Is Military Counter Intelligence (CI) Living Up to its Name?

By: Major Robin Nickerson

Major Nickerson transferred from the Military Police Branch to the Intelligence Branch in 2006 and deployed to the International Security Assistance Force Regional Command (South) Headquarters in Afghanistan, in 2007. Later that year, he returned to Canada to take up duties as the J2 Capabilities at Canadian Expeditionary Forces Command Headquarters, in Ottawa. In 2009, he was posted to the Canadian Forces Intelligence Liaison Office at Whitehall, London, UK, where he was formally trained as a defence analyst and British Defence Attaché, as well as completing the Kings' College London's Intelligence Study Programme sponsored by the Foreign and Commonwealth Office. He was also an analytical embed with the UK's Permanent Joint Headquarters during the Libya Crisis. In late 2012, he returned to Canada as a Support Officer for Canadian Defence Attachés, and later completed a seven months tour at Amman, Jordan. He is presently employed at National Defence Headquarters in Ottawa, Ontario.

Introduction

Academically and historically, the trend points to a weakening of military Counter Intelligence (CI) activity due to North Atlantic Treaty Doctrine. The NATO definition of *military* CI for contributing nations is surprisingly misaligned and skewed to meet what traditionally has been an activity that is designed to assess and exploit foreign intelligence opponents. From the outset, the NATO definition intertwines finite CI resources in the banners of massively complex strategies on terrorism and criminal activity while sabotage, likely classed as a criminal event today, and subversion extend well past what would objectively be described as military CI *in toto*. This NATO CI definition is formally embraced by contributing nations, impacting on what is accepted as military CI activity along with how finite resources are prioritized and employed.

CI is both an analytical process and an operational multi-disciplinary function designed to corrupt the *secret* intelligence and intelligence capabilities of an opponent, forming an intelligence practitioner versus intelligence practitioner joust in the shadows.[1]

As explained by Mr. Angleton (former head of the United States (US) Army CI in 1947) at the Church Committee (examining Government operations with respect to intelligence activities in 1975), "CI is the activity of gathering intelligence so as to confront, penetrate and frustrate other intelligence agencies, and in certain instances…[deal] with their CI."[2]

From an academic perspective, CI is a foray into the murky world of deception activities with the ultimate goal of spoiling foreign intelligence (including foreign military intelligence) processes. In peacetime, the military CI environment must remain consistent with this aim to hone highly specialized skills, experience, international relations amongst friendly intelligence organizations, and blended activities with domestic security organizations to permit an informed and agile military CI organization to react before, during and after a military deployment. Historically, military CI activities will be briefly examined from the beginning of the First World War through to the end of the Cold War. However, since the fall of the Iron Curtain, military CI has struggled to achieve a coherent focus on foreign intelligence.

This paper will explore CI from both academic and historical perspectives as an underlay to contrast the de-enrichment of military CI focus and capability today in the face of widening and increasing levels of foreign intelligence activity. From this examination, key elements of course correction for military CI will be identified.

Three Interactive, Inter-Dependent Pillars – The Academic Foundation for CI

CI takes the form of a supporting pillar to the main intelligence and security contests in order to keep our secret intelligence, secret.[3] But how do these concepts interact and mutually support each other? Firstly, *secret* intelligence is acquired by discretely or clandestinely collecting and processing protected information *without knowledge* of the opponent. This is a key concept that differentiates it from the intelligence-like reporting in the mass media by investigative journalists; both intelligence personnel and journalists attempt to piece together

knowledge which is not readily available.[4] The intelligence opponent, however, actively and passively resists being collected upon. Sophisticated intelligence opponents will also attempt to engage their CI effort in offensive and defensive roles against our own collection activities. In response, CI permits the advanced applications of detecting, assessing and manipulating foreign collection efforts and capabilities to ultimately safeguard our secret intelligence.

Secondly, a security program establishes standards to keep information away from those without a need to know.[5] Weakness in a sustainable, comprehensive, reactive and enforceable security programme make secret intelligence increasingly vulnerable to acquisition by an opponent (even the public) through poor physical controls. A lax security environment can also harbour and conceal disgruntled employees who can be recruited by foreign intelligence services as agents, or at least permit de-briefing opportunities to foreign intelligence operatives to the point of unearthing semi-precious nuggets of intelligence value. Instances of spectacular cases of espionage within an intelligence organization can precipitate devastating ramifications as represented in the wake of the spy cases of Ames (a Russian Spy in the US CIA's CI Branch) and Philby (a Russian Spy in the British Secret Intelligence Service CI Branch). Episodes like these not only compromised secret intelligence but also caused the apprehension and execution of friendly agents whose identities were revealed to Russian CI.[6]

Poor security will invariably cause information to hemorrhage to those without a need to know, through a combination of inadequate security safeguards and weak operational security practices by employees. Breaches of security immediately cause the critical elements of *secret* intelligence to evaporate as an opponent reacts to the intelligence collected and assessed against them. Consequently, it is in the advanced resolution of unusual incidents pertaining to traditional physical, personnel, communications and cyber security that only the closest engagement and collaboration will enable CI pursuit. Such cross-cuing is vital for the detection and manipulation of low profile foreign intelligence signatures probing the security appendages of the State and military alike.

For CI, according to Michael Herman, "[it] is used to convey the multi-disciplinary effort to penetrate the many different disciplines of the adversary."[7] CI also partially answers how great the danger from the possibility of deception by an opponent is.[8] In these two instances, it only makes sense that intelligence should be the expert on foreign intelligence organizations and how to deceive them.[9] As a supporting feature to secret intelligence and security, CI becomes an important brace in terms of offensive and defensive initiatives to strengthen both.

Overall, the state of effectiveness and the mutually supporting features of these inter-dependent pillars reinforce an intelligence organization's ability to safeguard, acquire, produce and disseminate *secret* intelligence without an opponent's knowledge. From another perspective, the actual CI sub-contest aspires to silently assess and penetrate the opponent's security defences to spoil opposition intelligence; thereby, safeguarding our own secret intelligence and reinforcing our protection against a grievous security breach.[10]

CI and Deception

On deception, James J. Angleton (CIA Director for CI 1954-75) opined that intelligence services establishing corrupted channels that the victim relies on for its secret information via false defectors, double agents, diplomatic chatter, etc. are the key.[11] The deceiver also uses a second network of covert communication lines to get a fix on the victim's reactions to these poisoned messages. Without such a feedback loop, the deceiver cannot be sure if he's tricking the opposition or not.[12] To accomplish these conditions for deception, military CI has to integrate into the mainstream CI arena. Military deception operations, especially under today's rapid deployment scenarios, oblige military CI integration within the wider mandates of civilian security and intelligence services. Military CI cannot commence from scratch when the first "boots" hit the ground. Lines of communication and verification of deception must be pre-established as part of larger the intelligence community's activities. These undertakings against likely opponents are not short term but are rather medium to long-term commitments, with civilian agencies and services. It is at this specific junction that a major turning point for military CI exists in order to prepare conditions for deception as part of future military planning contingencies, requirements and strategy.

Historical Rooting for Military CI: World War One to the Cold War

In January 1909, the Committee of Imperial Defence (CID) was formed in London, in reaction to the growing fear of German spies assisting with the preparation of an invasion of England, along with the rising subversive threat posed by Communism. From its outset, an inter-Departmental framework was created as the CID brought together police, postal and custom services to identify aliens suspected of spying. The CID created the Secret Service Bureau, which would later evolve into MI5 by January 1916.[13]

By the late 1930s, German Intelligence (the Abwehr) once again posed a threat to British national security on the eve of World War Two. MI5 efforts were to result in an unprecedented and clear CI victory: the wholesale control of the Abwehr agent network in England by striking what was dubbed the 'double-cross system'. The double-cross system relied upon Human Intelligence (HUMINT) tips and, more significantly, de-coded German ciphers to identify, arrest, co-opt and run double agents against an unsuspecting Abwehr. MI5 leapt from the unknown, concerning Abwehr agents' activities in England, to the complete control of the entire network by 1940.[14] Against this backdrop of spectacular success, ironically, the British agent network in Holland was completely neutralized at the outbreak of the Second World War due to underestimation of the risks of penetration by the very same Abwehr opponent.[15]

At its time of choosing, MI5 began to introduce false information to confuse and misinform the Abwehr. Under the Treachery Act, several Abwehr agents were executed as spies after their arrest, while others were co-opted into their new double agent role as an alternative to escape certain death. With Abwehr double agents (now under complete MI5 control) and reporting reasonably accurate air raid damage information during the Blitz, confidence and credibility were established in their reporting from the perspectives of Abwehr handlers and analysts alike. At this point, fabricated information was deliberately introduced to the corrupted agents' reporting stream. In this specific instance, the state of British preparations against German invasion was reported to be stronger than it actually was.[16] Both the Secret Intelligence Service and MI5 had a near complete understanding of the Abwehr's order of battle (ORBAT) by 1943.[17] With this understanding and insight, the foundation was set for CI operations to support Operation Overlord's deception plan for the Allied invasion of Normandy in June 1944 via double-agent reporting in concert with the creation of dummy installations/landing crafts, diversion activities, radio deception, *inter alia*.[18]

In retrospect, MI5 objectives during the war described a genuine CI effort. These MI5 goals are applicable today as they were back then, "… to keep our agents … well fed with accurate information so as to not lose the confidence of the enemy to control as many of the agents in this country … [so that] they need not send anymore whose arrival we might not be aware, by careful maneuvering of these agents and careful study of the questions, to mislead the enemy on a big scale at the appropriate moment."[19]

During the Cold War, western CI organizations squared off against a massive, sophisticated Soviet Intelligence enterprise. In the US, the notion of integrating the Department of Defense's (DoD) military CI communities into the larger national picture set the stage for closer cooperation – a key theme to which we'll return later. Under the Carter Administration, US military CI activities were fused into the national CI design vis-à-vis the National Security Council's Special Coordinating Committee overseeing all domestic CI matters. This move was in reaction to the omnipresent threats to the DoD by foreign intelligence attempts to penetrate civil research, engineering and procurement projects. Individual Service jurisdictions could not effectively deal with this threat working independently. As an example of CI performance within this new national level framework, the US Army CI effort studied foreign intelligence modus operandi and conducted Multi-Disciplinary CI (MDCI) assessments to acquire knowledge and understanding of the Soviet Block's intelligence effort, directly feeding Army CI investigations and operations. Signals Intelligence (SIGINT), Imagery Intelligence (IMINT) and HUMINT represented the basic components for their MDCI process. MDCI products directly linked into overarching intelligence assessments, which also provided the basis for counter-measures and improvements to security against foreign intelligence collection. At its apex of success, Army CI had approximately 100 Soviet Block agents under its control and had indeed impinged upon the Soviet Block's HUMINT

collection effort. The US Air Force and US Navy did not use CI specialists and fell short of achieving the same measures of effectiveness, primarily due to slow acceptance of the MCDI concept and reliance on general intelligence analysts for CI work.[20]

The US Army's CI experience during the Cold War serves as a model for today's military CI practitioners. The DoD's connection to the mainstream CI effort with civilian agencies; the Army's use of the MDCI assessment concept; use of CI specialists; actually conducting double agent operations; and sustained focus on the Soviet Block intelligence apparatus culminated into a tangible and effective CI programme. However, from these historical CI best practices, today's NATO CI effort is not so clearly focused or applied.

The Military CI Definition – The Problem

NATO introduces a series of problematic terms, which directly weaken and potentially confuse military CI by definition:

> Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services and organizations *or by individuals engaged in* espionage, *sabotage, subversion or terrorism* [emphasis added].[21]

The identification and counteraction of activities associated with sabotage, subversion and terrorism (organized crime is also included)[22] serve to clutter the actual military CI aim. This communal definition is important since it is accepted by all NATO representatives, thereby automatically linking a keystone reference into national military CI doctrines. Looking more critically at the problem terminology, sabotage has become an outdated term, in that, traditional Intelligence gathers on this form of warfare. In peacetime, sabotage is also more like a criminal act for law enforcement intervention and intelligence collection purposes than military CI. Subversion is an equally troublesome piece since normal security clearance activities should be addressing an employee's loyalty and reliability as part of a national security clearance investigation process. Terrorism is a global matter for the larger intelligence and policing communities to detect and counter. While military CI may have limited input into this area, such as a terrorist network attempting to collect information on an armed forces installation for attack purposes, it is by no means a key contributor to the massive array of intelligence resources assigned to this mission domestically and internationally. Finally, criminal activity in the NATO CI definition completely crosses a clear line of responsibility (and focus) into the policing domain. Policing conforms to a specific legal framework along with collection requirements which do not work for military CI (e.g. disclosure of evidence and collection methods, public scrutiny of due process, the disclosure of source identities in court, etc).[23] While liaison in the policing community is arguably a supporting CI activity, it does not belong in an over-arching military CI definition.

The corollary of what can be described as 'bolt-on' terms to the NATO CI definition creates an atmosphere whereby redundant and superfluous activity can exist, perhaps avoiding the real and demanding task of actually tackling foreign military intelligence in peace and war - a far more daunting, sensitive and exclusive endeavour. In summary, the definition of NATO CI introduces too many threat categories, impairing military CI's unity of effort and focus.

MDCI Concept –A First Corrective Step Forward

The first order of business on the road to re-shaping military CI today is establishing a MDCI assessment construct to determine the efficacy of the adversary's intelligence collection capabilities and activities.[24] In a military context, MDCI analysis needs to reach widely amongst existing intelligence staffs and organizations to identify and understand a foreign military's intelligence function as well as the best ways to impair it. This involves exploring and pre-determining an opponent's SIGINT, IMINT, Cyber Intelligence, and HUMINT capabilities with a view to degrading the targeted intelligence enterprise during all phases of a military deployment. It is here that guided military CI activities are best accomplished by a dedicated CI analyst at the center of a MDCI process.[25] Harnessing existing technical, military and civilian agencies to provide their expertise is essential to build military CI awareness and comprehension as well as identifying areas for further CI work to fill gaps. As a process, the MDCI concept is neither widely accepted nor used by the NATO military CI community and stands as a vital missing component to a contemporary CI architecture.

Military CI – The Next Changes in Practice

In Gestalt psychology terms, Intelligence and CI can be viewed as two differing 'mind sets': where an image of an opponent is seen in one of two ways, but not both ways simultaneously.[26] Intelligence will focus on how to visualize an opposing force, whereas military CI will focus on how the opponent is visualizing our own forces. Not fitting into this clinical context, military CI (or more specifically Counter-HUMINT [C-HUMINT]) is sometimes grouped in a team-like organization with HUMINT collection activity.[27] As we've discussed, *supra*, CI assessment and collection has to be fundamentally multi-disciplinary as a process. As a result, the blending of CI and HUMINT into a team concept tends to promote confusion and tension as both mandates (and *foci*) compete for limited time and resources to achieve different information requirements. Thus, there is no logical fit for CI directly linked to a HUMINT grouping within the overarching intelligence organization.[28] In functional terms, CI requires a nesting within a central intelligence framework, which can empower it to reach widely amongst assessment and collection communities across the entire spectrum of military and civilian intelligence operations; strong international ties with close and like-minded partners are also essential.

CI involvement in mainstream intelligence collection activities, particularly in support of military operations, should increase the chances of detecting hostile CI influence or at least reduce the risk of operational level deception. This is a challenging task as foreign intelligence activities are not readily detectable, and the assembly of fragmentary evidence is not a straightforward exercise. For example, even in a low-technological environment, the threat of deception or misinformation can be an easy trap to fall into as experienced by the US during the early days of the Vietnam conflict. Prior to 1968, South Vietnamese intelligence and police services were heavily infiltrated by Vietcong agents who provided inadequate and sometimes dangerous information.[29] Another example of foreign intelligence manipulation was highlighted by Iran in the 1980s and 1990s when covert action was used to reinforce deceptive messaging to the US. The Iranians manufactured the existence of a notional group of Iranian moderates in Tehran. Iranian manipulation led the US to believe that these moderates could be empowered via arms sales, economic assistance, and by pressuring Israel on behalf of Palestinians and Lebanese Shiites.[30] Simply put, extending from these examples, Military CI has no other option but to be in a position to understand the foreign intelligence dynamic and cannot be expected to rapidly acquire knowledge, understanding and expertise to support short notice military ventures abroad.

Military CI must partner and work together - where mandates permit - with their larger national security and foreign intelligence agencies to be credible and responsive. As long as mandates are respected, especially in areas of primary control and accountability of the CI activity to hand, conditions exist for military CI participation under the lead of a civilian Agency (or Service). Serving to illuminate this need, the UK's Defence Concepts and Doctrinal Centre articulates that, 'success in future conflict, especially against adaptive and agile adversaries, *will* require a shift away from kinetic to influence activity, underpinned by a greater understanding of the enemy.'[31] This statement points, in part, at a MDCI understanding of both foreign and foreign military intelligence capabilities and intent as well as opening the door to their manipulation in order to assist in achieving this 'influence'. Neither foreign nor foreign military intelligence can be understood (and manipulated) in the time constraints required to support a short notice military force deployment. Therefore, working closely with civilian security and intelligence counterparts is logical to enable military CI responsiveness as part of the 'influence' metric for a military force.

Of special interest to a military CI function are cyber-espionage, leveraging SIGINT, and countering foreign (and hostile) HUMINT collection on deployments. In the Twenty-First Century's post-modern intelligence world, web-based networks are the richest treasure ever for espionage and a grave potential vulnerability.[32] As with any CI related activity, the basics of detection, intervention, assessment, and manipulation of foreign intelligence activities remains extant in cyberspace. Military CI must reach out on collaborative and assessment fronts with the cyber-security community for CI target acquisition purposes, remembering that what foreign intelligence is seeking forms a major part of defining a military CI analyst's area of interest as well as the CI operator's task.

Exactly the same military CI considerations are applicable to integrate and collaborate with SIGINT activities. Finally, C-HUMINT activities on military deployments must learn and adapt to how an adversary acquires information from the indigenous population, exploiting the seam of poorly vetted local personnel who work inside and outside military installations as well as general observers monitoring friendly force activities from public areas. As an illustration, the attack on a German convoy in June 2003 at Kabul, Afghanistan pointed to the successful collection effort by ISAF locally hired employees who passed targeting information to the Taliban on ISAF convoy movements.[33] Military CI needs to be fully engaged to identify and counter the non-technical acquisition of information within a mission area which can form the basis of workable intelligence for an opponent, compromising the basic elements of surprise and force protection. In other words, military CI must be empowered to resurrect a 'double-cross system' for the tactical needs of a deployed force.

Military CI is responsible to understand the activities of foreign and foreign military intelligence in peacetime. This extends to assessing (and keeping current) a foreign military's intelligence ORBAT as well as how a foreign military force will use its intelligence ORBAT to 'sense' our own military deployment. Proportionality of CI effort against an adversary must also be calculated carefully; the weight of effort towards an unsophisticated State may not lead to the same level of CI effort against a cutting edge Foreign Intelligence Service or military Intelligence organization with vast arrays of covert collection means and options.[34] With these aforementioned considerations in mind, military CI needs to re-position itself and initiate difficult changes in its practices to actually achieve its stated mission: countering foreign military intelligence.

Conclusion

Military CI needs to objectively respond to the challenge of re-orientating its activities to actually concentrate on identifying and counteracting threats to security posed by hostile intelligence services and organizations. The pruning of other divergent, thematic branches connected to the NATO CI definition (eg. *sabotage, subversion, terrorism, criminal activity)* is necessary to concentrate limited resources on a series of advanced foreign intelligence initiatives. The cobblestones of an inclusive relationship with civilian security and intelligence organizations need to be better established to empower military CI to re-discover expertise, experience and deeper understanding of foreign military intelligence organizations during peacetime; thereby, pre-positioning it for action during a crisis. As a basic underpinning to any military involvement with civilian agencies, mandate primacy remains an important constraint, but closer collaboration can usher in new (and advanced) levels of multi-lateral engagement, access, unity of effort, and success. Military CI is further obliged to generate leadership and expertise to drive the CI process as a deliberate and sustained intelligence activity. Ultimately, as widely articulated academically and historically, military CI has to deliver an interpretation of a foreign military intelligence enterprise and be prepared to launch activities to deceive it. Without a clear military CI definition and process; closer integration with civilian agencies in pursuit of military related CI activities; and widespread engagement across a MDCI frontage (enabling *action* to foil a military intelligence opponent), military CI simply cannot live up to its name.

Endnotes:

1. Mark Lowenthal, *Intelligence from Secrets to Policy* (Washington, DC: Congressional Quarterly Press, 2000), 98.
2. M. Holzman, *The CIA and the Craft of Counterintelligence* (Amherst, Massachusetts: University of Massachusetts Press, 2008), 3.
3. Michael Herman, *Intelligence Power in Peace and War*, 14th ed. (New York: Cambridge University Press, 2011), 178.
4. R. Dover and M. Goodman M, "Spooks and hacks: blood brothers", in *British Journalism Review*, Vol. 20, No.4 (London: B.J.R. Publishing, December 2009): 3.
5. Abram N. Shulsky and Gary J. Schmidtt, Eds. (2002), *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington DC: Potomac Books Inc., 2002), 9.
6. Herman, 179-180.

7. *Ibid*., 528. Also, Roy Godson, *Comparing Foreign Intelligence: The US, the USSR, The UK and the Third World*, (Washington, DC: International Defence Publishes, Inc., 1988), 32.
9. Herman, 55.
10. *Ibid*., 179.
11. E. Epstein, *Deception: The Invisible War between the KGB and the CIA* (New York: Simon and Shuster, 1989), 106.
12. Ibid., 106-107.
13. F. H. Hinsley and C.A.G. Simkins, *British Intelligence in the Second World War, Vol. 4, Security and Counter-Intelligence* (London: Her Majesty Stationery Office, 1990), 3- 4.
14. *Ibid*., 87.
15. Herman, 178.
16. Hinsley and Simkins, 97-100.
17. *Ibid*., 159.
18. *Ibid*., 243-242.
19. *Ibid*., 98.
20. Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (New Jersey: Transactions Publications, 2001), 115-116.
21. North Atlantic Treaty Organization, *Allied Joint Publication (AJP) 2 (2003),* "Allied Joint Intelligence, Counter Intelligence and Security Doctrine" (Brussels: NATO Presses, 2003), 2-1-1
22. *Ibid*., 2-1-7 to 2-1-8.
23. Godson (2001), xxvii – xxix.
24. Shulsky and Schmitt, 114.
25. Godson (2001), 201.
26. Epstein E (1989), 102.
27. United States Army, *ST 2-22.7 (FM 34-7-1) (2002), Tactical Human Intelligence and Counterintelligence Operations* (Fort Huachuca, Arizona: US Army Intelligence Center), at http://www.scribd/doc/9688731/ST-2227-Tactical-Human-Intelligence-and-Counterintelligence-Operations.
28. Herman, 174.
29. Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books, 1987), 172-173.
30. Godson (2001), 235.
31. United Kingdom Ministry of Defence (2010), *Strategic Trends Programme: Future Character of Conflict* (Schrivenham: Development, Concepts and Doctrine Centre, 2010), at http://www.mod.uk/Defence Internet/MicroSite/DCDC/Our Publications/concepts/FutureCharacterOfConflict.htm, 17.
32. Peter Jackson and L.V. Scott, Eds., *Understanding Intelligence in the Twenty-First Century: Journeys in the Shadows* (London: Routledge, 2004),
33. Shulsky and Schmidtt, 9.