Defence Studies

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fdef20

The trouble with TESSOC: the coming crisis in British and allied military counterintelligence doctrine

Philip H.J. Davies & Toby J. Steward

To cite this article: Philip H.J. Davies & Toby J. Steward (2024) The trouble with TESSOC: the coming crisis in British and allied military counterintelligence doctrine, Defence Studies, 24:2, 234-256, DOI: 10.1080/14702436.2024.2303084

To link to this article: https://doi.org/10.1080/14702436.2024.2303084

Published online: 11 May 2024.

DEFENCE STUDIES
2024, VOL. 24, NO. 2, 234–256
https://doi.org/10.1080/14702436.2024.2303084

Routledge
Taylor & Francis Group

The trouble with TESSOC: the coming crisis in British and allied military counterintelligence doctrine

Philip H.J. Davies[a] and Toby J. Steward[b]

[a]Brunel University Centre for Intelligence and Security Studies (BCISS), Brunel University, Uxbridge, UK; [b]Royal Air Force Officer, Chief of the Air Staff Trenchard Fellow; Honorary Research Fellow Brunel University Centre for Intelligence and Security Studies (BCISS), Brunel University, Uxbridge, UK

ABSTRACT

This article examines the evolution of UK military doctrine on counterintelligence (CI), one of the more consistently troubled aspects of military doctrine in general and intelligence doctrine in particular. We argue that current UK and NATO CI doctrine are in thrall to a deeply problematic defining concept in TESSOC (Terrorism, Espionage, Sabotage, Subversion and Organised Crime) that conflates an intractably diverse assortment of security threats under CI. Furthermore, TESSOC is the latest embodiment of a slow, century-long oscillation between two different basic concepts of CI. The first focuses purely on human threat vectors (referred to here as Human Threat CI or HTCI) while the latter entails a more comprehensive, all-source range of adversary technical and open as well as human source intelligence activities (designated Multidisciplinary CI or MDCI in US doctrine). That oscillation is driven largely by the balance between conventional and asymmetrical operations in defence priorities and recent campaign experience. TESSOC is a legacy of the recent, pre-Russo-Ukraine War emphasis on counterterrorism (CT) and counterinsurgency (COIN) operations. Consequently, UK and allied military counterintelligence doctrine are entering the second quarter of the 21st Century fundamentally ill-equipped to cope with strategic peers and their use of full-spectrum and hybrid strategies.

ARTICLE HISTORY
Received 31 August 2023
Accepted 4 January 2024

> It is safe to estimate that the efforts of the enemy to gain information will be at least as energetic as our own, and that he will neglect none of the various methods which are usually followed. David Henderson. (1904, 46)

> The object of counterintelligence is to destroy the effectiveness of the enemy intelligence organization. War Office (1946, 1).

Introduction[1]

As philosopher Peter Burke recently argued: "In times of war, military operations are, among other things, battles between ignorance and knowledge, attempting to keep the

CONTACT Philip H.J. Davies philip.davies@brunel.ac.uk Brunel University Centre for Intelligence and Security Studies (BCISS), Brunel University, Middlesex, Uxbridge, UK UB8 3PH

enemy ignorant of one's plans while trying to discover theirs" (Burke 2023, 40). If the latter of these is the role of intelligence, the former task of keeping the adversary in ignorance is the role of two distinct but closely related functions: operations security (OPSEC) and counterintelligence (CI). Recent decades have seen the growth of a substantial historical literature on what has been called "positive" intelligence (Kent 1949, 3, 210) which is to say intelligence concerned with the operational environment and adversary capabilities and intentions. There has also evolved a somewhat slimmer conceptual and theoretical literature (e.g. Davies 2016, 2022; Davies and Gustafson 2019; Ferris 2003, 2004; Handel 1990; Herman 1996, 240–256; pp.121–124; Hughes-Wilson 2004, 1–15; Kahn 2001; Odom 2003, 84–119; Tripodi 2018; Wolfberg 2016). By comparison, counterintelligence in the military realm – as opposed to the high policy domain of the national security and intelligence agencies – remains profoundly underdeveloped. While it does appear as a subordinate theme in many historical narratives (e.g. Clayton 1993, 152–171; Davies 1997, 39–40, 48, 78–79 and *passim* pp.35; Hasswell 1973 *passim*; and *passim*; Parritt 2011, 173–174, 203–204, 2320233 and *passim*; Van der Bijl 2013 *passim*), there have been at most a handful of conceptual or policy-oriented contributions on the matter over the last two decades (e.g. Magee 2011; Bridgeman 2009; Melendez 2019). Indeed, a 2020 bibliometric survey of articles on intelligence in defence organizations published between 2009 and 2018 concluded that only 10 of 211 articles addressed CI at all, whether historically or conceptually (compared with, for example, 62 discussing intelligence collection, 30 addressing "adaptation and reform" or 29 the "Intel-policy nexus"; Reijtens 2020, 724–725).

This lack of attention is more consequential than a mere intellectual lacuna in an important area. It has an added, more urgent, significance because UK and allied counterintelligence doctrine and policy currently find themselves in a very real state of crisis. Basic concepts in current military CI thinking are often confused and uncertain and largely the result of unexamined, short-term incremental changes in CI thinking. Those incremental shifts have been wedded to a myopic focus on current threats and campaigning priorities while ignoring developments in the wider strategic and security environment. Nowhere is this more starkly visible than in the recent UK and NATO defining remit for CI being not just "identifying and counteracting the threat from hostile intelligence services" and the unauthorised and possibly inadvertent disclosure of sensitive information, but an oddly unfocused suite of threats covering 'individuals engaged in "terrorism, espionage, sabotage, subversion and organized crime", collectively referred to as "TESSOC" (DCDC 2015 2-6; Royal Air Force Police 2022).

TESSOC presents a number of problems, not least of which is that terrorism and organised crime would appear to have little to do with, as the second epigraph to this piece puts it, "destroying the effectiveness of the enemy intelligence organization." The inclusion of terrorism and organised crime effectively *broadens* the concept of counterintelligence to the point that it is concerned with *all* manner of internal security threats. But this effectively conflates counterintelligence with the existing broader concept of *security intelligence*. The result is increased doctrinal vagueness, overlap and duplication that offers little or no conceptual or practical advantage in exchange. The idea of "security intelligence" has long been established as the omnibus concept in the Anglophone intelligence world (see, e.g. Kent 1949, 209–210; Security Service 1993, 20–21), and has even been enshrined in Canadian statute law in this capacity since 1982 (Government of

Canada 1982 §2(2), §12; Government of Canada (1991), 37–39). But this is perhaps less important than the second problem, which is actually one of conceptual *narrowing*.

At the same time that TESSOC broadens the range of security threats covered by CI, it actually reduces the range of specifically *intelligence* threats with which CI should be concerned. It is virtually axiomatic in the field of intelligence that intelligence collection and analysis are supposed to be *all source* enterprises (e.g. Herman 1996, 42–43), covering the entire gamut of available and appropriate forms of intelligence collection methods or "disciplines" (e.g. Director of Central Intelligence 1994, 1; DCDC 2011, 2-11 – 2-14), human and technical alike. Adversary signals intelligence (SIGINT), imagery and geospatial intelligence (IMINT and GEOINT), measurements and signatures intelligence (MASINT) and even open source intelligence (OSINT) are all as a much a part the work of, and threat from, "the enemy intelligence organization" as are the recruitment of human agents for espionage, sabotage or subversion. And yet, TESSOC focuses purely on what might best be termed human threat vectors in an approach to CI that will be referred to here as "Human Threat CI" (HTCI). It offers no framework for counter-intelligence to think about, let alone *counter*, adversary technical collection and OSINT capabilities and efforts. The result is a CI doctrine that ill-suited to the current strategic environment of major power full-spectrum challenge and conflict, irregular and hybrid warfare and a global miasma of information and disinformation operations (see, e.g. Cabinet Office 2021, 2023).

To cope with the problem of TESSOC effectively we need to understand how these circumstances have arisen. While it might be intuitively appealing to assume that this current doctrinal *cul de sac* is purely the result of a comparatively recent doctrinal mission creep, this significantly oversimplifies the matter. In fact, the very trouble with TESSOC is *not* that it is not an isolated mis-step or idiosyncrasy rooted in the recent near-exclusive allied campaigning – and hence doctrinal – focus on counter-terrorism (CT) and counter-insurgency (COIN). It is, in fact, the most recent manifestation of a much more fundamental and universal dilemma in all counterintelligence thought, one with which the intelligence community has been struggling for just over a century. That basic and pervasive dilemma is brought into especially sharp relief in the defence and military context, however. This is because of the especially palpable threat presented by often highly technical adversary intelligence, surveillance and reconnaissance (ISR) capabilities to the ability of friendly forces to operate and deliver effects. The first step, therefore, is to understand that basic dilemma. Then one can examine how successive iterations of military intelligence doctrine have tried to navigate that dilemma.

The Counterintelligence 'Discipline' Dilemma

Counterintelligence is a field of intelligence where the basic mission and core concepts and definitions are, if it all possible, even more contested and uncertain than in other spheres of intelligence activity (for some key conceptual debates in intelligence, see e.g. Breakspear 2013; Davies 2012, 44–74; Herman 1996, 114–120; Phythian 2013 *passim*; Warner 2002). CI has been dogged for decades with persistent debates and disputes over the natures of offensive versus defensive CI ((e.g. Copeland 1974, pp.160–197; Dulles 1963; Felix 1963, pp.129–137; pp.122–124; Herman 1996, 172–182; Olson 2019, 40–43; Prunckun 2012 and *passim*; pp.35–49; Zuehlke 1980, 13–18, 26–30), the role and status of

CI in intelligence agencies and communities (e.g. Miler 1979; Odom 2003, 167–184) and the relationship between counterintelligence and, variously, protective security and law enforcement (e.g. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981; Posner 2006, 2009; Zuehlke 1980, 16–18).

The current crisis in counterintelligence, however, reflects a less well-known, less explored but equally if not more fundamental quandary about the basic nature of the counterintelligence mission. That fundamental quandary is, essentially, *what is counter-intelligence supposed to be countering?* The seemingly obvious answer that one is countering adversary or enemy intelligence actually opens up an underlying and, in CI terms, very troubling question of *how do you define intelligence anyway?* In 1980, Arthur Zuehlke warned that "the traditional assumption that CI is counter-HUMINT" should be seen as "a misapprehension fostered by a long history of espionage, whereas technical means of collection are a relatively recent phenomenon" (Zuehlke 1980, 18). In the modern world, he argued "The threat is 'multi-disciplinary,' encompassing SIGINT [signals intelligence], PHOTINT [photographic intelligence], and HUMINT" as well as "much effort . . . devoted to overt collection as well" (Zuehlke 1980, 19).

Much the same point was made in the mid-1990s by Abram Shulsky and Gary J. Schmitt (2002 [1996] p.114). At the time, they invoked the concept of "multidisciplinary counterintelligence" (MDCI) which was then in currency in US military intelligence doctrine.[2] In the UK, much same case was made at around the same time by Michael Herman. Herman reserved the notion of "counterespionage" to refer to counter-HUMINT, arguing that "counterintelligence" had "a wider meaning of 'intelligence on foreign intelligence:' getting information on *all* foreign intelligence threats . . . by *any* means (Sigint [sic] and other sources as well as agents and defectors)." The idea of counterintelligence should, therefore, properly denote "the multi-disciplinary effort to penetrate the many different [collection] disciplines of the adversary" (Herman 1996, 52, emphasis in the original).

One finds, therefore, two profoundly different, competing views of what counter-intelligence is supposed to counter. And the history of counterintelligence concepts over the last century has, in many respects, been one of wavering between HTCI and MDCI-oriented approaches to counterintelligence. As the transatlantic discussion of CI theory and the discipline dilemma above indicates, the tension between HTCI and MDCI is not confined to any specific national system. Indeed, one of the most important aspects of this dilemma has been the degree to which CI concepts and doctrine have evolved at an alliance level. They are as much emergent properties of international discussion and frameworks for cooperation as they are of sovereign deliberation and decision-making. As a result, current counterintelligence doctrine is the outcome of a multinational discourse, especially between the memberships of North Atlantic Treaty Organisation (NATO) and the Five Eyes (FVEY) intelligence "special relationship" between the UK, USA, Canada, Australia and New Zealand (on FVEY see e.g. Kerbaj 2022; Office of the Director of Central Intelligence 2023; Richelson and Ball 1985; Wells 2020; on NATO/FVEY doctrine sharing see; Davies 2022; Dowell 2011). The acute need for both multi-national interoperability and high levels of mutual trust based on common standards and practices in these alliances has been essential to the rise to dominance of HTCI and the consequent UK and NATO adoption of TESSOC. Therefore, to understand the origins and impact of TESSOC on UK defence and military concepts, doctrine and practice it will

be necessary to locate it within that wider doctrinal discussion and deliberation across the UK's alliances and over the longue durée.

The HTCI roots of counterintelligence

Multidisciplinary CI is, of course, a phenomenon of modernised, industrialised and technology intensive warfare. Much before the First World War, counterintelligence, or *counterespionage* rather, was almost by definition a human threat vector affair. Nowhere is this clearer than in the Earl of Essex's 1642 instructions to his Provost Marshal to "Discover the lurking subtleties of spies and by learning the true interpretation of men's words, looks, manners, forms and habits of apparel, to be able to pull out the devil of malicious deceit though he lie hid in never so dark a corner . . ." (quoted in Davies 1997, 24). And this would be a fairly accurate description of the counterintelligence mission in centuries before the rapid 19th and 20th century evolution of telecommunications, powered flight, global correspondence and news media that were the seedbed for the explosive evolution of technical and open source intelligence collection from the First World War onwards.

The earliest iteration of recognisable counterintelligence doctrine in the contemporary sense appears a decade before the outbreak of the First World War in Lt Col David Henderson's formative *Field Intelligence*, quoted in the first epigraph to this piece. While he offered the prescient warning that the enemy would "neglect none of those various methods" of intelligence collection available, those "various methods" were necessarily confined to enemy "overt" reconnaissance and "disguised observers". The "duty of obscuring" the former, Henderson admonished, "falls primarily on the cavalry screen" and on observing outposts and was "not a matter in which the Intelligence Officer [sic] need interfere" (Henderson 1904, 46). Rather, the Intelligence Officer's "direct concern" was "the enemy's disguised observers" such as "non-combatants" frequently "in the vicinity of the lines, in a position to see what is going on, and any one of [whom] may be a spy for the enemy" (Henderson 1904, 46–47)). Against these "the only effective safeguard is stoppage of communication", that is, field security measures such as censorship, movements control and investigation of suspect individuals (Henderson 1904, 47–50). He also added, again with prescience, that "we should even go farther, and garnish our obstacles [to enemy intelligence] with attractive but deceitful pitfalls in the way of false information and misleading appearances" (Henderson 1904, 46 *supra*). This linkage between counterintelligence and deception would also prove a recurrent theme in subsequent CI doctrine.

During the First World War the establishment, regularization and expansion of the Intelligence Corps led to a much more systematic and granular elaboration of core intelligence functions and concepts. From the outset, counterintelligence was as much a basic function of the Intelligence Corps as was the collection of information about adversary capabilities and intentions. Counterintelligence was, therefore, dogged with a taxonomical problem from its inception. On the one hand, it was the converse counterpart to "intelligence" in the latter sense of information support to command decision-making. On the other, it was also a sub-category of "intelligence" as a command staff function. The working solution to this terminological problem was to fall back on organization of the Intelligence Staff,[3] in which information about the enemy was

designated I(A) and counterintelligence I(B) (Hasswell 1973, 91). But as has so often been the case, institutional designations became terms of art and *de facto* conceptual frameworks. "B work" quickly became the preferred term for CI, not only inside the Intelligence Corps but more generally in the UK intelligence world, and especially notably in the nascent Secret Intelligence Service (SIS)[4] (see, e.g. Mackenzie 1931, 13, 80, 241, 251, 341, 388).

The terms employed at the time have a significance beyond mere labels of convenience or convention. The preferred term for the "B work" task in both the Army and SIS was the French loan word *contrespionage* (sometimes given as *contre-espionage*). During the interwar years *contrespionage* in its assorted variations fell out of use in favour of the its English counterpart "counterespionage," both in military circles, as we shall see, but also in national intelligence (see, e.g. Curry [1946] 1999, 44–46 and *passim*). Indeed, the very term "counterintelligence" would not come into currency in British practice until the middle of the Second World War. To be sure, there was an isolated and atypical use of "counterintelligence" in a sub-section of the 1922 *Encyclopedia Britannia* entry on "Military Intelligence" (Drake et al. 1922, 504–512).[5] The entry's actual content, however, reverted to "*contre-espionage*" [sic]. The distinction between CE and CI, however, would prove to be more than merely a choice of synonyms. As we shall see shortly, when "counterintelligence" was eventually adopted, it would be in the dual contexts first of alliance and combined operations, especially with the United States, and second of a growing move towards MDCI.

By contrast there is little on counterintelligence in Admiralty archives of the period. What there is indicates that that Royal Navy (RN) came to the function rather later than the Army, and in many key respects followed War Office conventions. According to one post-war review of naval intelligence: "Before the war [the RN] intelligence organisation was primarily concerned with reporting movements of foreign men-of-war and protection of trade" but by the end of the war "To these is now added Colonial Defence questions – Trade Intelligence – *Contre Espionage* [sic] and many newly evolved subjects of a most secret nature" (NID 1921a, emphasis added). Because of the global scale of British naval commitments across the British Empire there were inevitable parallels between the field organization of naval intelligence and the intelligence staff of deployed military (i.e. Army) headquarters. The Royal Navy maintained a very large number of permanent naval facilities across the British Empire and in friendly ports, and many of these in turn accommodated regional Naval Intelligence Centres. Their work entailed providing not only intelligence support to the defence of British possessions, facilities, trade and communications but also, in collaboration "with the Security Intelligence organisation[6] to obtain and distribute information on persons likely to act contrary to the interests of the British Empire" (NID 1921b). Like Henderson and the Intelligence Corps, the DNI's approach to counterintelligence was HTCI.

Being formally constituted only at the end of the First World War, the Royal Air Force (RAF) came even later to the problem of counterintelligence. Unlike the Army and Navy who approached CI as an *intelligence* problem, the RAF treated it as an extension of force protection by the Royal Air Force Police (RAFP). According to Stephen Davies, CI originally became a concern for the RAF "when intelligence reports claimed that elements of the British Communist Party were trying to infiltrate themselves into the armed forces" and "the Provost Marshal [professional head of the

RAFP] was tasked to ensure that no such elements were retained or recruited into the service to spread their subversive and dangerous beliefs" (Davies 1997, 35). By 1936, however, attention was shifting towards German military espionage (Davies 1997, 39). From the outset, and largely thereafter, and despite a highly technical approach to intelligence 'A' work, the RAF's approach to counterintelligence would remain entirely HTCI.[7]

Nascent MDCI between the World Wars

The post-First World War capture of military counterintelligence concepts and experience presented by the 1922 *Manual of Military Intelligence in the Field* (War Office 1922) set a number of important precedents, some of which would persist and others fall by the wayside. It would, for example, reinforce and enshrine in doctrine the wartime improvisation of 'A'and "B" work. It also revised and expanded the CI remit in a detectably MDCI direction. Echoing Henderson, the *Manual* warned its readers that "the objects of the enemy's secret service will be similar to our own", and divided B Work into Field Security under "I"(B)ii which undertook "protection against espionage *from without*" and Military Security, "I"(B)iii, concerned with "to prevent espionage and safeguard information *within* our own forces". The work of the former included, *inter alia* "measures for the prevention of espionage, of sabotage, and the leakage of information . . . Collating of information regarding the enemy's police and intelligence personnel and their methods [and] Counter-propaganda amongst the civilian population". And the latter was not just charged with security, counter-sabotage and counter-propaganda measures amongst military personnel, but also "all special security measures connected with operations" – today's OPSEC – and "Advice on and coordination for all forms of military deception, including camouflage" (War Office 1922, 77–79, emphasis in the original). Both sub-divisions were exhorted to "equally share the responsibility for discovering and nullifying every endeavour on the part of the enemy to penetrate our secrets and attack our moral and material resources by underhand means" (War Office 1922, 77).

Hard lessons, of course, had also been learned about the susceptibility of allied and German operations on the Western Front to tactical SIGINT. No less hard a lesson was the failure of British Army counterintelligence to follow up on indications of successful German penetration of allied battlefield landline communications (Beach and Bruce 2020, 4–5). As a result, Military Security was also assigned a GSO(3) "responsible for all matters connected with the security of signals, codes and ciphers in the field." This officer's task "in close co-operation with the corps of signals, is to draft instructions for the safety of signal communications of every kind," to ensure compliance therewith, and also that "not only the material means of communication" were secure but also "the cryptographic systems and methods employed." This was not only a passive, security compliance role, however. "I"(B) was also to ensure that "steps are also taken to ensure any code or cipher is changed as soon *as there is reason to believe that it may have been compromised*" (War Office 1922, 79 emphasis added). In other words, the counter-espionage effort of "I"(B) in 1922 included also a counter-signals intelligence (SIGINT) task that went beyond protective communications security (COMSEC nowadays) to also collecting and assessing on enemy COMINT activities.

Wartime MDCI and the adoption of 'counterintelligence'

Two significant, parallel trends contributed to the shaping of UK counterintelligence thinking during the Second World War. The first of these was the need to adapt the kind of CI concepts that had been articulated in the interwar doctrine to the new, increasingly technology intensive conduct of both war fare and intelligence during the conflict. The second was the increasingly close military and intelligence collaboration with the United States. This was an especially collaborative enterprise in the combined headquarters of major expeditionary operations such as Allied Forces Headquarters (AFHQ) for the invasion of Algeria and Morocco in 1942 and Supreme Headquarters Allied European Forces (SHAEF) for the 1944 D Day Landings. By this time, US Army had adopted the "counterintelligence" in preference to "counterespionage" around the same time that they reconstituted their Intelligence Police as the Counter-Intelligence Corps (CIC) in 1941 (N.A., N.D., 4). Almost certainly not coincidentally, at around the same time that combined headquarters were becoming the Allied norm "counterintelligence" begins to appear in British doctrine as the preferred doctrinal term of art by 1943 (War Office 1943a, 1943b). Indeed, by 1944 a constituent part of the SHAEF intelligence organisation was its combined, allied Counterintelligence War Room.[8]

Entirely separately from the allied context, the shift from "counterespionage" to "counterintelligence" also aligned with an increasingly multi-disciplinary approach that sought to counter enemy reconnaissance and open source activities not readily describable as "espionage". The 1943 iteration of the War Office *Manual* exhorted counterintelligence to "destroy the effectiveness" of enemy intelligence' through "the adoption of measures designed to prevent the acquisition by the enemy of information concerning our true situation and plans, and to nullify covert attack by the enemy against material and morale" (War Office 1943a, 9, 1943b, 1). This edition also harked back to Henderson's original guidance, quoting almost verbatim (but without attribution) his warning that "It is only logical to assume that the enemy's intelligence service is at least as efficient as our own. It is probable that he will employ all the methods used by us for acquiring information" (War Office 1943a, 2). However, by 1943 the technical intelligence explosions in SIGINT and IMINT were in full swing. As a result, the notion of "*all* the methods used by us" meant something very different from Henderson's day, including an implicit rejection of his notion that counter-reconnaissance was *not* the concern of counterintelligence.

And so the 1943 *Manual* went beyond measures against the usual HTCI suspects of "enemy agents" and "spies" in the form of "agents or persons who may be in sympathy, and communication, with the enemy". Counterintelligence was also directed to counter "observation and reconnaissance (air and ground)", warning that "movements of any kind will inevitably attract the attention of *enemy reconnaissance agencies*". Following from the 1922 doctrine, in 1943 CI was also to be concerned matters such as "Camouflage and concealment, track discipline, night movements, use of cover etc" all of which were aspects of "active security measures that can be taken by all to defeat enemy observation and reconnaissance" (War Office 1943b, 3 emphasis added). The same doctrine took a more passive approach to enemy SIGINT than the 1922 iteration. It provided very detailed explanations of the kind of SIGINT techniques the enemy employed and equally detailed guidance on communications

security methods (War Office 1943b, 40–47). It did not, however, give explicit instructions about collecting and assessing evidence of a successful enemy penetration of friendly communications as had the 1922 edition.

At the same time, censorship was subsumed within CI as, essentially, what today would be termed counter-OSINT. Previously, censorship been a separate Intelligence Staff function as I(C), alongside "A work" and "B work" (War Office 1922, 79–82, pp.93–95). "Items of news, announcements or letters published in the Press", warned wartime doctrine, "including the technical and local Press, radio broadcasts etc. may contain information of value to the enemy". Consequently "All such materials must, therefore, be subjected to censorship" (War Office 1943a p.6), and that censorship was consequently a constituent function of counterintelligence.

Decolonization and a return to HTCI

Almost immediately after the Second World War, British counterintelligence doctrine began a retreat from MDCI to a nearly exclusive attention to human threat vectors. The initial post-war CI doctrine from 1946 retained the core convictions and ideas of wartime military counterintelligence, including its multidisciplinary view of the intelligence threat (War Office 1946 esp. pp.1–6). This was followed, however, less than a year later by a substantially revised CI doctrine that took a very different approach to both the nature of counterintelligence, and the nature of expected future campaigns in which counter-intelligence would play role. The authors of the 1947 doctrine evidently held the view that, after the recent conflict, the likelihood of war with a military peer was a rapidly retreating likelihood. The 1947 *Manual* complacently assured the reader that:

> . . . intelligence, in any but its crudest forms, is the prerogative of a few highly organized states. It demands resources of personnel, money and technical skill which are beyond the reach of smaller, less developed countries. In a conflict between two major powers intelligence may well be a vital factor; but in a conflict . . . between one such power and a backward or less well organized opponent, it is unlikely to be of decisive importance. (War Office 1947, 5)

As a result, the counter-observation and counter-reconnaissance elements of wartime doctrine were quietly dropped. Intelligence doctrine now focused its efforts on purely human forms of espionage, sabotage and subversion. Indeed, the operational side of counterintelligence was now dominated by methods of investigation, interrogation and vetting, with detailed guidance on raids, searches and arrest procedures (War Office 1947, 19–41; 101–108). The only technical collection aspect and carry-over of wartime experience was a detailed discussion of the value of counter-clandestine W/T intercept "interception and direction finding" (War Office 1947; this set a sustained precedent, see, pp.12–13; Office 1962, 51). But this, of course, was primarily concerned with technical intelligence collection against human threat actors. Even censorship was notable by its absence from counterintelligence, although it would remain separate part of the wider military intelligence suite of activities and was supposed to be coordinated with CI (War Office 1959, 13, 1962, 81–84).

The information requirements of CI were also defined entirely in terms of human threat vectors and would continue to be so for some decades. "Counterintelligence information" requirements according to the 1962 *Manual* included information on

"enemy intelligence service capabilities and methods relating to espionage, sabotage and subversive activities", their "order of battle and networks, including personalities … methods of communication … equipment, especially sabotage and communication equipment" as well as "targets of CI interest" on any "line of advance" and "black" and "white" lists of probably hostile or unfriendly persons respectively in the local civilian population. Practically, this meant "hostile agents, known or suspect … movements of hostile or potentially hostile intelligence personnel including those with diplomatic or quasi-diplomatic status … dissemination of subversive or seditious views" and "known or suspected enemy collaborators, sympathizers or other persons whose presence may prove a security threat" (War Office 1962, 50–51).

The 1962 doctrine is probably the first moment where one can see terrorism explicitly drifting into the sphere of British counterintelligence. This edition was dominated in large part by a concern with intelligence and counterintelligence in "internal security situations" (War Office 1962, 37–44 and *passim*), what today would be referred to as insurgencies. The impact of successive "emergencies" such as those in Malaya, Kenya, Cyprus and elsewhere dominated the 1962 *Manual*. As a consequence, at the end of its list of classic counter espionage, sabotage and subversion information needs, the doctrine added "*enemy guerrilla and partisan activities*" (War Office 1962, 51, emphasis added).

Unfortunately, there is a dearth of available primary sources on CI doctrine between the early 1960s and the late 1990s. Writing in retrospect in 2013, Nick van der Bijl has described the inclusion of terrorism within counterintelligence as "recent", in comparison to the traditional concerns of espionage, sabotage and subversion (Van der Bijl 2020 [2013] p.3). On the other hand, van der Bijl also notes that the 1972 Official Irish Republican Army (OIRA) bombing of 16 Parachute Brigade's Officers' Mess in Aldershot prompted Intelligence Corps' "Security Companies worldwide [to] develop and adopt counter-terrorist measures" (Van der Bijl 2020 [2013] p.265). Terrorism was, of course, an escalating security concern across NATO throughout the 1970s but to shift the issue from field security and defensive force protection to counterintelligence as such was, functionally as well as conceptually, something of a step-change. So the question is how or why did terrorism move from one to the other.

As we have just seen, enemy guerrillas and partisans figured in the 1962 counterintelligence doctrine essentially because they constituted non-state purveyors of those traditional CI concerns of of sabotage and subversion. Terrorism appears to been incorporated into mid- to late-1970s US counterintelligence theory for much the same reason, because it was perceived as essentially a highly kinetic variety of subversion, conducted chiefly by non-state militant groups. A US intelligence community lexicon included terrorism within the definition of CI as early as 1977 (ICS 1977). In 1980 two American intelligence practitioners, one of whom was military, argued at a US conference on counterintelligence that terrorists should be "treated as spies behind the lines … *engaged in sabotage*" (Godson 1980, 156 emphasis added). At the time there was also a tendency to perceive – and misperceive terrorists – chiefly as proxies for hostile state actors. US intelligence officer Newton Miler captured this sentiment clearly in 1979 when he described the task of CI as to "prevent foreign intelligence services and foreign-controlled political movements, *which are often supported by intelligence services*, from infiltrating our institutions and establishing the potential to engage in espionage, subversion, *terrorism and sabotage*" (Miler 1979 p.49 emphasis added).

Over the course of the 1980s, terrorism would not only acquire a steadily growing security priority, but equally steadily acquire an increasingly important identity as a threat distinct from Cold War major power manoeuvring. At the national level, the rise of terrorism as a distinct threat in its own right would prompt the creation of dedicated counter-terrorist intelligence hubs in the national intelligence systems of both the UK and USA. In the UK MI5 had treated terrorism as a sub-category of subversion until 1975, but would abandon this approach in the 1980s and eventually operated two distinct counterterrorism branches, G Branch in 1988 and T Branch in 1990 (Andrew 2009, 647,700,745–746).[9] In the USA, the surge in terrorist activity against US targets that began to intensify after 1983 drove the establishment of the Counterterrorism Centre (CTC) in the Office of the Director of Central Intelligence in 1986. This was followed by a separate Counterintelligence Centre (CIC) the following year. (Davies 2012, 291–292,141; National Commission on Terrorist Attacks Upon the United States 2004, 92).

To a certain degree, therefore, the military inclusion of terrorism within CI rather than treating it as a threat in its own right was somewhat out of step with national intelligence practice during the last decade of the Cold War. It is not surprising, therefore, that its inclusion in the NATO CI triggered something of a sharply expressed push-back from within the UK's military intelligence community during the 1990s.

MDCI and the Counter-ISTAR Moment

To understand what happened next it is worth remembering Henderson's warning in the first epigraph to this piece, so often echoed in subsequent editions of the *Manual*. The implications of this maxim acquired new depth and significance as the Western allies emerged from the Cold War into the so-called "revolution in military affairs" (RMA, sometimes "military-technical revolution", MTR). RMA entailed an unprecedent synergy of technological step-changes in capability covering not just so-called "smart munitions" but in (what would become known as) the intelligence, surveillance and reconnaissance (ISR) systems used to target these weapons, and in the global, networked information and communications technologies that integrated these new capabilities with command and control (C2) (e.g. Hundley 1999; Lindsay 2013, 425–433; Rosen 2010). Besides dramatic change in kinetic capabilities, RMA had profound implications for military intelligence at all command levels.

In response to RMA, and initially largely independently of one another, both the US and UK defence communities struggled to articulate concepts and doctrine for the transformed and transforming realm of military intelligence. As a result, two parallel different counterpart suites of concepts emerged on opposite sides of the Atlantic. In the immediate Cold War interval, the term "RISTA" or "reconnaissance, intelligence, surveillance and target acquisition" appeared as the common NATO term of art (Davies 2022, 97–80; also e.g. United States Army 1995) until supplanted in the second half of the decade. Largely led by figures in the United States Air Force, RISTA was superseded in the USA by the concept of "intelligence, surveillance and reconnaissance" (ISR) while in the UK – largely on a British Army initiative – the dominant concept was that of "intelligence, surveillance, *target acquisition* and reconnaissance" (ISTAR) (Davies 2022, 80). For much of the subsequent two decades, most NATO countries, other than

the USA, as well as Australia all ended up using both ISR and ISTAR to one degree or another (Davies 2022, 82). In both cases, ISR and ISTAR approached intelligence in military operations firstly in terms of technical surveillance and reconnaissance capabilities, and then occasionally (even grudgingly) acknowledging the significance of human intelligence (e.g. House of Commons Defence Committee 2010, 13, 18).

Having articulated intelligence doctrine for an age of RMA, it was only a matter of time until defence thinkers followed Henderson's lead and began to ask *what if an adversary develops the same RISTA/ISR/ISTAR capabilities and uses them against us?*

Towards the middle of the 1990s the United States Army was clearly shifting to an MDCI approach. By 1993 it was defining CI as activity to counter 'opposing foreign intelligence and security services (FIS) activities . . . [including] . . . both those identifiable as intelligence collection (Human Intelligence [HUMINT], Signals Intelligence [SIGINT], Imagery Intelligence[IMINT]) and FIS activities that have other objectives (analysis and production, assassination, counterintelligence, deception, disinformation, propaganda, sabotage, sedition, subversion), (United State Army 1993, 1). In 1995, US Army doctrine explicitly stated that "By its nature, *CI is a multidiscipline effort* that includes counter-human intelligence (C-HUMINT), counter-signals intelligence (C-SIGINT), and counter-imagery intelligence (C-IMINT) designed to counter foreign all-source collection" (United States Army 1995 p.iii, emphasis added; further reinforced by nearly identical phrasing p.1–7 emphasis added). They framed this perspective in terms of RISTA, asserting (slightly awkwardly) that "As the adversary worries about our C-RISTA [counter-RISTA] capability, our CI efforts target his RISTA capabilities" (United States Army 1995, 1–4). Consequently, the 1995 doctrine concluded "Multidiscipline counterintelligence (MDCI) is an integral and equal part of intelligence and electronic warfare" (United States Army 1995, 1–4).

There was, however, a significant caveat to MDCI at the level of deployed forces. "CI focuses on the HUMINT threat in the AO [Area of Operations]" noted the 1995 doctrine but "provides analytic support in identifying enemy SIGINT and IMINT capabilities and intentions." This reflected the resources available to a CI cell in the field which "has a limited neutralization and exploitation capability directed at low-level adversary HUMINT collectors or sympathizers acting in a collection or sabotage capacity" (United States Army 1995, 1–7). In other words, the CI intelligence analytic picture should be an MDCI undertaking but operations were an HTCI affair. Much the same approach was also articulated in the US Marine Corps counterintelligence doctrine of 2000 (USMC 2000 pp.C-1 – C-23), albeit without explicitly referencing the RISTA concept.

Similar concerns were manifest in British defence circles when, four years later, the UK issued the first edition of its tri-service Joint Intelligence Doctrine, *JWP 2–00 Joint Operational Intelligence* ((Joint Doctrine and Development Centre (JDCC) 1999; for an overview of the evolution of UK joint intelligence doctrine see Davies and Gustafson (2019)). This first edition was a product both of the RMA deliberations over the preceding eight years and campaigning experience of the 1980s which had been dominated by the Cold War on the one hand, and drawing lessons from the Falklands conflict on the other (Davies 2022, 79). Another significant influence was the degree to which UK military operations during the 1990s had been dominated by peace support actions (Davies and Gustafson 2019, 19). This initial joint service intelligence doctrine explicitly

eschewed the NATO definition of CI as "identifying and counteracting the threat to security posed by hostile intelligence services and organisations, or by individuals engaged in espionage, sabotage, subversion or terrorism" (JDCC 1999 p.1A–5, referencing NATO's AAP-6). Instead, it was asserted that "While counterintelligence ... is generally regarded as countering activities within the human dimension, this document views the threat from the perspective of the enemy's ISTAR capability" (JDCC 1999 p.1A–5 *supra*). CI, it stated, "should first attempt to identify the ISTAR threat, then recommend measures to minimise its effectiveness" and "contribute to the development of offensive measures to degrade adversary ISTAR and so assist in achieving overall information superiority" (JDCC 1999 1A–5 *infra*).

The joint staff intelligence or 'J2' cell's counterintelligence staff (J2 CI staff) were instructed to craft "a formal estimate" of "the adversary's ISTAR capability and a plan of countermeasures". This CI estimate would draw on the intelligence picture of "Adversary ISTAR assets, including current posture and operational profile" and an "estimate of adversary intelligence requirements and ensuing collection priorities". This counterintelligence appreciation of enemy ISTAR would then feed into an "own force deception plan" and "force protection plan and priorities" (JDCC 1999 1A–6). Unlike US Army doctrine, JWP 2-00 omitted any caveat about deployed headquarters CI being confined to human threats. That being said, the 1999 doctrine offered only the most cursory discussion of CI and did not go into much practical detail about how counter-ISTAR was supposed to be delivered in practice. Nonetheless, both the UK and USA were committed to MDCI by the end of the decade.

J2X and the rise of TESSOC

If UK and certain allied CI concepts were moving back towards MDCI through counter-ISTAR and counter-RISTA during the 1990s, this trajectory was brought to an abrupt halt by the terrorist attacks of 11 September 2001. An early hint of the direction thinking would take after 9/11 can be found in the Marine Corps CI manual from the year before. Even though, as we have seen, the Corps largely shared the US Army's approach to MDCI in CI analysis, they also noted that while US Army CI was oriented to both tactical and strategic operations "The Marine Corps CI orientation is entirely tactical" (USMC 2000, 1–3). Consequently, they argued "Due to the intelligence requirements of commanders in direct contact with hostile forces, the line between CI and HUMINT at the tactical level is blurred almost beyond differentiation" (USMC 2000, 2–6).

This perception has propelled a post-9/11 shift to purely HTCI in the form of the J2X formula. Between 2005 and 2006 the US Joint Chiefs of Staff conducted lesson-learning exercise on operational intelligence that putatively drew on experience from the 1990s in the Balkans as well as more recent and far more vivid experiences of Afghanistan and the Iraq quagmire. The JCOS review mandated that, at every command level, CI and positive HUMINT were to be amalgamated into a single J2 subsection, J2X, which "tasks, manages, coordinates, synchronizes and deconflicts all ... CI and HUMINT source operation" (Costa 2006 quoting a 2005 US Joint Chiefs of Staff whitepaper at some length in n.5 17–18). CI would become formally a complementary, but in practice subordinate, task to operational and tactical HUMINT. Although some dissenting voices raised concerns about conflating CI with HUMINT (e.g. Bridgeman 2009, 136–137 with

reference to the Defense Intelligence Agency (DIA) rather than deployed commands), the JCOS conclusions stood and J2X quickly became the authoritative US approach to military CI (see, e.g. United States Army 2002 2-2 - 2-4).[10]

In much the same fashion, the next UK iteration of joint intelligence doctrine in 2003, *JWP 2-00 Intelligence Support to Joint Operations*, abandoned counter-ISTAR and also shifted entirely back to HTCI. Indeed, CI as a whole was given a strikingly cursory treatment. This consisted of a single paragraph which parroted the NATO doctrinal definition of CI as "those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services and organisations, or by individuals engaged in espionage, sabotage, subversion or terrorism". This second edition amounted to an almost explicit repudiation of the 1999 first edition. It continued that countering "activities within the human dimension, and can make a significant input to Force Protection (FP), Operations Security (OPSEC) and other security measures" (JDCC 2003 p.1A–3). Readers were otherwise directed to NATO joint doctrine for intelligence, security and counterintelligence (JDCC 2003 p.iii).

Exactly when, why or how *organized crime* became incorporated into the counter-intelligence remit is not clear from publicly available sources. A drift in this direction was already visible in the British 2011 *third* edition of the UK Joint Intelligence Doctrine, now entitled *JDP 2-00 Understanding and Intelligence Support to Joint Operations*, which proposed a new definition of CI "awaiting NATO approval". Under this definition, "counter-intelligence" [sic] was broadened to cover "activities that identify the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion, terrorism *or other non-traditional threats*" (DCDC 2011, 2–15, emphasis added). Reflecting the inclusion of "non-traditional threats", JDP 2-00's CI vignette did not actually address anything remotely like "destroying the effectiveness of the enemy's intelligence service". Instead, it recounted a criminal investigation by the RAF Police into private contractors for Camp Bastion in Helmand Province, Afghanistan, who were in possession of "unauthorised automatic weapons" which "were held contrary to Afghan Law and there was a risk that they could be stolen or used against Coalition forces" (DCDC 2011, 2–16).

In 2014 NATO produced a comprehensive recrafting of its *AJP 2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security* that drew heavily, often verbatim and at length, on the British 2011 doctrine (Davies and Gustafson 2019, 31–32; NATO, 2019, 2016). AJP 2 invested far more attention in CI and security than the British, devoting two chapters to the subject rather than JDP 2–00's two *pages*. Despite being based so closely on the British doctrine in other regards, however, NATO rejected Britain's proposed, "new definition" of CI. Instead, it retained the established AAP-6 criteria of "identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism" (NSO 2019, 34) that had been so sharply criticized by the UK's 1999 doctrine.

The renewed dominance of HTCI went hand in glove with the NATO and UK adoption of the US J2X formula. To be sure, in the 3rd edition of its Joint Intelligence Doctrine, the UK avoided explicitly, formally adopting the US J2X scheme. Rather, the UK placed the J2 CI Cell at the same organisational level as the J2X HUMINT cell, alongside other cells for geospatial intelligence, open source intelligence, all-source analysis and "material and personnel exploitation" (DCDC

2011, 5-17 – 5-16).[11] That being said, the 2011 doctrine also asserted that that "HUMINT activities often occur alongside those involving counter-intelligence and many of the skills and capabilities are common" and consequently should "be regarded as being complementary intelligence functions and must not become competitive." Indeed, the remit of counterintelligence operational activity was defined in almost purely human threat vector terms as entailing "liaison, investigations, casework, screening of locally employed civilians and intelligence collection" (DCDC 2011, 2–15). Unsurprisingly, while CI might not have been formally subordinate to J2X, the latter was awarded the authority to "maintain the register of sources and de-conflict both HUMINT and counter-intelligence activity" (DCDC 2011, 5–18).

NATO, on the other hand, imported the US J2X formula whole cloth by the latest in its 2014 intelligence doctrine (NSO 2016 p.8–2).

The final steps towards TESSOC and J2X in the UK were incremental ones, starting with a July 2012 Ministry of Defence decision that the UK "should use NATO doctrine wherever we can, and ensure coherence of UK doctrine with NATO wherever we cannot" (UK "green page" to DCDC 2015; see also DCDC 2014 p. v). At the same time, the 2011 version of JDP 2–00 relegated detailed discussion of counterintelligence to a planned sub-doctrine, *JDP 2.10.2 Counterintelligence* which would have been issued at RESTRICTED (DCDC 2011 p. v). During a 2014 update to JDP 2–00 the decision was taken to cover CI in a RESTRICTED Joint Doctrine Note (JDN), *JDN 1/14*, rather than doctrine as such (DCDC 2014, vi). Doctrine Notes differ from formal doctrine statements in that they are discussion papers "raised to either encourage debate, place 'markers in the sand' or capture and disseminate best practice" rather than "endorsed" authoritative statements of doctrine (DCDC 2022). Unlike ratified doctrine which remains authoritative until replaced, Joint Doctrine Notes also have a limited lifespan, and eventually expire. Consequently, as and when JDN 1/14 expired the UK was committed under the 2012 decision to adopting NATO CI doctrine in the absence of any new UK policy on the matter.

The next stage was NATO adoption of TESSOC. The first publicly visible use of TESSOC was the 2015 edition of the NATO force protection (FP) doctrine. Throughout the FP doctrine, "intelligence" figured centrally and with reference to this full TESSOC suite of security threats (DCDC 2015 2–6). And yet, for reasons that remain unclear, the FP doctrine made no reference to the concept of 'security intelligence, despite the widespread use of "security intelligence" noted in the introduction to this article, *and* the fact that the term was already employed in NATO Doctrine (e.g. NSO 2019 115). Instead, "counterintelligence" was used in the omnibus role, stretching the definition well beyond the prior existing NATO standard. This approach did, however, align significantly with the re-definition of counterintelligence that had been suggested by the UK in 2011 but that had been ignored or rejected by NATO in 2014. Under the NATO FP doctrine, therefore, counterintelligence was defined as " . . . the threat to security posed by hostile intelligence services or organizations or by individuals engaged in TESSOC" (DCDC 2015 A-14). Also on the basis of the 2012 NATO doctrine decision, the NATO force protection doctrine was adopted by the UK with the inclusion of UK annexes or

"green pages". This meant that the UK was now committed to equating TESSOC with counterintelligence, at least in force protection terms.

Consequently, when JDN 1/14 was finally withdrawn, it was all but inevitable that the UK would adopt NATO counterintelligence doctrine and consequently accept TESSOC as the definitive approach to counterintelligence in British intelligence doctrine. And with NATO CI doctrine also came the final adoption of the J2X concept, although by 2020 it had been *de facto* British practice for some time simply in order to align with, and ensure interoperability with, NATO practice. HTCI was now thoroughly "baked into" British and allied doctrine, organization and practice.

In late 2023 the UK issued the fourth edition of *JDP 2-00 Intelligence, Counterintelligence and Security Support to Joint Operations* (DCDC 2023). Drafting had commenced during the Donbas 'frozen war' but was completed in the wake of Russia's 2023 invasion of Ukraine. During the revision and rewrite process the state of UK and allied counterintelligence thinking was one of the main points of concern. As a result of these deliberations the new doctrine substantially revised and expanded its discussion of counterintelligence, and made some effort to clarify the relationship between security, security intelligence and counterintelligence. TESSOC was retained but as a taxonomy of *security* threats, and 'security intelligence' took on the the same omnibus meaning it has elsewhere in the intelligence world. The new JDP 2-00 reverted to the slightly narrower and older NATO AAP-6 remit of CI (espionage, sabotage, subversion and terrorism) and warned readers that 'security is not the same as counter-intelligence, although security functions underpin counterintelligence efforts and support counterintelligence outcomes' (DCDC 2023 93). Progress has, however, been partial. While the new doctrine noted that CI operates 'across all operational domains', that is, maritime, land, air, and 'cyber and electromagnetic activities' (CEMA) it remains human threat oriented. It has, furthermore, formally enshrined the J2X formula in UK doctrine (DCDC 2023 80). In the meantime, NATO doctrine still retains TESSOC as the framework for counterintelligence as well as J2X. Finally, there remains little visible progress amongst the UK and her allies towards explicitly aligning CI with counter-ISR, or more fundamentally addressing the entire question of multidisciplinary CI.

Conclusion: Military Counterintelligence For the 21st Century

British and allied militaries are, therefore, approaching the second quarter of the twenty first century with a suite of counterintelligence concepts, doctrine and processes that are profoundly unfit for purpose. TESSOC is not the sole manifestation of the malaise. It does, however, capture the essence of the dual problem of adding security threats that have little to do with the core mission of *countering adversary intelligence* while disengaging military CI activity from some of the most important intelligence threats to military operations from enemy technical ISR systems and open source exploitation. This not to say terrorists and criminals do not engage in intelligence collection and assessment against friendly forces. Indeed, they are often alarmingly good at doing so (see, e.g. Gentry and Spencer 2010; Ilardi 2010; Mobley and Ray 2019). Understanding, detecting and countering terrorist or criminal intelligence activity is, therefore, a very real part of counterintelligence in an asymmetrical conflict. But the scale of policy response, operational activity and resource allocation required to address the terrorist kinetic and

political threat lies well beyond the purview of "destroying the effectiveness" of their *intelligence* activities and capabilities. Much the same can be said of criminal activity, especially organised crime.

At the heart of the TESSOC and J2X matter is the principle that *overlap is not equivalence*. TESSOC does, indeed, provide a very succinct framework, a set of conceptual handrails if you will, for thinking about the fuzzy boundaries between the various security threats. Involvement in criminal activity lays an individual open to the kind of pressure that can lead to their recruitment as a human source by an adversary. It figures centrally in the classic human intelligence concept of "MICE" – money, ideology, compromise and ego – and is understandably a key insider threat warning indicator (e.g. Kont et al. 2018 *passim*). But of the many military persons who may be involved in criminal activity, serious or petty, opportunistic or organized, few will ever actually be recruited by hostile foreign intelligence services. And only then are they properly counterintelligence concerns rather than questions of criminal investigation. TESSOC is an entirely reasonable model for *security intelligence*, but counterintelligence is, as Kent (1949), a "most dramatic" sub-category of security intelligence. It is not, nor should it be, a synonym.

What the evolution of counterintelligence doctrine displays over the *longue durée* is not a random oscillation between HTV and MDCI. One can see CI thinking being systematically driven back and forth between the two approaches by successive campaigning experiences. During periods of asymmetrical conflict in "internal security situations" against terrorists and insurgents, CI practice and thinking becomes confined to the largely human intelligence threat vectors that dominate that kind of setting. However, where engaging nominal strategic peer, state-level actors with highly capable, all-source intelligence, surveillance and reconnaissance capabilities a multidisciplinary approach to CI is required to address those capabilities.

The problem with the campaign-driven oscillation examined here is that while MDCI can encompass counterintelligence activity against human threats, an HTV approach to CI induces something akin to doctrinal amnesia regarding technical intelligence threats. Bluntly, MDCI can be adapted to asymmetrical conflict but HTCI *cannot* be adapted to symmetrical. From this it therefore also follows that HTCI falls short against so-called "full spectrum" or "hybrid" threats because these entail both symmetrical and asymmetrical axes of engagement. The adversary's proxies and irregular combatants are as likely to be supported by national strategic and military intelligence assets such as SIGINT systems, airborne strategic stand-off radars and reconnaissance satellites as by local agents and clandestine reconnaissance.[12] Indeed, in any conflict involving clandestine, deniable and hybrid aspects, counterintelligence must necessarily become the first line of defence (For a more detailed discussion of this matter and illustration employing the Ukraine case, see Davies 2024). In 2010, the drafting team crafting the 3rd Edition of the UK's Joint Intelligence Doctrine committed themselves to the principle that intelligence doctrine should not be beholden to the "threat du jour," the dominating campaign concerns at the time (Davies and Gustafson 2019, 23). The longevity of that doctrine, which remained in force until October 2023, suggests that on "A work" that effort may have succeeded. But on "B work" it regrettably failed.

Notes

1. We are deeply indebted to the valuable comments and suggestions from the journal's peer reviewers as well as to colleagues at the Brunel Centre for Intelligence and Security Studies (BCISS), the UK Ministry of Defence, and attendees at the North American Society for Intelligence History conference in Calgary in July 2023 for comments on earlier versions of this article.
2. Their usage of MDCI was somewhat different from that in US intelligence doctrine because, as will become apparent below, Shulsky and Schmitt used MDCI *only* to countermeasures against the technical collection disciplines while actual US doctrine used it to refer to *all* collection disciplines, human, technical and open source.
3. This was, of course, well before the UK adoption of the French version of the Continental command staff model and its numbered branches with "G2" as intelligence.
4. The term "MI6" was not employed during the First World War but was adopted in late 1939/early 1940. During Mackenzie's time the preferred circumlocution was MI1c. See Davies (2004) p.109.
5. I am deeply indebted to Dr Jim Beach at the University of Northampton for bringing this item to my attention.
6. This is almost certainly a reference to MI5 despite that agency's status being both much reduced and in flux with the brief rise and fall of Basil Thompson's Directorate of Intelligence.
7. Unlike War Office and Admiralty files in The National Archive (TNA), counterintelligence makes *no* appearance in AIR intelligence papers at TNA.
8. A substantial body of alliance CI materials and the work of the SHAEF CI War Room can be found in the WO 208 series at The National Archive, especially, *inter alia*. W0 208/5198 and WO 208/4701).
9. G Branch was originally an omnibus counterterrorism branch then focused purely on foreign terrorism after T Branch was established to focus on Irish and other domestic terrorism.
10. Others also raised concern about the HUMINT focus. Jennifer Sims, for example, proposed what might be termed a discipline-agnostic approach to CI through the notion of "mission-based" CI, although her substantive examples were largely counter-HUMINT. Robert Wallace argued for attention to technical surveillance but this was mainly in the investigatory sense of covert physical and technical surveillance rather than the military ISR sense, with a similar case by James Gosler focusing on cyber and computer network security rather. See, variously, Sims and Gerber (2009) Wallace and Gerber (2009), 112–115 and Gosler and Gerber (2009), 181–185.
11. Material and Personnel Exploitation is a multi-int discipline combining, essentially document exploitation, physical and digital forensic analysis and detainee interrogation.
12. For example on Russian use of capital asset military electronic warfare systems in the Donbas so-called "frozen war," see Fish (2017).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported in part by a 2019-2020 Chief of the Air Staff Trenchard Fellowship awarded to Wing Commander Toby Steward.

Notes on contributors

Professor Philip H. J. Davies is Professor of Intelligence Studies at Brunel University and Director of the Brunel University Centre for Intelligence and Security Studies (BCISS). He was an author on both the third and fourth (current) editions of the UK military joint intelligence doctrine and the first edition of the joint doctrine on 'understanding' for operational commanders.

Wing Commander Toby J. Steward is an RAF officer with a broad professional background in security liaison, special investigations and military Space operations. He is a previous recipient of a Chief of the Air Staff's Trenchard Fellowship, a graduate of United States Air War College and is a BCISS Honorary Research Fellow.

ORCID

Philip H.J. Davies http://orcid.org/0000-0003-3820-8862

References

Andrew, Christopher. 2009. *Defence of the Realm: The Authorized History of MI5*. London: Penguin.

Beach, Jim, and James Bruce. 2020. "British Signals Intelligence in the Trenches, 1915–1918: Part 1, Listening Sets." *Journal of Intelligence History* 19 (1): 1–23. https://doi.org/10.1080/16161262.2019.1659580.

Breakspear, Alan. 2013. "A New Definition of Intelligence." *Intelligence & National Security* 28 (5): 678–693. https://doi.org/10.1080/02684527.2012.699285.

Bridgeman, Vincent H. 2009. "Defence Intelligence, Reconceptualised." In Vaults, Mirrors and Masks: Rediscovering US Counterintelligence, In Jennifer, Sims, and Burton Gerber edited by. 125–148. Washington DC: Georgetown University Press.

Burke, Peter. 2023. *'Ignorance in War'* Military History Matters *Issue 132 (February/March 2023) 40-45; Extracted from Burke, Peter (2023) Ignorance: A Global History*. New Haven, CT: Yale University Press.

Cabinet Office. 2021. Global Britain in a Competitive Age the Integrated Review of Security, Defence, Development and Foreign Policy *CP403*. London: Her Majesty's Stationery Office (HMSO).

Cabinet Office. 2023. *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World*. London: His Majesty's Stationery Office (also HMSO).

Clayton, Anthony. 1993. *Forearmed: A History of the Intelligence Corps*. London: Brassey's (UK).

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. 1981. *Second Report: Freedom and Security Under the Law*. Ottawa: Minister of Supply and Services Canada.

Copeland, Miles. 1974. *The Real Spy World*. London: Weidenfeld and Nicolson.

Costa, Christopher P. 2006. Phoenix Rises Again: HUMINT Lessons for Counterinsurgency Operations Unpublished dissertation. Newport: US Naval War College. [Accessed December 5, 2023]. https://apps.dtic.mil/sti/pdfs/ADA463402.pdf.

Curry, John. [1946] 1999. *The Security Service 1908-1945*. London: Public Record Office.

Davies, Philip H.J. 2004. *MI6 and the Machinery of Spying*. London: Frank Cass.

Davies, Philip H.J. 2012. *Intelligence and Government in Britain and the United States*. Vol. 1. Santa Barbara, CA: Praeger Security International.

Davies, Philip H.J. 2016. "The Problem with Defence Intelligence." *Intelligence & National Security* 31 (6): 797–809. https://doi.org/10.1080/02684527.2015.1115234.

Davies, Philip H.J. 2022. "ISR versus ISTAR: A Conceptual Crisis in British Military Intelligence." *International Journal of Intelligence & CounterIntelligence* 35 (1): 73–100. https://doi.org/10.1080/08850607.2020.1866334.

Davies, Philip H.J. 2024. "Counterintelligence and Escalation from Hybrid to Total War in the Russo-Ukrainian Conflict 2014–2024." *Intelligence and National Security* 39(3): 496–514. https://doi.org/10.1080/02684527.2024.2329419.
Davies, Philip H.J., and Kristian C. Gustafson. January 2019. "Intelligence and Military Doctrine: Paradox or Oxymoron?" *Defence Studies* 19 (1): 19–36. https://doi.org/10.1080/14702436.2018.1538698.
Davies, Stephen R. 1997. *Fiat Justicia: A History of the Royal Air Force Police*. London: Minerva Press.
DCDC. 2011. *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. Shrivenham, UK: DCDC.
DCDC. 2015. *AJP-3.14 Allied Joint Doctrine for Operations Security and Deception*. Shrivenham, UK: DCDC.
DCDC. 2022. *Development, Concepts and Doctrine Centre*. [Accessed October 24, 2022]. https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre .
DCDC. 2023. *Joint Doctrine Publication 2-00 Intelligence, Counterintelligence and Security Support to Joint Operations*. Shrivenham, UK: DCDC.
Development, Concepts and Doctrine Centre (DCDC). 2014. *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations – with Change 1*. Shrivenham, UK: DCDC.
Director of Central Intelligence. 1994. *Consumer's Guide to Intelligence*. Washington DC: Office of the Director of Central Intelligence.
Dowell, J. A. E. K. 2011. JADEX Papers 5 Intelligence for the Canadian Army in the 21st Century "Enabling Land Operations. Ottawa: Canadian Army by the Directorate of Land Concepts and Designs.
Drake, Reginald. 1922. Secret Service and Counter-Intelligence. In *Intelligence, Military, Encyclopaedia Britannica*, edited by. Atkinson, Charles. 12th. London: Encyclopaedia Britannica 504–512.
Dulles, Allen. 1963. *The Craft of Intelligence*. London: Weidenfeld and Nicolson.
Felix, Christopher. 1963. *The Spy and His Masters: A Short Course in the Secret War*. [James McCargar]. London: Martin Secker & Warburg Ltd.
Ferris, John. 2003. "A New American Way of War? C4ISR, Intelligence and Information Operations in Operation 'Iraqi Freedom': A Provisional Assessment." *Intelligence & National Security* 18 (4): 155–174. https://doi.org/10.1080/02684520310001688916.
Ferris, John. 2004. "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence & National Security* 19 (2): 199–225. https://doi.org/10.1080/0268452042000302967.
Fish, Tim. 2017. "Russia Steps Up Electronic War in Ukraine." *Digital Battlespace* 9 (4): 7.
Gentry, John, and David E. Spencer. 2010. "Colombia's FARC: A Portrait of Insurgent Intelligence." *Intelligence & National Security* 25 (4): 453–478. https://doi.org/10.1080/02684527.2010.537024.
Godson, Roy. 1980. *'General Discussion'. Intelligence Requirements for the 1980s: Counterintelligence*, 156–158. Washington DC: National Strategy Information Centre.
Gosler, James R. 2009. "Counterintelligence: Too Narrowly Practiced." In Vaults, *Mirrors and Masks: Rediscovering US Counterintelligence*, edited by. Jennifer, Sims, 173–198. Washington DC: Georgetown University Press.
Government of Canada. 1982. *The Canadian Security Intelligence Service Act*. [Accessed June 16, 2023]. https://laws-lois.justice.gc.ca/eng/acts/c-23/.
Government of Canada. 1991. *On Course: National Security for the 1990s*. Ottawa: Minister of Supply and Services Canada.
Handel, Michael I.1990. "Intelligence and Military Operations." In Michael I. Handel, ed. *Intelligence and Military Operations*. London: Frank Cass, 21–32.
Hasswell, Jock. 1973. *British Military Intelligence*. London: Weidenfeld and Nicolson.
Henderson, David H. 1904. *Field Intelligence: Its Principles and Practice*. Melbourne: J. Kemp Government Printer.

Herman, Michael. 1996. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.
House of Commons Defence Committee. 2010. *The Contribution of ISTAR to Operations: Eighth Report of Session 2009-2010 HC225*. London: The Stationery Office.
Hughes-Wilson, John. 2004. *Military Intelligence Blunders and Cover-Ups*. London: Robinson.
Hundley, Richard O. 1999. *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the US Military?*. Santa Monica, CA: RAND.
Ilardi, Gaetano Joe. 2010. "IRA Operational Intelligence: The Heartbeat of the War." *Small Wars & Insurgencies* 21 (2): 331–358. https://doi.org/10.1080/09592318.2010.481429.
Intelligence Community Staff (ICS). 1977. *'Intelligence Definitions Working Group' CIA-RDP91M00696R000300020005-7, CIA Research Tool (CREST)*.
JDCC. 2003. *Joint Warfare Publication 2-00: Intelligence Support to Joint Operations*. 2nd ed. JDCC: Shrivenham, UK.
Joint Doctrine and Concepts Centre (JDCC). 1999. *Joint Warfare Publication 2-00: Joint Operational Intelligence*. Shrivenham, UK: JDCC.
Kahn, David. 2001. "An Historical Theory of Intelligence." *Intelligence & National Security* 16 (3): 79–92. https://doi.org/10.1080/02684520412331306220.
Kent, Sherman. 1949. Strategic Intelligence for American World Policy.*Princeton*. NJ: Princeton University Press.
Kerbaj, Richard. 2022. *The Secret History of the Five Eyes: The Untold Story of the Shadowy International Spy Network, Through Its Targets, Traitors and Spies*. London: Blink Publishing.
Kont, Markus, Mauna Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, and Anna-Maria Osula. 2018. *CCDOE Insider Threat Detection Study*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.
Lindsay, Jon R. 2013. "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations." *Journal of Strategic Studies* 36 (3): 422–453. https://doi.org/10.1080/01402390.2012.734252.
Mackenzie, Compton. 1931. *First Athenian Memories*. London: Cassell.
Magee, Aden C. 2011. "Counterintelligence in Irregular Warfare: An Integrated Joint Force Operation." *American Intelligence Journal* 29 (2): 16–23.
Melendez, Victor. 2019. "Counterintelligence: An Asymmetric Warfighting Tool for the U.S. Navy." *International Journal of Intelligence & CounterIntelligence* 32 (4): 737–769. https://doi.org/10.1080/08850607.2019.1621108.
Miler, Newton S. 1979. "Counterintelligence." In Godson, Roy, ed. *Intelligence Requirements for the 1980s Number One: Elements of Intelligence*. Washington DC: National Strategy Information Center, 47–60.
Mobley, Blake W., and Timothy Ray. 2019. "The Cali Cartel and Counterintelligence." *International Journal of Intelligence & CounterIntelligence* 32 (1): 30–53. https://doi.org/10.1080/08850607.2018.1522218.
National Commission on Terrorist Attacks Upon the U.S. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company.
NATO Standards Organization (NSO). 2019. *AAP-06 NATO Glossary of Terms and Definitions (English and French)*. Brussels: NSO.
Naval Intelligence Department (NID). 1921a. *Draft Minute to Treasury Chambers, 16 November 1919*. ADM 116/1462. The National Archive (TNA).
NID. 1921b. Naval Intelligence Organisation Abroad NID 10388/21 ADM 116/1842. TNA.
Odom, William E. 2003. *Fixing Intelligence for a More Secure America*. New Haven, CT: Yale University Press.
Office of the Director of Central Intelligence. 2023. Five Eyes Intelligence Oversight and Review Council (FIORC). [Accessed June 20, 2023]. https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

Olson, James M. 2019. *To Catch a Spy: The Art of Counterintelligence*. Washington DC: Georgetown University Press.
Parritt, Brian. 2011. *The Intelligencers: British Military Intelligence from the Middle Ages to 1929*. Revised ed. Barnsley, Lancs: Pen & Sword.
Phythian, Mark. 2013. *Understanding the Intelligence Cycle*. 2013. London: Routlege.
Posner, Richard A. 2006. *Uncertain Shield: The US Intelligence System in the Throes of Reform*. New York: Rowman & Littlefield Publishers.
Posner, Richard A. 2009. "Counterintelligence, Counterterrorism, Civil Liberties and the Domestic Intelligence Controversy." In *Vaults, Mirrors and Masks: Rediscovering US Counterintelligence*, edited by Sims, Jennifer and Burton Gerber, 261–280. Washington DC: Georgetown University Press.
Prunckun, Hank. 2012. *Counterintelligence Theory and Practice*. New York: Rowman & Littlefield Publishers.
Reijtens, Sebastiann. 2020. "Intelligence in Defence Organizations: A Tour de Force." *Intelligence & National Security* 35 (5): 717–733. https://doi.org/10.1080/02684527.2020.1737397.
Richelson, Jeffery T., and Desmond Ball. 1985. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries - United Kingdom, United States of America, Canada, Australia and New Zealand*. Boston: Unwin Hyman.
Rosen, Stephen Peter. 2010. "The Impact of the Office of Net Assessment on the American Military in the Matter of the Revolution in Military Affairs." *Journal of Strategic Studies* 33 (4): 469–482. https://doi.org/10.1080/01402390.2010.489704.
Royal Air Force Police. 2022. Counterintelligence and Security Squadron [Accessed October 25, 2022]. https://www.raf.mod.uk/our-organisation/units/counter-intelligence-and-security-squadron/.
Security Service. 1993. *The Security Service*. London: HMSO.
Shulsky, Abram, and Gary J. Schmitt. 2002. *Silent Warfare: Understanding the World of Intelligence*. 3rd ed. Washington, DC: Potomac Books.
Sims, Jennifer E. 2009. "Twenty-First Century Counterintelligence: The Theoretical Basis for Reform' in Reconceptualised." In Vaults, *Mirrors and Masks: Rediscovering US Counterintelligence*, edited by. Jennifer, Sims and Burton Gerber, 19–50. Washington DC: Georgetown University Press.
Tripodi, Christian. 2018. "The British Army, 'Understanding', and the Illusion of Control." *Journal of Strategic Studies* 41 (5): 632–658. https://doi.org/10.1080/01402390.2016.1196359.
United States Army. 1993. *Army Regulation 381-20 Military Intelligence the Counterintelligence Program*. Washington DC: Headquarters, Department of the Army.
United States Army. 1995. *Field Manual 34-60 Counterintelligence*. Washington DC: Headquarters, Department of the Army. See also HTML version of FM 36-40 held by the Federation of American Scientists. https://irp.fas.org/doddir/army/fm34-60/index.html.
United States Army. 2002. *FM 2-22-2: Human Intelligence Collector Operations*. Washington DC: Headquarters of the United States Army.
United States Marine Corps (USMC). 2000. *MCWP 2-14 Counterintelligence*. Washington DC: Department of the Navy, Headquarters United States Marine Corps.
Van der Bijl, Nick. 2013. *Sharing the Secret: A History of the Intelligence Corps 1940-2010*. Barnsley, UK: Pen & Sword.
Wallace, Robert. 2009. "A Time for Counterespionage." In *Vaults, Mirrors and Masks: Rediscovering US Counterintelligence*, edited by. Jennifer, Sims, 101–124. Washington DC: Georgetown University Press.
Warner, Michael. 2002. "Wanted: A Definition of Intelligence." *Studies in Intelligence* 46 (3):15–22.
War Office. 1943a. *Manual of Military Intelligence in the Field Pamphlet No.1 General Principles and Oganization*. London: His Majesty's Stationery Office. G.S. Publication. Copy provided by the Intelligence Corps Museum.

War Office. 1943b. *Manual of Military Intelligence in the Field Pamphlet No.3: Security. (Counter Intelligence)*. London: His Majesty's Stationery Office. G.S. Publication. Copy provided by the Intelligence Corps Museum.
War Office. 1922. *Manual of Military Intelligence in the Field*. 20 287/228, TNA.
War Office. 1946. *Manual of Military Intelligence*. WO 279/372, TNA.
War Office. 1947. *Manual of Military Intelligence: Pamphlet No.5 Counterintelligence: Civil Security and Counter Espionage* [sic]. WO 279/374, TNA
War Office. 1959. *Manual of Military Intelligence Pamphlet No.1 A Guide to Military Intelligence*. WO 279/375, TNA.
War Office. 1962. *Manual of Military Intelligence Pamphlet No.1 Intelligence Staff Duties*. WO 279/374, TNA.
Wells, Anthony R. 2020. *Between Five Eyes: 50 Years of Intelligence Sharing*. Oxford: Casemate.
Wolfberg, Adrian. 2016. "When Generals Consume Intelligence: The Problems That Arise and How They Solve Them." *Intelligence & National Security* 32 (4): 460–478. https://doi.org/10.1080/02684527.2016.1268359.
Zuehlke, Arthur A. 1980. "What is Counterintelligence?" In *Intelligence Requirements for the 1980s: Number Three Counterintelligence*, edited by Godson, Roy, 13–39. Washington DC: National Strategy Information Centre.