of Western intelligence agencies to identify those North Korean officials who are looking for policy reforms within North Korea. But these intelligence operations need to be conducted carefully because these reformers hold a key to the only real hope for change in North Korea. The network of corrupt officials, the Princeling, and the so called Bonghwajo network, must be intensively analysed, and then neutralised. (Rank, 2012) It could be argued that Western intelligence has given too little attention to the Bonghwajo structure because its international activities considerable:

> Like ‘Crown Prince Party, or The Princelings,’ a group of the children of prominent and influential senior communist officials in China, Bonghwajo is comprised of children of ranking officials of the North Korean Workers´ Party, military and senior members of its Cabinet. Due to their parent´s influence, the children reportedly landed jobs at powerful organisations and are earning money through illegal activities such as counterfeiting and narcotics trafficking." (N. Korea´s Bonghwajo, 2011)

Having said that, the analysis of this network will be extremely difficult, but there is anecdotal evidence that this is beginning. Early results show that its members are privileged: they can travel, set up businesses, establish international contacts, and send their children to prestigious schools. It is not suggested that all of the members are criminals and it is through these that open up opportunities for intelligence agencies to establish informal channels into the regime. On the one hand, as with the communist dictatorships of the former Eastern Bloc, some open-minded North Korea individuals are likely to exist and start pushing for reforms. On the other hand, one can also assume that other individuals take advantage of the opportunities they have and transfer money abroad or participate in sanctioned activities.

Additionally, Western intelligence agencies would benefit from developing scenarios that include a change in attitude of China towards North Korea: drug trafficking, among other undesirable activities in the border region, represents an increasing provocation for China. Although many Chinese benefit from cheap North Korean labor, the unpredictable activities of North Korean criminals could affect this. (Cathcart, 2012) Social, and thus political, stability in this region is at risk if future international criminal enterprises should gain influence. China is unlikely to accept this. (Zhang, 2010) The Chinese population has an interest in ensuring that the economic development in the border region is undisturbed. (Moore, 2008)

The Chinese intelligence services and police have acted against illicit drug trafficking in recent years, and have publicly expressed their anger:

> Affected by the decrease in the output of drugs from the ‘golden triangle’ area, enormous changes have taken place in the structure of the world drugs market, and international drug trafficking forces have stepped up their infiltration and development in the Sino-DPRK border areas… Tempted by exorbitant profits, persons participating in trans-border drug trafficking in the Sino-DPRK border areas have become increasingly complicated. They

> include not only persons in inland areas, border inhabitants, jobless persons, and persons released from prison after serving their sentences but also persons living on the frontiers outside China and persons without nationality; not only full-time organizers but also temporarily hired ‘gangsters‘… Some drug crimes carry the nature of criminal syndicates or are committed in collusion with underworld and evil forces, thus causing extremely great danger. What merits attention is that following the increase in the number of the DPRK individuals who illegally enter or stay in China or are illegally employed in the Sino-DPRK border areas, drug-trafficking cases committed by such individuals are increasing. (Lijun, 2009)

The substantial military and intelligence cooperation between China and North Korea may potentially decrease in the near future, even if there are still networks between both countries, which have their roots in the past. (Blancke and Rosenke, 2011)

Despite all the negative experiences and forecasts of the past, a few developments must be taken into account. This includes the fact that there is hardly any solid evidence of involvement of the North Korean government in the drug trade at the present. It is very unlikely that these activities remain unnoticed in a totalitarian surveillance state. One must therefore assume an implicit acceptance by the responsible authorities.

As in the case of forged currency, the involvement of North Korea in the global illicit drug production is estimated to be very low. (Sovacool, 2009) However, this does not alter its illegality and the negative impact on the security situation. Incidentally, the vast majority of drug trafficking can be attributed to the deplorable living conditions many North Koreans have to suffer. (UN, 2013) Hunger, isolation, labor camps, and total government control are common facts that lead to the erosion of ethical values within any society. It is a further tragedy that there is evidence of a growing illicit drug problem following revelations by a number of North Korean refugees who have made new homes in South Korea:

> The report sent to Rep. Park Joo-sun's office revealed that 297 defectors have been incarcerated from 2009 through August of this year. Of the total, 65, or roughly 22 percent, broke the law by using outlawed substances . . . ‘There have been reports of wide spread substance abuse in the North and the high numbers among escapees seem to reflect this,’ an

> aide to the lawmaker said. He said there is a need to strengthen programs to help escapees overcome such addictions. (Drug use leading, 2014)

In recent times, South Korean intelligence services have been accumulating evidence that alleges North Korean refugees have actually been drug traffickers who were arrested by the Chinese or North Korean police. They were then given a choice: either be sent to a labour camp or infiltrate the North Korean community of refugees in South Korea. Strategic intelligence studies on these social issues are important in order to be able to forecast the likelihood of stability within North Korea.

CONCLUSIONS

Although it might appear somewhat contradictory, North Korea continues to be a stable state whose collapse has not occurred despite numerous predictions. Rather, it looks like the current government and the economic situation have been consolidated. Despite numerous sanctions, economic performance and trade with other countries, especially China, is increasing. Sanctions cannot be completely implemented and there are always new ways for North Korean companies to circumvent them.

Should other states agree to maintain the much debated sanctions into the future, then it is up to Western and Asian intelligence agencies to keep a keen focus on individual North Korean actors and their illicit networks. New intelligence methods need to be established in order to understand this opposing force—a nation that consists of different clandestine networks, actors, interests, and even ethnicities and cultures. The focus on prominent individuals may be misguided. In the past, there was intense attention placed on Pablo Escobar as a person, without paying attention to his network. Only when intelligence agencies infiltrated and analysed the network were they able to neutralise Escobar. This same method calls out to be applied to North Korea. Subject experts might explore a merging in perhaps in a special international intelligence fusion center. As long as bureaucratic barriers stand in the way there will be no long-term success.

REFERENCES

Blancke, Stephan (2009). “North Korean Intelligence Structures,” in *North Korean Review,* 5 (2), 6–20.

Blancke, Stephan, and Rosenke, Jens (2011). "Blut ist dicker als Wasser. Die chinesisch-nordkoreanische Militär-und Geheimdienstkooperation, in *Zeitschrift für Außen-und Sicherheitspolitik*, 4 (2), 263–294.

Blancke, Stephan (2014). "Criminal Connections. State Links to Organised Crime in North Korea," in *Jane's Intelligence Review*, 26 (04), 34–37.

Cathcart, Adam (7 May 2012). *Hire a North Korean: Chinese Economic Magazine*. Retrieved 6 April 2014, from http://sinonk.com/2012/05/07/hire-a-north-korean-chinese-economic-magazine.

DeForest, Orrin, and Chanoff, David (1990). *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam*. New York: Simon and Schuster.

Drug Use Leading Cause of North Korean Escapees' Imprisonment in South: Report (3 September 2014). Retrieved 6 April 2014, from http://www.globalpost.com/dispatch/news/yonhap-news-agency/130903/drug-use-leading-cause-n-korean-escapees-imprisonment-south.

Kang, David C. (2013). "Securitizing Transnational Organized Crime and North Korea´s Non-Traditional Security, in Kyung-Ae Park (ed.), *Non-Traditional Security Issues in North Korea* (pp. 75–99). Hawaii.

Kim Jong-un´s Secret Billions (12 March 2013). Retrieved 6 April 2014, from http://english.chosun.com/site/data/html_dir/2013/03/12/2013031201144.html

Lijun, Meng (2009). "Study on Problem of Trans-Border Drugs Crimes on Sino-DPRK Border," in *Journal of Chinese People's Armed Police Force Academy*, Issue 1.

Manhattan US Attorney Announces Arrests of Five Defendants For Conspiring to Import 100 Kilograms of North Korean Methamphetamine Into the United States (20 November 2013). Retrieved 5 April 2014, from http://www.justice.gov/usao/nys/pressreleases/November13/StammersScott.php.

Manhattan US Attorney Announces Arrests of Two Former US Soldiers and One Former German Soldier For Conspiracy to Murder a DEA Agent (27 September 2013). Retrieved 5 April 2014, from http://www.justice.gov/usao/nys/pressreleases/September13/HunteretalArrestsPR.php

Merritt, Michael (2006). *Statement Of Michael Merritt, Deputy Assistant Director, Office of Investigations, United States Secret Service, before the Subcommittee on Federal Financial Management, Government Information and International Security, Committee on Homeland Security and Government Affairs*. Washington, DC: United States Senate, 25 April 2006.

Moore, Gregory J. (2008). "How North Korea Threatens China´s Interests: Understanding Chinese 'duplicity' on the North Korean Nuclear Issue. *International Relations of the Asia-Pacific*, 8, 1–29.

Noland, Marcus. *Chinese Bling*. Retrieved 24 May 2014 from http://blogs.piie .com/nk/?p=7475

North Korea`s 'Bonghwajo' Club Doing Drugs, Counterfeiting (18 April 2011). Retrieved April 6, 2014, from http://english.donga.com/srv/ service.php3?biid=2011041878048

Plaza, Sonia (28 July 2011). "Is it possible to send remittance to North Korea?" Retrieved 6 April 2014, from https://blogs.worldbank.org/peoplemove/is-it-possible-to-send-remittances-to-north-korea.

Pontell, Henry N.; Fang, Quan; & Geis, Gilbert (eds.) (2014). "Economic Crime and Casinos: China's Wager on Macau," in *Asian Journal of Criminology*, 9 (1), 1–13.

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

Rank, Michael (19 January 2012). The Ponghwa Behind Pyongyang´s Throne. Retrieved 4 April 2014, from http://www.atimes.com/atimes/Korea/ NA19Dg01.html

Salisbury, Daniel, and Stewart, Ian (2014). "Li Fang Wie (Karl Lee) Proliferation Case Study Series." *Project Alpha*. London: Centre for Science and Security Studies, King´s College.

Sovacool, Benjamin K. (2009). "North Korea and Illegal Narcotics: Smoke but No Fire?" in *Asia Policy*, 7, 89–111.

The 88 Queensway Group (2009). *A Case Study in Chinese Investors´ Operations in Angola and Beyond*, US–China Economic & Security Review Commission, Washington.

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

United Nations, (2013) *World Report*. Retrieved 28 June 2014, from http://www.hrw.org/world-report/2013/country-chapters/north-korea

United States Department of Justice (2007). *Asian Transnational Organized Crime and Its Impact on the United States*. Washington, DC.

United States District Court, Southern District Of New York, *Indictment S8 13 Cr. 579*, p. 6.

Zhang, Yong-an (3 December 2010). *Drug Trafficking from North Korea: Implications for Chinese Policy*. Retrieved 6 April 2014, from http://www.brookings.edu/research/articles/2010/12/03-china-drug-trafficking-zhang

ACKNOWLEDGEMENT

The author thanks the referees for their feedback on his draft manuscript.

ABOUT THE AUTHOR

Dr Stephan Blancke is a German-based political analyst whose research focus is on international state and non-state intelligence structures. His area of expertise is North Korean and Chinese espionage, these countries international clandestine networks, and their use of front companies. His other research interest is the current development of organised crime groups. Blancke holds a diploma in administrative law as well as a diploma in political science. His doctoral dissertation examined the private intelligence activities of non-state actors, such as religious cults and outlaw motorcycle gangs. Dr Blancke works closely with the government in Berlin, Germany.

- o O o -

Research Article

IMPERIAL JAPANESE ARMY INTELLIGENCE IN NORTH AND CENTRAL CHINA DURING THE SECOND SINO-JAPANESE WAR

Simon Hall[†]

The Japanese today seek to improve their national intelligence apparatus, particularly in relation to human intelligence assets and higher echelon coordination. To be successful, Japan must examine its wartime past in the intelligence field. The Imperial Japanese Army maintained a prolific intelligence presence in North and Central China during the Second World War. Its intelligence apparatus encompassed all aspects of information collection, with considerable overlap between intelligence organisations in an effort to avoid gaps in intelligence coverage. Japan's intelligence system in North and Central China was nevertheless inefficient, exacerbated by inherent weaknesses and reactive rather than proactive alterations throughout the course of the conflict. This paper examines this lack of efficacy within Japan's intelligence system during the Second Sino-Japanese conflict, and the efforts made to overcome difficulties faced by Japanese intelligence in North and Central China throughout this period.

Keywords: Japanese intelligence, Second World War, China; puppet armies

Only recently has Japan sought to reestablish its foreign intelligence service to keep an eye on its near neigbours, a weakness in its intelligence capability since the end of World War II. Furthermore, Japan is all too aware of its lack of expertise in human intelligence capabilities (Dorling, 2011). With the formation of a National Security Council in December 2013, Japan has replaced former security and defense councils that have suffered from inefficiencies, and seeks to improve its modern-day foreign intelligence apparatus' and practices (Berkshire Miller, 2014). To guarantee requisite improvement in intelligence

[†] Corresponding author: hailsimon@gmail.com

capability, Japan must objectively examine its wartime experience in the intelligence field. This paper provides an examination of Japan's military intelligence experience in North and Central China during the Second Sino-Japanese conflict, a period when Japan's intelligence apparatus' and operations were most abundant in an area in which it now seeks improvement. Factors found within this paper may easily be transposed onto a modern civilian intelligence system.

Following the Manchurian Incident (also known as the Mukden Incident), essentially a black flag operation that lead to Japan's full annexation of Manchuria, Japanese forces in North China [and later to a lesser extent in Central China] became complacent in regard to their intelligence activities, this due to their having only ever faced inferior forces. Information on enemy forces had previously been inconsequential in Japan's previous victories, having only served to minimise casualties. As such, an ill-informed culture of inattention to intelligence matters and organisation developed (Strategic Services Unit, para. 32).

North China being furthest from Japan's strategic and tactical fronts, where fighting was still active, was considered occupied. Beyond the need to prevent subversive and guerilla activities, intelligence was no longer prioritised, and Japanese Army intelligence activities in this area were henceforth dealt with in the manner in which the commanding officer thought fit (Strategic Services Unit, para. 27). To demonstrate, in July 1940 the Chinese communist Eighth Route Army, previously held in low regard by the IJA (Imperial Japanese Army), undertook its "Hundred Regiments Offensive" resulting in the deaths of some 20,000 Japanese personnel. The offensive came as a surprise to the Japanese who at that time, despite having gathered some information on the Kuomintang, had little then on the Chinese Communist Party, this despite the conflict having been ongoing since 1937 [Kotani, 2009, pp. 44-45].

Within North and Central China, the Imperial Japanese China Expeditionary Forces (CEF), operating beneath Imperial General Headquarters in Tokyo (IGHQ), operated at the same level as the Southern Area Army in Southeast Asia and the Pacific and Kwantung Army in Manchuria. Its 2nd Section (Intelligence) was responsible for strategic information collection and intelligence coordination of forces under its command (including the collation of intelligence forwarded to it by commanders in China's North, South and Central areas) for use by its commanding officer in the formulation of war plans and dissemination to IGHQ (Strategic Services Unit, 1946, para. 9).

IGHQ operated as supreme military command, issuing only the broadest direction for intelligence, often holding itself above intelligence matters, intelligence being delegated to the IJA and IJN (Imperial Japanese Navy) General Staffs and counterpart Ministries (Gorman, 1945a, p. 1). The intelligence apparatus of the China Expeditionary Forces included the following main sections:

i) field or combat intelligence within its armies;

ii) sabotage and fifth column;

iii) espionage;

iv) counterespionage;

v) policing and peace preservation; and

vi) economic control through government monopolies (Strategic Services Unit, para. 3).

Particular areas of intelligence were usually covered *predominantly* by one particular intelligence organ (for instance, counter-espionage was for the most-part a *Kempei Tai* concern, although it should be remembered that *Kempei* Units were assigned to IJA formations). Considerable overlap existed however between the different intelligence organisations, this was considered an acceptable practice so as to avoid gaps in intelligence coverage. In Shanghai, for example, there was the Army with its counterpart Army Bureau (*Rikugun Bu*), the Peace Preservation Corps, Puppet Armies, the *Kempei Tai* and its subordinate Police Force, the Foreign Office and its Consular Police and development companies, the railroad police, and others. All areas related to intelligence were thus covered in a most comprehensive fashion by one or all of the above organisations. Rather than liaise with one another to coordinate activity and exchange information however, each organ had its own channels of reporting and maintained its own network of informants and agents (Strategic Services Unit, para. 69).

Responsibility for each intelligence function lay not with Headquarters' Head of Intelligence, but rather remained predominantly the responsibility of army commanders and their respective intelligence staffs. Notably, each army commander was neither required nor obligated to report to Headquarters each and every detail of intelligence operations within their area of operations. Armies operating within a particular area would thus operate their own intelligence organisations (Strategic Services Unit, para. 3).

Beneath the CEF operated the North China Expeditionary Force and the Central China Expeditionary Force (operations of the South China Area Army and its successor 23rd Army lay outside the scope of this paper). The North China Expeditionary Force's 2nd Section (Intelligence) served primarily as an office through which intelligence streamed, at irregular intervals, to the Supreme Headquarters in Nanking. Its role in direction, instruction and supervision of intelligence activities of those organisations within its jurisdiction, themselves only loosely connected, was only minor (Strategic Services Unit, para. 18).

The Central China Expeditionary Force Headquarters' 2nd Section (Intelligence) was located in Nanking, acting in a supervisory role over intelligence sections in formations under its command. Its scope of activity was limited, Area Army Intelligence Departments relaying information only on concerns deemed to be of particular importance to higher formation HQ. More often than not, Commanding Generals utilised information without relaying the same to CEFHQ (Strategic Services Unit, para. 62).

Area Armies maintained an intelligence section, Armies an intelligence unit, and beneath Army level Divisions and Battalions would have their own units. Reports were made to the unit commander, who would pass this information to the intelligence representative, who in turn would report this through his lines. Reports would hence be collated by progressively larger units, finally reaching General Headquarters who would assemble all available reports to develop a situational appreciation. As such, intelligence representatives and officers had no direct liaison with General Headquarters (United States Strategic Bombing Survey (USSBS), 1945, p. 5).

Only at Army level was a full-time intelligence officer employed. Below Army level personnel were tasked with intelligence duties as only part of their duties. Notably, toward the latter part of the conflict even full-time intelligence officers were undertaking other duties due to a lack of personnel (USSBS, p. 5). Brigades and Regiments did not contain designated intelligence formations, with intelligence activity being undertaken by the service units themselves. It is understandable that of primary concern to these units was information related to immediate tactical combat conditions, this information being relayed to their immediate superior formation. Other information of a non-tactical basis was no doubt collected but was incidental; reporting on the same was likely *ad hoc*, haphazard at best.

Military Intelligence Departments thus essentially operated as clearing houses for subordinate units. Furthermore, those tasked with information collection received only broad direction from upper echelon Intelligence Departments, and reporting was consequently subjective. Information relay was thus dependent on the relative importance placed on it by the officer involved.

PUPPET ARMIES

The Japanese command structure was held in high regard, and as such even the smallest of garrison units spread throughout North China might be considered frontline units of information collection. For this reason it is thought rarely were special intelligence units posted by Brigade, Division, Army or North China Army Headquarters' (Strategic Services Unit, para. 39). Aiding the Japanese, both in terms of combat troops, but also in relation to information gathering, were the "Puppet Armies" organised by the Japanese to aid in their occupation of China. The number of "puppet" troops in February 1944, according to British intelligence sources, numbered 627,200, including 299,800 regulars. Chinese Communist sources believed there to be 900,000 puppet troops in 1945, 410,000 thought to have been regulars (Jowett, 2004, p. 72).

Peace Preservation Corps were armed forces charged with military responsibility for maintaining order, including combatting guerilla forces (this in contrast to Pacification units who are thought to have dealt primarily with subversive elements, be they anti-Japanese, Communist, etc.) ("Peace Preservation," n.d.). Information was gathered by the Japanese through the use of agents and from frontline intelligence gathered by regular combat units, but also through these "puppet" formations. Combat patrols collected information on both Chungking and Communist forces. Agents were also used to infiltrate enemy lines under the guise of merchants, etc. Small towns at the front were filled with local informants, but were also covered by the Peace Preservation Corps.

By way of example, in 1938 the 5th Brigade of 43rd Army Intelligence Department, known as *Tokumu Kikan* (see below), entered and occupied Tsingtao on the Shantung Peninsula. Most of its activities were directed at Communist elements through the use of combat intelligence teams who collected information relating to enemy dispositions, public order in occupied areas, topography and weather conditions. Information was gathered through the use of local agents, including voluntary informers among the local populace, the Imperial Collaboration Army, Puppet Armies and Peace Preservation Units (Strategic Services Unit, para. 28).

The commander of the local Peace Preservation Corps in each province was concurrently the Provincial Governor, and each puppet intelligence unit within reported, through its head, to puppet civil authorities. In this manner, both civil and military intelligence were directed through the same channel. Conversely, those intelligence units not part of the Peace Preservation Corps, but within other puppet armies, came under direct control of the Japanese Expeditionary force in China, as did the army as a whole. These intelligence units came under direct command of the regular Japanese intelligence service of the Japanese army under which it operated (Byse, 1945, p. 3).

Puppet army intelligence units were then answerable to their respective army commanders yet units always had a Japanese official attached, ostensibly operating under direction of the Intelligence unit, but in actual fact the unit was under Japanese' command. A Japanese subordinate, usually placed as second-in-command, often accompanied these officers. All information was made available to these Japanese commanders but for those reports delivered on a clandestine basis directly to the puppet intelligence head or other superior officer within the puppet military (Byse, p. 3). Nevertheless, as the puppet intelligence chief, and the puppet army, answered to the Japanese at a different level, presumably such intelligence made its way to Japanese hands at a later time.

Although theoretically the puppet army intelligence organisation' was structurally separate and operated independently to that of the Japanese, it was however controlled by the Japanese, and was required to operate in Japan's interest. Intelligence products of the apparatus were provided to the Japanese commander, who, *when appropriate*, would forward these to their superiors (Byse, p. 3).

Of consequence, Japanese "liaison officers", obviously intelligence officers, were not solely employed in this role. Rather, these men acted also as the local Japanese representative in the area and as such were also charged with investigation of economic data, taxation, etc. These officials further employed their own agents, predominantly Chinese, who reported directly to them (Byse, p. 4).

Puppet commanders held considerable influence over their areas of jurisdiction, and due to a history of Chinese loyalty to their respective commanders, puppet commanders were essentially let be by their Japanese overseers in so far as nothing overly serious was committed against Japan's interests. Many puppets were thus involved in selfish criminal enterprise at the expense of local populations (Jowett, p. 69). Dissemination of information by the puppet apparatus was made on a particularly informal basis, based on personal communication between puppet commanders (Byse, p. 4). Furthermore, when safe to do so, the majority of puppet troops and officials were likely to act against the Japanese (Office of Strategic Services, Research and Analysis Branch, 1943, p. 6). Information gathered by these units and relayed to Japanese leadership was hence likely of minimal consequence, meeting minimum requirements to maintain Japanese support and patronage. Such systemic weaknesses exacerbated, even created, the need for those Japanese-in-command to develop their own agent networks as described above. These Japanese then were spread rather thin in their intelligence functionality and effectiveness.

TRAINING

The quality of the intelligence staff was lacking. When asked as to how officers were selected for intelligence duties, Lieutenant-General Arisue Seizo, Chief of the 2nd Department (Intelligence), Army General Staff, IGHQ in Tokyo from August 1942 to the end of the conflict, stated it was safe to say only second-class officers were chosen, or rather "…the dregs were thrown into the intelligence service. There was no way of choosing." (USSBS, p. 7).

Low-level intelligence staff, both officers and civilian, were selected according to their previous military service, language ability and residence in the locale of operations. Minimal training was provided. They learnt via experience (Strategic Services Unit, para. 70). No particular class or type of officer then received training solely and specifically for intelligence work. Language officers, or those who had spent some time stationed overseas, "naturally" fell into intelligence duties (Gorman, 1945b, p. 6).

Furthermore, in-depth training for intelligence staff who would hold higher position in China was essentially non-existent for the greater part of the conflict.

This lack of basic intelligence training was attributed to Japan's relatively successful operations in China without intelligence, leading to sentiment amongst General Staff Army officers that intelligence was not essential. This complacency continued until the onset of hostilities with the U.S. when Japan found itself in a war without an obvious front line, the I.J.A. finding itself without lines of communication and no intelligence planning (USSBS, pp. 6-7). Only by 1943 were many Staff Officers of CEFHQ transferred to other fronts and theatres, replaced with graduates of the Nakano Special Military Officer's School. These replacements nevertheless lacked experience, and were thought to be generally inferior (Strategic Services Unit, para. 22). Although the Nakano School, established July 1938, would train credible intelligence personnel educated in elements of intelligence outside the immediate tactical field, only a small number of graduates were available to the Japanese throughout the conflict, these being primarily sent to theatres outside China (Mercado, 2002, pp. 1-23).

Up to the Pacific conflict, little heed was paid to recruitment of Special Service personnel in China. Expatriate Japanese residents in China for some time were often employed on the assumption that their time spent in country somehow best qualified them for the work involved. Officers of IJA units stationed in China were also inducted despite having no experience, training nor aptitude for the duties involved. Such recruitment required no particular amendment prior to the "China Incident" of 1937, up until which the duties of the SSO revolved around clandestine operations and information collection (South-East Asian Translation and Interrogation Centre (SEATIC), n.d., p. 16). Practical experience served as mentor, missions of small scale being followed by those progressively larger and more complex (Leake, 1944, p. 10). Agents employed were predominantly Chinese, chosen for their contacts, intelligence, local area knowledge and reliability and trustworthiness, mentored by senior agents through field missions of increasing importance (SEATIC, 1944, p. 13).

Promotions within Intelligence, at least prior to 1943, were thus only offered after substantial service with the IJA. Activities of these officers were often not in accord with any formal plan, but rather reflected the individual interests of the intelligence officer involved. It is thought that this practice resulted in the formation of special service units (*Kikan*), formed for a specific purpose and dissolved following completion or failure (Strategic Services Unit, para. 76).

SPECIAL SERVICE ORGANISATIONS

Separate then to standard Army intelligence organisations were the *Kikan* (Special Service organisations, alternatively referred to as agencies), created by higher echelon Army Headquarters to perform particular duties and/or missions. These *Kikan* reported only to their respective Headquarters (Strategic Services Unit, para. 4).

The IJN had first sought to form a Special Service Organisation (SSO) in China around 1929, the IJA establishing its own a few years prior (Leake, p. 6). Before the "Manchurian Incident" of 1931, Japanese intelligence in China relied on Foreign Office embassies and consulates, with military intelligence dependent on Attachés. In order to avoid posting further Attachés to China, an action that would draw ire from the then Chinese Government, Japan created the position of *Chuzai Bukan* (Resident Officer), and posted these to important Chinese cities (Leake, p. 6).

From 1929 to 1937 IJA SSOs effectively came under control of the General Staff in Tokyo as their main activities related to espionage and counter-espionage, which the General Staff in Tokyo had always been responsible for (Leake, p. 6).

Numerous changes and reorganisations in the Japanese Special Service organisation occurred throughout the Chinese conflict over the span of months or even years. Around 1930 a sister organisation to the *Rikugun Chuzai Bukan Fu* (Army Resident Officer Department) was formed, known as the *Tokumu Kikan*, whose duties mirrored those of the *Rikugun Chuzai Bukan Fu* (the term *Tokumu Kikan* is here used as an overarching title rather than as a descriptive term used to identify individual Special Service units). *Tokumu Kikan* (a term also used to identify individual units) operated in area of less importance and further afield, and were established or dismantled as present conditions dictated (Leake, p. 6). The majority of *Tokumu Kikan* personnel were *Gunzoku* (civilian attachés or non-career personnel), with the largest *Kikan* having only four to five IJA personnel, with civilians, recruited there and then (Gorman, 1945b, p. 3).

With the onset of the Second Sino-Japanese conflict in 1937 came a second reorganisation. Following Japan's occupation of Nanking, IJA *Chuzai Bukan* continued to operate in Canton and Hankow, but elsewhere were dispensed with as SSOs were restructured and remodeled (Leake, 1944, p. 7). The IJA withdrew, if temporarily, their Attachés until the establishment of the Wang Ching-wei puppet government (Leake, p. 7).

The IJA SSO at this time adopted the title *Rikugun Tokumu Kikan* across all China, coming now under direct command of Supreme HQ Nanking. The *Hokushi Rikugun Tokumu Kikan* (North China IJA Special Service Department) was headquartered in Beijing, commanding IJA SSOs in Tientsin, Tsingtao, and some others in northern cities. Conversely, SSO in Nanking, Shanghai and Hankow were answerable only to IJA Supreme HQ in Nanking. The *Hokushi Rikugun Tokumu Kikan* held no jurisdiction over these areas (Leake, p. 7).

The IJA in 1938, due to the name *Rikugun Tokumu Kikan* becoming associated with espionage and counter-espionage activities, altered its title to *Tokumu Bu* but for those operations in Shanghai and Nanking. The reason for these apparent exceptions appears to lay in the function of these two formations, which were now primarily involved in collaboration with their respective puppet governments (Leake, p. 7).

With the growing importance of political intelligence, linked inextricably to the establishment of these puppet regimes by the Japanese, came the establishment of a most successful *Tokumu Kikan*, the *Ume* (Plum) *Kikan*. *Ume Kikan* was formed in 1939 under Major-General Kagasa Sadaaki with the objective to install the puppet government of Wang Ching-wei (Leake, p. 7). Following its establishment, *Ume Kikan* would remain in place to liaise with, and to further advise and lead Wang's regime (SEATIC, 1946, p. 4). Notably however *Ume Kikan* was disbanded soon after achieving its aim (Leake, p. 7). The practice of disbandment arguably diluted the pool of experienced intelligence officers available to the Japanese who were well versed in local political conditions, bearing in mind the lack of intelligence training and thus experience in the field required. The same may be said of the innumerable other *Kikan* dissolved over time.

The importance of *Ume Kikan* in the continuing evolution of Japanese intelligence in China appears nevertheless to have been substantial. Despite its disbandment in 1940, the term "*Ume*" continued to be associated with Japanese intelligence, primarily in the Shanghai area, with a particular series of intelligence reports entitled "*Ume*". Information found within these reports was however of a broad nature, often without obvious merit and of dubious credibility (Military Intelligence Service WDGS, 1945, pp. 34-36).

Control of Japanese SSOs in China was relegated in 1939 to Expeditionary or Area Army Headquarters' as "control could not be effectively exercised from Tokyo." (MacArthur, 1944, p. 15). As the puppet regime in China strengthened its position, and as military control decentralised, smaller SSOs were established, operating beneath local Area Army HQ or even Brigade HQ. One source states that around this time the Chief of Staff of the local Area Army was tasked with responsibility for SSOs, and subsequently the head of the SSO now became the former's subordinate, in effect combining Operational HQ and the SSO (MacArthur, p. 16).

With the Second Sino-Japanese War Japanese political and economic interest in China rose dramatically, as did the scope and range of SSO operations. As puppet administrations were established following the China Incident in 1937, military duties gradually became subordinate to administrative concerns, so that by 1944 military activities were only a very small proportion of SSO activities (Leake, p. 6). Expertise in areas including Political Affairs, General Affairs and Economics was now required, but the pool of recruits with such qualifications was insufficient to the end of 1941 (SEATIC, n.d., p. 16). From the beginning of 1942, SSO personnel began to be substituted by specialist civilians known as *Bunkan*, essentially educated civilians in a particular field (SEATIC, n.d., p. 17).

Between July 1942 and early 1943 an increasing number of IJA SSO functions were delegated to autonomous and provincial Governments. Both espionage and counter-espionage were separated from the newly formed *Renraku Bu* (Liaison Department) and centralised in HQ, Nanking under the title *Tokushu Kikan* (official name unknown) (MacArthur, p. 16). The IJA *Renraku Bu* was, officially, now limited to liaison with the puppet regime, economics and propaganda, with branches throughout all centres of the Nanking Government (MacArthur, p. 16). Irrespective of how delineation was now drawn, Japanese retained all key roles, and the *Renraku Bu*, through its commercial control, exercised "just as much power as its predecessors" (MacArthur, p. 16).

Functions once held by its predecessors in relation to operations of the puppet Government were absorbed into the *Renraku Bu* (in Shanghai this department operated under the title *Rikugun Bu* (Army Department)). The *Renraku Bu* differed from previous change in command structure in that its branches now answered directly to IJA HQ in its respective area (Leake, p. 8). The section of the IJA SSO concerned with espionage and counter-espionage, *Tokushu Kikan* and its detachments, remained responsible to Supreme HQ Nanking (Leake, p. 8).

CONCLUSION

Within China the Imperial Japanese Army did not from the onset of hostilities maintain a fully coordinated intelligence system with direct information relay to Imperial Headquarters in Tokyo. Within military intelligence, but across the intelligence apparatus as a whole, little direction was received from Imperial General Headquarters as to what was of importance, leading to rather subjective information collection by both local commands and staff involved.

Repetition and overlap of duties by different intelligence organisations was commonplace. IJA Special Service organisations, initially strategic intelligence units, had ostensibly been under command of the Second Department, IJA General Staff. In practice, Japanese intelligence units operated independently within their area of operations, decentralising further throughout the course of the conflict. Efficacy of Japan’s intelligence apparatus was further hampered by a lack of coordinated and specialised training of its Intelligence Staff. With the establishment of puppet regimes in China, primary focus in intelligence collection by Special Service units shifted largely from tactical to political concerns.

Continuous reorganisation and decentralisation of Japan’s intelligence apparatus, plus reactive rather than proactive practices in response to circumstances on the ground in China, lead to inefficiency for the duration of the conflict. Despite its prolific presence on the ground, a lack of cohesion over time circumvented the potential of Japan’s intelligence apparatus. Were the conflict lengthened lessons learnt and subsequent modifications to the intelligence apparatus by the Japanese may well have overcome its short-term inefficiencies, leading to a more efficient and effectual intelligence apparatus.

REFERENCES

Berkshire Miller, J. (29 January 2014). How Will Japan’s New NSC Work? *The Diplomat*. Retrieved from http://thediplomat.com/2014/01/how-will-japans-new-nsc-work/

Byse, C. M. (1945). *Memorandum*, 21 July 1945, Puppet Intelligence Study, Box No. 10, Japanese Activities in the Far East – China, Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of

Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

Dorling, P. (2011). WikiLeaks unveils Japanese spy agency. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/technology/technology-news/wikileaks-unveils-japanese-spy-agency-20110220-1b17a.html

Gorman, D. C. (1945a). *Memorandum for Captain Wallace S. Wharton*, 18 June 1945, Folder Okino, Mateo Capt. I.J.N., Box No. 4, Individuals (A to Z) and Capt. Matao Okino (I.J.N.), Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

Gorman, D.C. (1945b). *Memorandum for Lieutenant Commander Peter Belin,* 17 July 1945, Folder Okino, Mateo Capt. I.J.N., Box No. 4, Individuals (A to Z) and Capt. Matao Okino (I.J.N.), Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

Jowett, P.S. (2004). *Rays of the Rising Sun: Armed Forces of Japan's Asian Allies 1931-45, Vol. 1, China and Manchukuo*. Solihull: Helion & Company Ltd.

Kotani, K., *Japanese Intelligence in World War II* (Oxford: Osprey, 2009) pp. 44-45

Leake, E.W.R. (1944). *Interrogation of Japanese Naval Prisoner of War, Captain Okino, Matao,* 19 October 1944, Folder Okino, Mateo Capt. I.J.N., Box No. 4, Individuals (A to Z) and Capt. Matao Okino (I.J.N.), Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

MacArthur, D. (1944). *A Study on Japanese Espionage,* 31 December 1944, Folder Japanese Intel. Organs & Counter-Intel. Organs, Box No. 8, Japanese Activities in the Far East - Intelligence & Counterintelligence Organisations, Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

Mercado, S. (2002). *The Shadow Warriors of Nakano*. Washington D.C.: Brassey's, Inc.

Military Intelligence Service WDGS. (1945). *The Japanese Intelligence System*, 4 September 1945, Container #78, Entry# A1 9002: Studies on Cryptology, 1917-1977, SRH 245-SRH 255, Records of the National Security Agency/Central Security Service, Record Group 457, National Archives at College Park, College Park, MD.

Office of Strategic Services, Research and Analysis Branch. (1943). *The Guerilla Front in North China*, 21 May 1943, Folder China (1943), Box No. 10, Japanese Activities in the Far East - China, Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

"Peace Preservation – Pacification – Distinction between". (n.d.). Puppet Intelligence Study, Box No. 10, Japanese Activities in the Far East – China, Oriental Desk (Op 16-B-7-0), 1936-46, Office of Naval Intelligence, Sabotage, Espionage, Counterespionage Section (SEC), Records of the Office of the Chief of Naval Operations, Record Group 38, National Archives at College Park, College Park, MD.

South-East Asian Translation and Interrogation Centre. (n.d.). *General Ground Bulletin No. 133*, Records of the Office of Strategic Services, 1940- 1947, Record Group 226, Entry 210, Box 244, National Archives at College Park, College Park, MD.

South-East Asian Interrogation and Translation Centre. (1944). *Interrogation of Captain Okino Matao, I.J.N.*, S.E.A.T.I.C. Consolidated Interrogation Report, No. 75, 9 November 1944, Records of the Office of Strategic Services, 1940- 1947, Record Group 226, Entry 210, Box 244, National Archives at College Park, College Park, MD.

South-East Asian Interrogation and Translation Centre. (1946). *Special Interrogation of Colonel Hayashi Hidezumi of the Japanese Military Police*, 24 August 1946, The National Archives (TNA): Public Record Office (PRO), WO 208/3916.

Strategic Services Unit. (1946). *Japanese Intelligence Organisations in China (WWII)* (2 of 2), 4 June 1946, Box No. 5, Japanese Intelligence Organisations in China (WWII) to Nazis in South America, Vol. 3, First Release of Subject Files Under the Nazi War Crimes and Japanese

Imperial Disclosure Acts, 1934-2002, Records of the Central Intelligence Agency, Record Group 263, National Archives at College Park, College Park, MD, Section II.

United States Strategic Bombing Survey. (1945). *Interrogation of Lieutenant-General Arisue Seizo, I.J.A.*, Interrogation No. 238, Reports of Interrogations, Hoover Institution Archives.

ABOUT THE AUTHOR

Simon Hall is a PhD student at the University of Adelaide, Australia. He holds the degrees of Bachelor of International Studies and Master of Arts (International Studies). His doctoral research centers on Japanese intelligence from the First Sino-Japanese War to the end of Second World War. His broader research interests lay in the subject areas of intelligence studies, international relations, and strategic studies as they pertain to North and East Asia.

- o O o –

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.

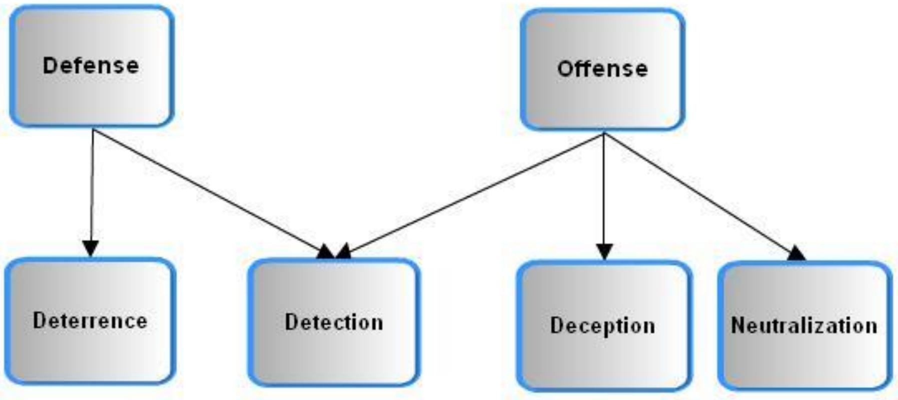


Figure 1 — A logical model of counterintelligence

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 -

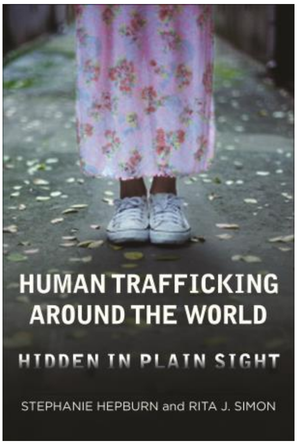
Book Review

Human Trafficking Around the World: Hidden in Plain Sight

by Stephanie Hepburn and Rita J. Simon

Columbia University Press, New York
2013, 525 pages
ISBN-13: 978-0-231-16145-9 (paper)
ISBN-13: 978-0-231-16144-2 (cloth)

Reviewed by Dr Susan Robinson



Human trafficking is the illegal trade in buying, selling and transporting of human beings for the purpose of exploiting them as slaves. The most common forms of modern day slavery involve commercial sexual exploitation and labour servitude. This book reports on the findings of an unprecedented, comprehensive study of sex trafficking across twenty four countries: Australia, Brazil, Canada, China, Chile, Colombia, France, Germany, India, Iran, Iraq, Israel, Italy, Japan, Mexico, Niger, Poland, Russia, South Africa, Syria, Thailand, The United Arab Emirates, The United Kingdom, and the United States. The authors are journalist Stephanie Hepburn and justice scholar Rita Simon who delve into the statistics and personally acquired qualitative data which they obtained from intimate personal interviews with victims, perpetrators and lobbyists to shed light on the illegal human trafficking practices known to exist in these countries.

The authors confront the reader with the harsh reality of human trafficking; the victims of which include men, women and children. When considering these crimes in the context of social inequality and powerlessness, as the authors do, it is no surprise that while men are sometimes victims, the majority are women and children. Hepburn and Simon point out that more than 12.3 million people are affected by this crime worldwide that reaps a profit of around $44.3 billion annually. They report that 43 percent of victims are trafficked for commercial sexual slavery, 32 percent for forced labour and 25 percent for a mixture of both. Between 40 and 50% of trafficked victims are children with 98% of victims trafficked for sexual exploitation are women and children.

The authors tell the background story that gives context to these figures and demonstrates that these victims are often forced into slavery in their own country or may be transported across international borders to be sold into slavery in other countries. Victims are taken by deception, coercion or force and once in the control of the trafficking ring they are controlled by severe deprivation, isolation, abuse and intimidation. Exorbitant fees are placed on such things as recruitment, travel, accommodation and food even when the victim is non-consenting or under the age of consent. They are commonly held in debt bondage and forced to repay these fees while being subjected to multiple other abuses that bind them psychologically to their captors.

Human trafficking is analysed from a global perspective and the complex nature of sexual slavery and forced labour, which are predominantly hidden practices, is highlighted. In addition the authors focus on anti-trafficking efforts and critique the current efforts to impede this form of organised crime. They discuss the obstacles and challenges posed by economic, political, geographical and social impediments and civil unrest.

One of the major underlying problems associated with the continuation of this crime is inequality and gender disparity. By tackling the context in which human trafficking is able to manifest and flourish, Hepburn and Simon tackle the difficult issues of power and control in the societies involved. What is astonishing about this problem is the way in which the immigration laws of several countries provide the conditions for human trafficking to occur. For instance, the work visa system that ties people to a particular employer actually works in the favour of traffickers who withhold passports and provide them to the authorities should a victim dare to try to "escape" or leave to go to another employer. Ironically, when victims are finally liberated it is they, rather than the traffickers who are prosecuted for breaches of visa conditions and crimes such as prostitution. Their status as a victim is often lost within the enforcement of border laws. In addition, they are often not included as trafficking victims in official statistics.

Human Trafficking Around the World: Hidden in Plain Sight is a very readable book that utilises real case examples to illustrate the abuses and back stories of the victims involved in this terrible practice. The authors deal sensitively but assertively with the issue, including the status and treatment of women and children in several of the countries of origin, which they argue allows such crimes to occur in the first place, and certainly allows them to continue.

The book provides numerous insights to help the reader understand the awful injustice of what has become a worldwide trend to blame the victim and to further victimise people liberated from trafficking by prosecuting and deporting them. But there is a glimmer of light on the horizon—Hepburn and Simon highlight the global effort underway to provide safe houses for victims and to change legislation and practices so that victims are no longer blamed and instead perpetrators are made accountable. This book is recommended reading for scholars and students interested in the topic.

ABOUT THE REVIEWER

Dr Susan Robinson is a criminologist, lecturer and researcher with the Charles Sturt University, School of Policing Studies. She has extensive experience working as a practitioner and manager in the public service in South Australia, the Australian Capital Territory, and the United Kingdom in the areas of child protection, juvenile justice and adult corrections. She holds a PhD in sociology (criminology) from Flinders University in South Australia and an Honors Degree in Social Work. Her research interests include: women in policing; female offenders; juvenile offenders; crimes against children; child protection; correctional services; custody; and police leadership.

- o O o -

Call for Papers

Salus Journal is a peer-reviewed open access e-journal for the publication of law enforcement and security agencies, as well as research findings and discussion papers regarding emergency management and public safety. *Salus Journal* seeks to contribute to practice by inspiring discussion through an interdisciplinary approach.

We invite submissions of articles of between 3,000 and 6,000 words for double-blind peer-review that:

- focus on issues that have an impact on criminal justice, law enforcement, national security, or emergency management;
- engage with contemporary topical practice issues; or
- add to the understanding of complex management conundrums.

Submissions can use either qualitative or quantitative approaches, including studies that employ the use of exploratory or holistic approaches. The journal also accepts discussion papers, critical essays, and analytical papers as long as a clear position is stated and the argument is grounded in sound practice, or the subject literature.

Book Reviews

Salus Journal also accepts book reviews that do not exceed 750 words. Reviews should go beyond the descriptive account of the book's contents. Reviews that discuss the implications of the book's message for practice or policy are sought for inclusion in future editions. Books can be either newly published, or vintage editions where the book's thesis can be applied to a current situation or in an emerging context.

Submission Process

Visit the journal's submissions page to see a copy of the author guidelines and a summary of the refereeing process:

www.salusjournal.com/submissions