COUNTERINTELLIGENCE AND FIRST LINES OF DEFENSE IN AN AGE OF HYBRID WARFARE

Date: November 16, 2023

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 16, 2023, Prof. Philip Davies presented *Counterintelligence and First Lines of Defense in an Age of Hybrid Warfare* for this year's West Coast Security Conference. The key points discussed were the relationship between Full Spectrum Conflict/Hybrid Warfare (FSC/HW) activities and counterintelligence (CI), especially with reference to the role of Foreign Intelligence Services (FIS) in delivering sub-threshold/grey zone operations, inconsistencies in current NATO counterintelligence thinking and professional practice, and the consequent difficulty adapting that CI theory and practice to meeting the CI aspects of the FSC/HW threat.

NATURE OF DISCUSSION

Prof. Davies provided insight into current problems in allied doctrine for counterintelligence and the lynchpin role of FIS role in delivering sub-threshold/grey zone components of FSC/HW that fall within the traditional CI mandates for counter-espionage, counter-subversion and counter-sabotage. There is also, however, a need to bring counterintelligence doctrine up to date so that it can inform countermeasures against adversary Intelligence, Surveillance, and Reconnaissance (ISR) activities in support of FSC/HW sub-threshold irregular warfare. Currently FSW/HW can slip into fracture lines in Western CI doctrine and methods that are purely focused on human threat vectors as a result of two decades focusing almost exclusively on counter-terrorism (CT) and counter-insurgency (COIN), and is largely unprepared for the multi-disciplinary intelligence threat presented by state-level strategic peers and tactics which those states use to provide support and assistance to their proxies and allies.

BACKGROUND

The traditional scope of counterintelligence encompasses a set of missions that are necessary to conceptualize and define in order to prevent mission creep when addressing the modern phenomenon of FSC. The core objective of the traditional counterintelligence mandate is, in the words of a 1946 British War Office CI doctrine, 'to destroy the effectiveness of the enemy's intelligence service'. Traditionally this entailed detecting and countering acts of sabotage, espionage, and subversion. Since the 1960s the notion of countersubversion has been a troubled and controversial one. Counter-subversion, also known first half of the 20th Century as Fifth Column activity, is fraught with political debate over the boundaries between nominally 'subversive' activity as legitimate dissent and, equally, legitimate engagement with foreign states/institutions in the context of civil society, as distinct from hostile influence and control. The term has been largely removed from the intelligence lexicon in the civilian domain but has remained in military doctrine, most likely because of the ease in framing it as a threat within discipline and regulations of the defense environment compared to the civilian. Adjoining the term to espionage as argued by, for example, the Canadian Security Intelligence Review Committee (SIRC) in the 1980s is unconvincing for two reasons. The first is that, functionally, espionage is about pulling information *in* to an agency while subversion is about pushing information *out* in order to influence and disrupt. The second is that espionage is easily identified as a criminal offence under various official secrets legislation while a great deal of what amounts to subversive activity is not covered by statutory controls at all.

Prof. Davies asserted that greater clarity regarding core definitions and concepts is necessary to prevent mission creep, or the tendency to move outside of one sub-mission scope and into another. This has been especially pronounced during and in the wake of the so-called 'War on Terrorism' during the first two decades of this century. Prof. Davies argued that if 'intelligence' is usually characterized as a multi-disciplinary, all-source collection and exploitation enterprise then it should follow logically that the goal of CI is to counter an adversary's multi-disciplinary all-source enterprise rather than being purely counter-human intelligence (counter-HUMINT). CI doctrine has been oscillating between these two alternatives, Multi-Disciplinary CI (MDCI) and Human Threat Vector CI (HTCI), since the 1920s. Because of the central role of technical intelligence collection systems in ISR, MDCI a particular significance for military CI. As a result, US military doctrine of the 1990s framed CI in terms of the predecessor doctrinal concept to ISR, RISTA (Reconnaissance, Intelligence, Surveillance and Target Acquisition) and British joint doctrine of the same period framed it as

counter-ISTAR (counter-Intelligence, Surveillance, Target Acquisition and Reconnaissance). US thinking argued that an MDCI to CI and especially CI analysis, should entail counter-IMINT, counter-SIGINT, counter-reconnaissance and counter-OSINT was as the traditional human threats of HUMINT, sabotage and subversion.

Since 9/11, US and allied CI doctrines have focused purely on HTCI and multi-disciplinary approaches have been neglected. No less importantly, the sweep of HTCI threats covered by CI doctrine has experienced significant mission creep. Current NATO doctrine is that CI should counter all of 'Terrorism, Espionage, Sabotage, Subversion and Organized Crime' under the acronym TESSOC. Prof. Davies argued that it is hard to see what terrorism and organized crime have to do with 'destroying the effectiveness of the enemy's intelligence service'. The inclusion of 'terrorism' in British CI requirements appears originally to come out of the Malayan Emergency in which insurgents and terrorists were perceived as what he termed 'non-state purveyors on sabotage and subversion'. In American CI discussion terrorists are described as "violent subversives" phraseology that reflected a tendency (prior to the second half of the 1980s) to perceive them as typically proxies for major powers such as the PRC and SOVBLOC. The inclusion of organized crime appears to have arisen from campaigning experience in Afghanistan where terrorist activities were funded by organized crime in terms of the narcotics trade in opium. The result is a conceptual conflation between CI and the omnibus concept of 'security intelligence' which appears in MI5 parlance, elsewhere in NATO doctrine and which has even been enshrined in Canadian statute under the 1982 CSIS Act.

In the early 2000s, during the 'War on Terrorism' a review conducted for the US Joint Chiefs of Staff noted the lack of distinction at the tactical level of military operations between counter-insurgency, counter-terrorism, and counterintelligence led to the joint chiefs modifying their mission in order to take into account the differences between adversaries at the state- and insurgent-level as well as their capabilities. All of these functions in a COIN campaign are also closely interdependent with tactical HUMINT activities. As a result, US doctrine and practice since has been to subordinate CI to the command staff HUMINT cell, J2X, a practice since adopted by NATO and subsequently also the UK. This has intensified the HTCI focus of military CI across the Western alliance.

The result is that in current NATO doctrine MDCI and counter-ISR have largely fallen by the wayside. Functional responsibility for MDCI and counter ISR is currently unclear due to conflicting perceived mandates in NATO doctrines for CI and for operations security (OPSEC) and deception. OPSEC doctrine expects

counter-ISR information to come from an intelligence that thinks J2's CI role is about TESSOC/HTCI, which Professor Davies pointed out differ little from Western notions of the 'comprehensive' approach to conflict, entail both the possibility of overt warfare but consist in a major part of sub-threshold/grey zone operations that can be characterized as a mixture of kinetic and non-kinetic operations falling within the sub-threshold of activity and below the threshold of traditional war. Kinetic operations include publicly declared paramilitary operations, deniable paramilitary operation (i.e.. Sovereign sabotage and assassination operations and paramilitary support operations (PMSO) which are delivered by proxies or allied. Non-kinetic means, on the other hand, include cyber-attacks/exploitation, influence/information operations (through the use of agents of influence and/or grey and black front organizations), and cyber disinformation including through automated software. A critical implication of this is that virtually all subthreshold FSC/HW measures are either delivered by, or fundamentally enabled by, FIS. This places them within the traditional CI remit of counter-espionage, counter-sabotage, and counter-subversion. An additional complication is that Russia's pursuit of FSC/HW during the Donbas 'frozen war' between 2014 and the 2022 invasion of Ukraine added the provision of support to Donbas proxies from Moscow-controlled, state-level ISR systems such as Russian Army Svet-Ku and Dzudoist mobile signals intelligence (SIGINT) systems. As a result, not only is CI the first line of defence against FSC/HW, to be effective what is required is a comprehensive, MDCI approach to CI rather than one focused narrowly on human threats alone, and especially not only liable to distraction by extraneous missions such as CT and organized crime from its core mission of 'destroying the effectiveness of the enemy's intelligence service'.

KEY POINTS OF DISCUSSION

- The core objective of a counterintelligence mandate is to disable the effectiveness of an enemy's intelligence infrastructure by countering acts of sabotage, espionage, and subversion. When it comes to FSC, a purely human threat approach to counterintelligence is inadequate in addressing it's the diversity and capabilities of that threat.
- The ideal counterintelligence strategy for counteracting sub-threshold activities involves understanding that the majority of the FSC/HI subthreshold activity is delivered or enabled by FIS organizations. Strategic peer FIS capabilities include technical intelligence collection disciplines, such as Russian electronic warfare (EW) support to Donbas militants. Consequently CI directed against FIS and FIS support to FSC/HW also needs to equally multi-disciplinary.

- The exclusive focus of US, UK and NATO counterintelligence doctrine on TESSOC and human threat vectors has left the role of countering MDCI and especially counter-ISR in doctrinal and organizational limbo. Consequently allied approaches to CI are woefully ill-equipped to act as the first line of defence against FSC/HW that they need to be.

FURTHER READING

Davies, P.H.J. (2021). ISR versus ISTAR: A conceptual crisis in British Military Intelligence. *International Journal of Intelligence and Counterintelligence, 35*(1). 73-100. https://doi.org/10.1080/08850607.2020.1866334

Davies, P.H.J. (2024). The Trouble with TESSOC: the Coming Crisis in British and Allied Military Counterintelligence Doctrine. *Defence Studies*. In press. DOI: 10.1080/14702436.2024.2303084.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/