National Security Journal

http://nationalsecurityjournal.nz

Published by:
Centre for Defence
and Security Studies,
Massey University

ISSN: 2703-1926 (print) *ISSN: 2703-1934 (online)*

Commanders Requirements: What Do New Zealand Commanders and their Staffs Expect of Military Intelligence Officers in the 21st Century.

Author: Seabrook, J. G.

To cite this article: Seabrook, J. G. (2024). Commanders Requirements: What Do New Zealand Commanders and their Staffs Expect of Military Intelligence Officers in the 21st Century. *National Security Journal*. Published 25 September 2024. doi: 10.36878/nsj20240925.02

To link to this article: https: doi.org/10.36878/nsj20240925.02

View CrossRef data: http://search.crossref.org/?q=10.36878%2Fnsj20240925.02

Journal Article published 25 September 2024 in National Security Journal.

COMMANDER'S REQUIREMENTS: WHAT DO NEW ZEALAND COMMANDERS AND THEIR STAFFS EXPECT OF MILITARY INTELLIGENCE OFFICERS IN THE 21ST CENTURY?

J. G. Seabrook[1]

Military intelligence supports commanders, operations and planning staffs, and their evolving needs.[1] With few foundations for what is expected of military-intelligence officers in scholarly literature, this article attempts to determine what military-intelligence soldiers, planning officers, operational staff, and commanders expect of military-intelligence officers in the 21st century operating environment. Literature, training doctrine, and public resources provide no data or succinct analysis justifying how New Zealand military-intelligence officers comprehend what their roles required of them. This research surveyed New Zealand Defence Force personnel to determine what they believe is best military-intelligence practice. While commanders' preferences differ, doctrine indicates military-intelligence officers should train for the most likely situations, and therefore commanders' most likely expectations.[2] This article presents analysis of what is required to be a good military-intelligence officer.

Keywords: Military Intelligence, Intelligence Skills, New Zealand, Collection, Competence, Domain Relevance

Introduction

Conflict historians General Petraeus and Professor Roberts argue, "A general's staff requires some professional naysayers if it is to be effective."[3] Arguably, military training and expectations appear more likely based on doctrine and personal experiences, than

1 Major Jack Seabrook is an officer in the New Zealand Army. Contact by email: john.seabrook@nzdf.mil.nz. The author gratefully acknowledges the guidance of Dr Rhys Ball who supervised the original research project this article is based on.

on revolving – even if stated – contemporary intelligence-customer needs. There is currently no regular survey or audit to confirm intelligence-customer needs. It seems New Zealand military-intelligence officers have not considered validated if they are meeting customer needs in a formal, structured manner. This leaves open the possibility current teaching and intelligence support is out of synch with what supported elements want from their intelligence officers. By collecting, synthetising and presenting facts on intelligence user's needs, the next generation's military-intelligence officers can hone their trade and meet informed commanders' expectations. This should also set an expectation to confirm these requirements at regular intervals, in turn reducing the chances of not only training for the last or wrong war, but also providing timely, accurate, and relevant intelligence support.

Definitions

This research seeks to define what is required of New Zealand military-intelligence officers by their superior commanders, their colleagues, and their subordinates. Defining each group is important for understanding the motivations shaping intelligence-consumer needs. Notably, this research is focused on the New Zealand context, and thus all personnel – specific and/or hypothetical – are drawn from there unless otherwise stated.

Military-intelligence officers, or simply 'intelligence officers' from here forward, are commissioned military professionals, whose responsibilities focus on the direction of intelligence activities, collection, processing, and dissemination of information into intelligence, and any ancillary activities as they pertain to forces outside the positive control of friendly forces.[4] In this context, these officers are drawn from the Royal New Zealand Navy (RNZN), New Zealand Army, and Royal New Zealand Air Force (RNZAF). Intelligence officers lead enlisted specialists, who operate technical equipment or master collection and analysis of data to provide context, assessments, or decision advantage to an intelligence consumer.[5]

Australian doctrine defines the commander as the focal point of intelligence support, and the key individual driving the intelligence process.[6] Intelligence's relationship with operations and plans staff ought to be symbiotic as all three branches support the same focal point. Understanding both the operations officer's current needs in the conduct of operations, and the plans officer's needs forecasting future activities are thus essential in supporting the commander.[7] This research focuses on defining where intelligence officers should focus efforts to best meet expectations of the next generation's commanders, operations/plans staff, and intelligence personnel, herein referred to as 'intelligence consumers.'

Literature

The relationship between the military-intelligence function and the chain of command is not homogeneous.[8] This relationship has been the subject of several scholarly texts and histories.[9] Military-intelligence triumphs and failures gave the basis of academic understanding and the doctrine guiding training and operations.[10] While lessons from history are important, the intelligence cycle's first step is 'Direction,' suggesting training and operations should start by confirming what commanders want.[11] Military-intelligence generals Michael Hayden and James Clapper both noted how this step was often imprecisely applied, because decision-makers needed education on how to articulate needs for every situation.[12] Echoing their arguments that intelligence must, 'speak truth to power,' Geraint Evans notes, while commanders' specified desires are foremost, they also equally need intelligence staff as a 'conscience,' even when – as suggested by Petraeus and Roberts – the latter are charged to deliver undesirable information.[13]

There are seemingly basic knowledge and literature gaps in articulating what commanders want. Bruce Berkowitz argues this literature gap widens as globalisation and the Information Age change society's expectations of how information should inform decision-making about increasingly fluid threats.[14] This gap in defining what commanders want becomes more complex when factoring in growing pressures for non-traditional roles, like gleaning intelligence from financial information taken during site exploitation.[15] A growing body of literature notes battlespaces' increased complexity, such as future reliance on open source intelligence (OSINT) and concepts of "Intelligentized warfare."[16] This is not accompanied by analysis on what intelligence officers are expected to do to meet these complexities.

In 2020, New Zealand Major General John Howard, then Deputy Director of the United States Defense Intelligence Agency (DIA), argued for transformation of the intelligence profession. He highlighted four attributes for contemporary intelligence professionals to prepare for leadership responsibilities by 2040: "awareness of complexity; focus on effects; comfort working in teams; and agility."[17] Intelligence officers should thus understand the nature of complex systems as they collect, process, and analyse data. That understanding should update collection focuses, information selection, processing and analysis speed, and certainty levels.[18] Here Howard argues for new expectations of intelligence officers, but without scholarly data to base his argument.

Several scholars note contemporary operations have created new demands of all commanders and their staffs. Smith argues staff-planning should be founded on effects-based thinking, requiring, "the full range of political, economic, and military actions a nation might undertake to shape the behaviour of an enemy, would-be opponent, or even allies and neutrals."[19] That range creates new considerations when defining any

problem and subsequently solving it. Effects-based thinking must be enabled through network-centric capabilities. These, Alberts, Gartska, and Stein argue, are essential for improving and synchronising information-sharing and situational awareness across a networked force.[20] This network centricity almost certainly affects New Zealand as it moves towards its Network Enabled Army concept, or the Joint Forces Commander's 2025 goal of a "truly networked combat force."[21] Confirming what intelligence decision-makers require for effects-based thinking and network-centric capabilities should thus become foundational requirements for contemporary intelligence officers.

Often doctrine refers to "commander's requirements" to support planning and decision-making processes.[22] But neither doctrine nor scholarly analysis seemingly relies on quantitative analysis for this. Primary sources, however, often explain what intelligence support leaders want. Brigadier Hugh McAslan, then New Zealand's Chief of Defence Intelligence, noted in 2020, intelligence staff, "must evolve – often at the same rate commercial companies enhance their open-source and data outputs to expand market share."[23] The Economist has reinforced this view in several articles.[24] In 2016, National Security Group leader Howard Broad publicly identified counter-terrorism and economic priorities he needed intelligence professionals to prioritise.[25] By virtue of military intelligence's integrated role in the National Security System (NSS), understanding military intelligence's non-military customers creates a national context, but also indicates influences on other New Zealand security agencies. McMaster also mentions satisfying commander's requirements repeatedly, without explaining those requirements' origins. This seems symptomatic of literature, especially among military scholars, who assume shared understanding not squarely founded in data.[26]

From the 2006 Iraq campaign of Joint Special Operations Command (JSOC) General Stanley McChrystal, Special Operations Forces (SOF) commanders integrated intelligence staff differently to more effectively counter contemporary insurgent threats, compared to state-actor threats like the Iraqi Army. A contemporary literature review indicates SOF intelligence officers became equal counterparts for operations officers during modern conflicts.[27] ISTAR[28] doctrine argued for seamless transitions from intelligence to operations staffs twenty-five years ago, although this greater equality in fact took 10-15 years to come to fruition.[29] McChrystal noted how contemporary asymmetric adversaries relied on massive amounts of data, which modern intelligence officers needed to intercept, process, and understand.[30] He identified all-source intelligence officers and analysts as a requirement in modern warfare over the single-source collectors endemic to 20th Century conflicts. Cline detailed how SOF also expanded intelligence responsibilities to continually update general-area studies, psychological-operations estimates, and civil-military-operations estimates.[31] This expansion – and intelligence staff's increased prominence in operations planning – saw intelligence skills delegated to whomever would be best placed to use them.[32] McChrystal and his intelligence officer Michael Flynn gave SOF operators more on-objective exploitation skills to expedite

operations in Iraq, changing JSOC functions long term.[33] This potentially changed how some intelligence consumers wanted to be involved in the intelligence cycle, creating expectations of greater integration.

Lowenthal's seminal work *Intelligence: From Secrets to Policy* provides context for top-down intelligence needs, and military intelligence's integration into broader systems. But it is an imperfect match for specifying tactical and operational intelligence-support needs. [34] Similarly, Hughes-Wilson writes from practical experience as a military-intelligence officer and scholar.[35] Unlike Lowenthal, Hughes-Wilson writes of specific intelligence techniques, such as developing indicators to track and pre-empt adversary actions.[36] Hughes-Wilson's publishing in 2016 and his 1970s experiences, however, suggest his analysis lacks some contemporary relevance.

International sources discuss training necessary for military-intelligence growth and cross-specialisation primarily focused on American needs,[37] and thus have limited applicability for New Zealand.[38] Other articles identify specific competencies like targeting and collection-planning.[39] Flynn argued for centralising 'hungry analysts,' employing "proactive information brokers," and centralised stability-operations information centres – though Blanken & Overbaugh argue against Flynn's unsubstantiated challenges to Cold-War military-intelligence structures.[40] Neither Flynn nor Blanken & Overbaugh rely on quantified consumer-preference data for their arguments.[41] Meanwhile, H.R. McMaster *et al.*, argues intelligence personnel must train in languages, urban considerations, social-information requirements, cyberspace, and developing technologies.[42]

Broad analysis of current literature suggests an overall hypothesis that commanders and their staffs want military-intelligence officers with greater knowledge and skillsets than traditionally taught. This research thus tested the propositions that commanders want: [43]

1. Only vital intelligence and especially significant planning considerations;
2. Insightful answers to their questions;
3. Intelligence officers to understand friendly-forces combat capabilities to aid thorough planning;
4. Intelligence officers able to prove their collection and analysis methodologies; and,
5. No intelligence considered interesting but irrelevant.

Method

This research aimed to provide current New Zealand military-intelligence officers empirical data to inform training and capability-development. In considering the method for finding out what commanders want; the plan was to ask them. A wide survey pool chosen from New Zealand Army Regular Force personnel ensured insight based on respondents' military-intelligence experiences and needs on operations. Free-form survey responses contextualised responses.[44] Primary- and secondary-source materials

acted as evaluative research, challenging stakeholders' biases with SOF examples.[45] As a result of survey responses, real-time aggregated data provided insights the NZDF can consider or act on.

Limitations

The NZDF's size and operational tempo made data collection difficult. Initially, both intelligence and combat respondents responded strongly. Respondents represented New Zealand's three services: 10.34% RNZN; 63.22% New Zealand Army; and 26.44% RNZAF. All but one respondent were regular force, and the exception was an ex-regular force reservist. The New Zealand Army is twice the Air Force and Navy's sizes with a more mature intelligence capability. The Army's historic dominance in the trade likely explained the Army's greater response rate.

Defining trade was left open-ended, to allow for differences between officer and enlisted ranks. Thirty-six respondents (42.38%) self-identified as intelligence officers or enlisted personnel. Nine respondents (10.34%) were combat support (engineers, communications, or artillery) or combat service support (logistics). Twenty-seven respondents (30.89%) identified as combat trades.

The survey pool provided a reasonably well-rounded balance of personnel that either produce or consume intelligence, with a higher representation of mid-ranked personnel with lived operational experience.

The median percentages demonstrated most respondents had completed one-to-three deployments: one, 15.91%; two, 20.45%; and, three, 25.00%. Responses on deployment lengths and numbers suggested the majority of respondents had some or significant operational experience. Similar statistics confirmed confidence for employing an intelligence staff. When ensuring respondents were appropriately familiar working with or relying on intelligence, only three respondents suggested they had rarely or never had intelligence support on operations. Meanwhile 56.47% had always had intelligence support.

In determining which intelligence disciplines respondents had exposure to, one survey question saw more than 80% of respondents had experience using OSINT, GEOINT, and surveillance & reconnaissance. Meanwhile over 50% of respondents had experience with Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and the analytical disciplines of all-source, fusion, and combat intelligence.[46] These results suggest which disciplines are seen to more broadly meet customer needs. It might also indicate where some respondents are unaware of intelligence woven into understanding without necessarily being explicitly stated – such as SIGINT's influence on an analyst briefing at a lower classification.

Finally, 66.28% of respondents believed they could employ intelligence very or extremely professionally. Concerningly, 29.01% of respondents noted only being able to 'somewhat professionally' employ intelligence, and four respondents felt professionally unable to employ intelligence. Given the respondent pool's bent towards officers (and thus leaders) and intelligence professionals, this could very much suggest an area of operational concern in the effectiveness of intelligence-led/intelligence-enabled operations.

Findings

Holistic themes

The data collection provided several consistent themes in intelligence-customer demands for "real-time" intelligence, especially accurate, concise, and timely information. These matched doctrinal explanations of intelligence's role.[47] Customer needs for intelligence officers' professional networks across agencies and partners nations was also ranked highly. This trend indicated a desire for intelligence officers to not necessarily know everything, but rather know where and who to go to for specific answers. Competence as a professional trait was a common theme throughout responses. More specifically, respondents wanted highly competent intelligence officers who were well-integrated into operations staffs and commanders' working cycles. Part of that competence seemed to indicate respondents wanted intelligence officers deployed forward but with the skills and resources to reach-back to New Zealand and into coalition and ally networks for information. One respondent noted they required the whole network from forward elements "at the tactical edge," integrated through both collection and analytical roles into all available sensors as well as strategic and Five Eyes (FVEY) resources, databases, and tasking authorities. This comment led a holistic theme desiring all relevant intelligence possible from well-connected networks.

'Domain relevance' emerged as a common holistic theme also, especially among air-force respondents most concerned with locating surface-to-air threats. The survey data noted 78.32% of respondents disagreed with oversimplifying intelligence officers into joint skills only, with nearly 80% of survey respondents believing there should be some form of clear distinction between maritime, land, and air intelligence officers. Interestingly, almost the same number of respondents (73.08%) opposed the notion that intelligence officers across maritime, land, and air domains all have the same skills. Comparable trends opposed there being only non-service-aligned 'joint' intelligence officers able to support all domains: 53.16% opposed and 29.11% strongly opposed.

Domain specialisation is almost specifically needed to make wide-ranging intelligence knowledge relevant to the supported intelligence customer. Air Force intelligence officers are more likely to anticipate a pilot's needs and provide insights as part of their systematic checklist approach to planning. Army officers meanwhile need more abstract

insights and opportunities to weigh for the cost/benefit of a manoeuvre. The data perhaps suggests an expectation of broad knowledge from a specialist who understands the culture, procedures, and operational goals of their intelligence customers. However, freeform survey responses supported the idea of some common training, in part to find efficiencies but also to inculcate networking skills and awareness of the tri-service domains early. Similarly, the majority of respondents supported the contention that all intelligence officers should understand the other domains' intelligence collection capabilities and requirements, even though they should primarily be specialised to their own domain.

This domain specificity seemed to lend support to another early theme that intelligence support should also predict where information would be useful and then proactively inform long-term deliberate planning as much as answer short-notice requests for information. This theme presages a requirement for expansive knowledge of where any given information might be of most value across the NZDF and the National Security System (NSS). It also portended a later theme indicating a strong desire (75.65%) for intelligence officers who were flexible and able to do anything asked of them in any tactical, operational, or strategic context.

In negation, several competencies and traits were identified for exclusion, among them were countervailing points like a desire to avoid 'incompetence'. Some very specific, personal experience of incompetence was provided in free-form answers stating respondents did not want intelligence support that enabled "disconnected intelligence projects not aligned to the operational outputs or commanders' intent;" "strategic perspectives in tactical spaces[;]" and an "Over-saturation of irrelevant or redundant information." Another theme of incompetence owing to misaligned expectations, exposure, and experience appeared, especially in the efficient tasking of collection assets and diligent dissemination of useful information.

Notably, a few respondents also discussed poorly managed access to intelligence. Examples included intelligence staff withholding information from people needing it, and single-source collectors going straight to commanders – and arguably offering too much or irrelevant information. Three respondents specifically referred to not wanting to "deal with HUMINT personnel," but wanting their product in an all-source assessment. This aversion to human-intelligence teams is especially notable given its contrast to a desire for better social skills – the primary value proposition of such teams. This suggests some specialist collectors will wish to prove their capabilities' worth by report quantity, rather than matching commanders' and staffs' desires for their work to inform well-reasoned and acutely relevant analysis. These aversions to HUMINT teams and to intelligence staff "silo-ing" information into disconnected teams, probably suggests intelligence officers need to know how to distribute information widely and properly credit contributing agencies.

A common respondent expectation for intelligence officers to weave "emotional intelligence skills" – or an aptitude for gaining trust and communicating – into more formal support suggests how some frictions may be addressed. Survey data resoundingly reinforced the notion that high emotional intelligence and social skills were essential. The survey data favoured balancing intelligence officers' roles with their operations counterparts. A majority of responses reinforced the preference for well-rounded intelligence officers, with equal rank and competence as operations officers - agreed (44.87%) or strongly agreed (28.21%). Contemporarily, SOF headquarters hold "Operations & Intelligence" briefs, balancing the inherent value of the problem-setter (intelligence officer) with the problem-solver (operations officer).[48] New Zealand survey respondents confirmed the desirability of this approach. A total of 83.11% favoured the proposition that chiefs of staff should evenly balance intelligence and operations officers. Similarly freeform responses indicated a preference for intelligence officers to offer tactics to beat threat groups, suggesting a more proactive role in helping operations officers. This matches what McChrystal and Flynn argued for, though it contravenes the best practice intelligence generals Hayden, Clapper, and Howard believe should see intelligence officers refrain from any operational advice.

Knowledge

To better determine which knowledge sets intelligence consumers expected from contemporary intelligence officers, a range of questions tested specific skills. This allowed a better understanding of what respondents believed was relevant and irrelevant, thus proving or disproving part of this research's hypothesis. Overall, respondents expressed a desire for knowledge, skills, and aptitudes quite likely beyond a single individual's capability and capacity. This reiterated the need for the NZDF to take a network approach where, at the very least, every intelligence officer is aware of what deep knowledge their peers have. The expected knowledge sets suggested Defence Intelligence ought to consider clearly tasking and coordinating which officers have which deep knowledge.

When asked to check all relevant knowledge an intelligence officer should have, all twenty-five competencies, at Table 1, were selected as important by at least half of all respondents. When measured, having all the skills seems likely beyond any one individual's ability – a reality later expressed in respondent answers. This balance suggests a significant gap between preferred skillsets and what is realisable. Arguably these data more realistically necessitate broad familiarity with each subject, some deep knowledge and then an active role in a collegial network of intelligence professionals. Some later freeform commentary argued general understanding was more appropriate than 'a detailed knowledge'. Some suggested 'detailed' knowledge of all threats was unrealistic. These points give pragmaticism to the high response rate. As priorities for all intelligence officers, however, the five highest response rates unsurprisingly indicated a

preference for: an ability to contribute to operational plans and courses of action development; a detailed knowledge of threat group capabilities; and a working knowledge of how to find contacts in any intelligence agency. In short, survey respondents clearly identified generalist skills over intelligence skills in their expectations.

ANSWER CHOICES–	RESPONSES–
A detailed knowledge of threat group capabilities	96.25%
A detailed knowledge of all national intelligence capabilities	76.25%
A detailed knowledge of maritime threats	58.75%
A detailed knowledge of land threats	67.50%
A detailed knowledge of air threats	61.25%
A detailed knowledge of space threats	52.50%
A detailed knowledge of cyber threats	58.75%
A detailed knowledge of information domain threats	66.25%
A detailed knowledge of friend forces capabilities	71.25%
Knowledge of friendly weapons and vehicles employment ranges	62.50%
Knowledge of a commander's background, qualifications, and experiences	62.50%
Knowledge of a commander's biases	61.25%
Knowledge of a commander's preferences	75.00%
An understanding of an operations officer's professional requirements	73.75%
An ability to contribute to operations management and concepts of operations	90.00%
An ability to contribute to information operations plans and management	85.00%
An understanding of a plans officer's professional requirements	60.00%
An ability to contribute to plans and course of action (COA) development	97.50%
An understanding of communications operating requirements and threats	71.25%
An ability to identify emerging technologies that may enhance friendly force capabilities	55.00%
An ability to identify intelligence that should inform training or update SOPs.	83.75%
Networks of contacts across all NZDF intelligence units	90.00%
Networks of contacts across all NZ intelligence agencies	76.25%
Networks of contacts across all FVEY intelligence agencies	77.50%
Working knowledge of how to find new contacts across any intelligence agency	91.25%

Table 1. Preferred knowledge among survey respondents.

Surprisingly, respondents showed a stronger preference for interoperability with operations and planning processes over detailed knowledge of domain-specific intelligence considerations. Contributing to team efforts seemed more important than high intelligence-tradecraft competence. Likewise, emotional-intelligence skills like intuiting

commanders' requirements through a thorough knowledge of their preferences, biases, and history ranked comparably with threat knowledge. These data largely reinforce a preference for strong generalist-officer skills. By questioning preferences for specific skills, such as contributing to staff products like concepts of operations and course-of-action development, these data identified key learning objectives intelligence-officer training should focus on. With such a strong preference for integration into broader systems, operations and plans officers have shown which generalist skills will meet their expectations. When later asked what else military-intelligence professionals should be able to do, respondents confirmed a strong desire for generalist-officer skills to command, lead, manage, and fulfil plans and operations roles. A minor trend emerged specifically denoting intelligence officers should have the skills required for planning and conducting operations – a further generalist skill that should be enhanced as part of intelligence-officer training.

The survey sought to delineate what knowledge intelligence officers should have of their own forces versus adversarial forces. Commonly, friendly-force knowledge is excluded from intelligence training as priority is placed on understanding threats groups in greater detail. However, nearly three quarters of respondents (72.5%) favoured intelligence officers having a detailed understanding of all friendly-force combat capabilities. This likely indicates an opinion that to support a capability credibly, an intelligence officer must first understand it. This figure dropped slightly to 64.1% in expecting detailed understanding of combat-support capabilities, while 19.23% disagreed. Interestingly, the figures swung further for intelligence officers' understanding of friendly forces' combat-service-support capabilities with 46.83% in favour, but a significant increase in disagreement to 25.31%. These weightings alone could shape how intelligence staff are trained, with a proportional focus more heavily on combat needs than on combat-support (artillery and engineering for example), and combat-service-support (logistics) needs. Importantly though, current doctrine which excludes training to understand friendly forces appears to be challenged by more contemporary preferences from commanders, operations and plans staff.

Meanwhile in confirming doctrinal focuses on threat knowledge, the research balanced expectations based on training and actual intelligence support. Almost equal portions of respondents agreed (33.77%) and disagreed (35.06%) intelligence officers should be knowledgeable on any threat group at any time – regardless of what intelligence priorities a commander might have set. The proposition was worded to challenge respondents on how broad officers' knowledges should be. It is unrealistic to expect one individual to have a detailed knowledge of all the world's threat groups, or even just all the threat groups in New Zealand's most likely operational areas – New Zealand, South West Pacific, South East Asia, and the Middle East.[49] Among the overall 37.67% who agreed, however, freeform responses suggest they wanted intelligence officers well-versed in the World's current threat groups as a matter of professional training and education.

In comparison, when moderated by a proposition for familiarity to current affairs as opposed to 'detailed knowledge,' 93.59% favoured intelligence officers being well-versed in current affairs. When the survey narrowed general-knowledge preferences, 38.46% strongly agreed and 51.28% agreed intelligence officers should be well-versed in all geopolitical situations of concern. This kind of broad understanding suggests intelligence focus areas should come either directly from a commander's requirements, the National Security Intelligence Priorities (NSIPs),[50] by implication of government policy documents like the Strategic Defence Policy Statement 2018, or through the professional networks respondents also preferred.[51]

Meanwhile, in narrowing the focus of intelligence training ahead of operational suport, the survey found 77.92% of respondents favoured intelligence officers having a detailed knowledge of threat-group weapon systems. It stands to reason technical knowledge of weapons systems is essential to meaningfully contributing to planning. Technical data on weapons systems also enables an understanding of a force's risk profile. Higher still, 88.31% favoured intelligence officers having a detailed knowledge of threat-group behaviours. This almost certainly owes to threat-group behaviours – or rather assessments on the willingness or intent to use a specified weapon – being an intelligence officer's primary contribution to military planning.

Future knowledge

The need for tech-savvy intelligence officers is becoming more prevalent in several sources of analysis.[52] Where once technical proficiency for current capabilities was enough, literature and this research indicate a desire for knowledge of future and emerging technologies available to both friendly and adversary actors. The optimal conditions for artificial-intelligence (AI) collection, big-data exploitation, and even the precise language around techniques must be established on a strong foundational understanding of how to put them all to the best use in millitary intelligence and operations.[53] Emerging and disruptive technologies – particularly biotechnology, quantum computing, cloud computing, graphics processing units, AI, machine learning algorithms, computer vision, natural language processing (NLP) and space – and their applications are all relevant for New Zealand's foreign policy, economic competitiveness, and military and intelligence operations.[54] Thus, it stands to reason contemporary intelligence officers should be proactively learning about each technology in order to advise leaders at any level on how to best use it.

The skills to implement data-analytics solutions include comprehension of coding and computer science. However, respondents showed a clear preference that intelligence officers should not need coding competence. This creates an interesting paradigm, and suggests respondents prefer intelligence enlisted personnel be proficient coders and technical innovators, but officers should only have a good general knowledge of the skillset and its lexicon. Similarly, when confirming expectations of OSINT skills, more

respondents were opposed to (38.96%) than in favour of (33.76%) intelligence officers collecting OSINT as competently as soldiers. These data align with the general collection-and-analysis-skills proposition, suggesting OSINT skills are viewed similarly to analytical skills.

ANSWER CHOICES–	RESPONSES–
Cyber warfare	88.16%
Information operations	93.42%
Joint operations	94.74%
Emerging Technologies	75.00%
Counter-terrorism considerations domestically	63.16%
Counter-terrorism considerations internationally	80.26%
Chemical, Biological, Radiological and Nuclear Warfare	60.53%
Science	27.63%
Economics	35.53%
NZ Strategic interests in Asia	85.53%
Pacific Regional Security	94.74%
Middle East Regional Security	51.32%
North African Regional Security	43.42%
Potential deployment locations	85.53%
New collection techniques	86.84%
New ISR platforms	86.84%

Table 2. Preferences for future intelligence knowledge sets.

National Security issues	96.05%
New Zealand domestic security issues	69.74%
Climate Change	46.05%
Non-traditional security (Health) issues	50.00%
Civilian-Military Relations	61.84%
All of Government approaches	78.95%

Table 3. Preferences for non-traditional intelligence knowledge sets.

When asked what subjects intelligence officers should be familiar with in the future, 90% of respondents chose joint operations, information operations, and Pacific Regional Security. Cyber warfare, counter-terrorism internationally, New Zealand's strategic interests in Asia, potential deployment locations, new collection techniques, and new ISR platforms were all high priorities for 80% or more of respondents – the latter two also support literature arguing for greater emerging-technology knowledge. Notably, a familiarity with science, economics, the Middle East, and North Africa all ranked low. Future development outside of traditional roles highlighted a high desire for intelligence officers to be familiar with New Zealand national-security issues (96.1%) and all-of-Government approaches to dealing with them (79.22%). Domestic security issues (normally outside NZDF responsibilities) still resulted in 68.83% of respondents in favour of some familiarity, no doubt in part shaped by the NZDF's recent roles responding to disasters, pandemics, and major events. Climate change and non-traditional security issues, like health, scored lower in this consideration with only 46.75% and 50.65% of respondents in favour. These data thus suggest the NZDF should put time and resources – preferably in training or structured secondments – into increasing intelligence officers' awareness of national-security issues and how the NSS will approach them.

Meanwhile, more targeted questions on future knowledge saw strong majorities for better legal, compliance, and risk-management knowledge relating to intelligence. There was a strong preference (80.52%) in favour of a detailed knowledge of intelligence-operations law – the legal frameworks and considerations shaping how intelligence operations must be lawfully conducted. These are modern aspects of intelligence activities, but doctrine currently lacks training these critical enabling factors into the next generation. A detailed knowledge of risk management was also favoured by a majority, with 68.83% agreeing this was an important intelligence-officer competency. A similar number (65.79%) of respondents agreed intelligence officers should have a detailed knowledge of compliance legislation. A majority rejected the proposition intelligence officers should be responsible for all intelligence-operations risk management, however. The low number in favour (16) suggests even among the survey's intelligence staff (42.38%), few believed they should wholly control intelligence operations. One respondent later noted (possibly owing to this question's recency) intelligence officers should not, "Accept risk that is not theirs to accept." These data provide a useful counterpoint to misinterpretations of McChrystal's rebalancing of intelligence- and operations-officer roles. Many interpret McChrystal's arguments for "intelligence-led operations" to mean intelligence officers directing operations.[55] Survey feedback highlighted a preference for 'intelligence-enabled operations,' seemingly a better term when meeting expectations for humble, collegial, and useful contributions to operations planning and execution. Notably, several respondents commented intelligence officers should not be subordinate to operations officers. The data also suggested any risk management ultimately falls to commanders alone and should not be delegated to any specific principal staff officer.

Further, respondents' comments matched several scholarly analyses and public discourses' suggestions for the focus of future intelligence capabilities.[56] Space, AI, and 'using technology to expedite big data analysis,' all ranked highly. Other skills mentioned included languages, anthropology, climate change, counter-intelligence, critical thinking skills, and economic warfare – the last of which was contrary to low preference for economics skills. This likely leaves several aspects for future detailed analysis and review.

Knowledge, Skills, and Aptitude

Overwhelmingly respondents agreed or strongly agreed (81.02%) intelligence staff should know of all friendly-force activities in their area of operations – similar to the 72.5% of respondents who favoured a detailed understanding of friendly-force combat capability. The implication is surely that to support a commander, their units, and their role in a higher plan, knowing how the supported elements are operating is critical to informing them. An overwhelming majority (92.5%) agreed intelligence staff should know what all maritime, land, air, and joint intelligence personnel are collecting and analysing in and around their area of operations. This suggests a strong expectation intelligence staff as a team understand what intelligence operations are under way and where intelligence will be readily available.

Graph 1. Survey respondents' preferences for what intelligence officer should know.

While being domain-specific was important to respondents, a professional network across all domains' intelligence staffs is also judged important. These values, however, dropped markedly when questioning a detailed knowledge of intelligence capability by domain. A total of 59.49% of respondents favoured knowledge of air intelligence collection capabilities being very well understood by contemporary intelligence officers. A similar majority (54.43%) favoured all intelligence staff should have a detailed knowledge of maritime collection capabilities. Meanwhile 68.36% agreed or strongly agreed all intelligence staff should have a detailed knowledge of strategic intelligence collection capabilities. Knowledge of intelligence collection requirements largely followed the same trends. The correlation of 'detailed knowledge' expectations, suggests most respondents would prefer all intelligence staff be familiar with collection capabilities regardless of domain. However, there was subsequent context from freeform responses that a detailed knowledge of all three domains may be unrealistic, and access to a detailed knowledge – through a professional network – may suffice.

Similar to stronger general staff-officer skills, all but three respondents agreed intelligence officers should continually update a threat situation. While an obvious response for a profession focused on emerging and evolving threats, this data point suggests current threats and more importantly vital intelligence should form a greater focus than deeper analysis or specific target development. Doctrinally, intelligence branches have current intelligence officers (J23) to support operations staff, while still allocating resources to future intelligence and plans (J25) or deeper analysis (J22).[57] To balance this overwhelming desire for continuous threat situation updating, 30% of respondents agreed intelligence officers should only update vital intelligence immediately relevant to operations, however, 56.25% were opposed, suggesting more nuance that likely covered the 'especially significant planning considerations' the research proposition included, was still required. The majority's disagreement suggests some understanding that foundational data sets and greater depths of knowledge proactively inform a current threat picture. The 30% portion of responses focused on only updating vital intelligence could suggest the need to exclude 'interesting' information or atmospheric intelligence. Further survey comments identified an expectation for sound judgment in identifying vital intelligence and the confidence to communicate.

When considering intelligence responsibilities other than judgement and context-based vital intelligence, the survey tested which areas respondents thought should be handled without wasting commanders' time. Data suggested intelligence officers should minimise an overt focus on security and counter-intelligence work, while reassuring supported commanders that standards and processes are well-established and adhered to. This is a fairly clear sign the bulk of counter-intelligence responsibilities should take minimal command attention.

Intelligence skills

When breaking down which skills intelligence officers should have, a broad theme became apparent. Where the NZDF's size has made it necessary for officers and soldiers to have interchangeable skills, responses suggest the preference for the future is for broadly knowledgeable officers enabled by enlisted deep specialists. This would likely shift intelligence-officer profiles to be more socially relatable to their unit and wider professional networks, and less technically focused. Simultaneously, it could create the space necessary for enlisted specialists to flourish, innovate, and excel while officers are less directly involved in collection and analysis processes.

The survey asked how many practical intelligence skills intelligence officers should have. While officers should have strong skills for coordinating collection and intelligence priorities, the technical skills they should have are not as clear. This difficult balancing act was variously highlighted in both freeform and Likert data sets. Respondents believed some technical skills were necessary to credibly employ and command intelligence capabilities, but they also clearly stated a desire for intelligence officers to leave collection and analysis to enlisted ranks. Arguably an easy solution for collection skillsets is being trained in them, without the same exposure and experience as enlisted personnel in applying those skills. This research also found the majority agreed (61.54%) or strongly agreed (20.51%) intelligence skills should permeate non-intelligence roles, devolving skills to on-the-ground operators.

The NZDF is small, and thus has traditionally necessitated crossover in intelligence roles. Where the RNZAF kept enlisted ranks as collection specialists and officers as all-source analysts, the Army comparably trained officers and soldiers on combat-intelligence skills. Respondents were evenly split with 33.33% in agreement and 35.9% opposed to officers being upskilled to collect and analyse to the same degree as intelligence soldiers. Nearly an equal portion 30.77% neither agreed nor disagreed, suggesting more specifics would determine this preference. While this does not provide a definitive expectation, it reinforces the ambiguity previously highlighted. Given some intelligence professionals must have either agreed, disagreed, or abstained given their 42% self-identification, it seems likely there is no agreement among practitioners. Interestingly, 57.14% disagreed with the proposition that intelligence officers and enlisted personnel should be interchangeable on operations – this suggests opinions on comparable skills do not extend to comparable officer and enlisted employment of those skills on operations.

To determine more specific expectations, the survey sought to identify which skills should be focused on and avoided. A total of 45.45% opposed intelligence officers having the same exploitation skills as enlisted personnel, compared with 25.98% in favour. This was a 12% increase in opposition compared to the more general proposition. How-

ever, this percentage then switched back in line with the general proposition, when respondents considered intelligence officers being trained to analyse collected exploitable material comparably to enlisted personnel. Here the responses were nearly equal again: 36.84% opposed, 32.9% in favour. This, along with the majority against coding skills, suggests officers should not have technical collection skills to exploit data. However, officers should be comparably trained to analyse data, probably as a means of incorporating intelligence into planning and operations processes and being able to articulate this to commanders.

In directly testing the proposition that officers should be kept from technical aspects of intelligence production, 50.44% opposed intelligence officers being limited to leading capabilities, not conducting collection and analysis. This suggests respondents still want the flexibility to employ intelligence officers broadly. Thus, intelligence officers should have collection and analysis skills, but not to the same technical proficiency as their specialists. This matches most military disciplines, though notably contravenes HUMINT officers qualifying on all the same courses.

Freeform responses suggested officers should have leadership and some technical skills, owing to the NZDF's size. Some technical skill was seen as necessary for credibility and effective management. In discarding language skills, one respondent argued officers need to employ people with these skills then ensure their own credibility and competence.

> What is essential is intelligence officers employ the collection assets, [Processing, Exploitation, and Dissemination], and analysis persons appropriately. Military-intelligence officers should be able to provide robust enemy assessments, then aid commanders in achieving location intelligence or positive identification. [They] should enable command by leading capabilities in the collection of intelligence to inform operations.

When asked what intelligence officers should be barred from, freeform responses suggested only activities where they would be overstepping their responsibilities – like tactical decisions and coordinating operations. Over-involvement in analysis and exploitation arose, though may have been biased by the questions. "Nothing" was one of the most common responses, suggesting further evidence of a desire for intelligence users to maintain flexibility in any operational environment. In this vein, a later proposition noted only three respondents were in favour of limiting intelligence officers to integration roles.

Lastly, freeform answers resulted in some 'skills' trends expressing an expectation intelligence officers should be trained to effectively communicate both in writing and verbal briefs. These 'skills' extended to social intelligence, collegiality, and a sense of humour, indicating possible reinforcement of Flynn's desire for proactive "information brokers"

pushing information across their peers, partners, and allies, while coordinating future work. Thus, intelligence-consumer data here updates Blanken and Overbaugh's Cold-War skillsets with quantified measurements. The links between these two trends, suggest communication skills should range so information can be informally presented or raised during broader staff processes.

Conclusion

The survey data confirmed the propositions of this research's hypothesis. Likert data and freeform responses confirmed 'vital intelligence' as a priority and the negation that intelligence officers should avoid information that is not immediately useful. Furthermore, commanders and their staff clearly want only insightful answers to their questions – notably summarised as "news you can use." The research also suggests detailed knowledge of risk management, compliance legislation, national-security issues, all-of-Government approaches, and domestic security issues should become part of intelligence-officer training. Each further complicates the NZDF's ability to prioritise skillsets. Those priorities as well as the other 25 strongly-supported competencies suggest the NZDF will have to innovate cleverly if it wants to maintain a network of the skillsets intelligence users want. Ensuring the NZDF cultivates skills with a view to its national integration will be vital for achieving the expectations this research found among respondents.

Meanwhile, survey respondents broadly understand intelligence officers cannot have a detailed knowledge of all competencies and yet 75% of the same respondents identified 13 of 25 competencies as fundamentally important. This was balanced by lowered expectations of 'detailed knowledge' of each operational domain with a more 'general understanding' – high expectations dampened by only pragmatism. Regardless, fundamental to enabling commanders, intelligence officers must understand friendly-forces combat capabilities in enough detail to benefit thorough planning. Combat officers are not expected to achieve the same technical competence as their enlisted personnel but they should completely understand the capabilities – an alignment intelligence professionals should follow. Likewise, intelligence officers should be able to prove their collection and analysis methodologies. This builds credibility, but the act of trusting subordinates creates more space to collaborate collegially with peer staff-officers.

This research clearly reinforces the view that commanders do not want intelligence considered interesting but irrelevant. This negation was probably the most commonly referenced theme. In recognising lacking time and resources, the survey data suggested intelligence officers should understand their supported commander, platform, and mission, and align all intelligence outputs to them. A joint approach to foundational training would help this, by better preparing intelligence officers, their networks, and their cross-domain familiarity before they specialise.

Lastly, intelligence officers will have to find a way to balance often conflicting expectations from superiors, peers, and subordinates. On one hand, they must, "First and foremost, plan and lead intelligence collection and analysis across the Joint spectrum," but a key recommendation would be enhancing intelligence officers' generalist skills above normal expectations. Their mastery of staff processes coupled with flexibility and intentionally-developed professional networks across the NZDF, government agencies, and the FVEY, are what intelligence consumers want.

---

1 Australian Army, *LWD2-0: Intelligence*, 7; US Army, *ADP 2-0: Intelligence,* 2-1 (page 29); Army Doctrine Publication, *Land Operations* (Shrivenham, UK: Director General Development and Doctrine, 31 March 2017),193, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf, accessed 04 April 2021; US Army *Field Manual FM 34-36*: *Special Operations Forces Intelligence and Electronic Warfare Operations*, available at https://www.globalsecurity.org/intell/library/policy/army/fm/34-36/pef.htm#iv (accessed 10 October 2021.)

2 H.R. McMaster, Scott Berrier, Kevin Mangum, and Richard Davis, *The US Army Functional Concept for Intelligence 2020-2040*, U.S. Army Training and Doctrine Command, Fort Eustis, 01 February 2017, https://apps.dtic.mil/sti/pdfs/AD1028373.pdf (accessed 10 April 2021) 9, 12, 13, 25, 28, 32.

3 David Petraeus, & Andrew Roberts, Conflict: The Evolution of Warfare from 1945 to Ukraine, William Collins, 2023, page 15.

4 Australian Army, *Land Warfare Doctrine 2-0: Intelligence 2018*, 18. New Zealand often uses Australian Defence Force Doctrine, providing New Zealand adjustments in classified supplements.

5 Headquarters, Department of the Army, *ADP 2-0: Intelligence* July 2019, Glossary-4 (page 76).

6 Australian Army, *Land Warfare Doctrine 2-0: Intelligence.*.

7 Australian Army, *LWD 2-0*, Chapter 2, 11.

8 Geraint Evans, "Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle," *Defence Studies,* Vol. 9, No. 1 (March 2009), 22.

9 Mark Lowenthal, *Intelligence: From Secrets to Intelligence*, Eighth Edition, (Washington D.C.: Sage, 2019); John Hughes-Wilson, O*n Intelligence*, (London: Constable, 2016); Michael Warner, *The Rise and Fall of Intelligence*, (Washington D.C.: Georgetown University Press, 2014); Christopher Andrew, *The Secret World: History of Intelligence*, (New York: Yale University Press:2018); Christopher Andrew, Richard Aldrich, & Wesley K. Wark, *Secret Intelligence: A Reader*, Second Edition, (London: Routledge, 2019).

10 Australian Army, *Land Warfare Doctrine* (*LWD) 2-0: Intelligence*, 2014; US Army, *ADP 2-0: Intelligence,* 2019; *Army Doctrine Publication: Land Operations,* 193.

11 Evans, "Rethinking Military Intelligence Failure," 27; LWD 2-0, 4-7; McMaster *Functional Concept*, 32.

12 Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, (New York: Penguin Press, 2016); James Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence*, (New York: Viking, 2018).

13 Evans, Rethinking Military Intelligence Failure, 24.

14 Bruce Berkowitz, *Best Practice in the Information Age*, (New Haven, Connecticut: Yale University Press, 2000) 21-22; Evans, Rethinking Military Intelligence Failure, 27.

15 Concepts and Doctrine Centre, *Joint Doctrine Note 2/20: Threat Finance and the Economic Levers of Power*, UK Ministry of Defence, November 2020, available at www.gov.uk/mod/dcdc, 37; Bryan Harris and Dave Lee, "The cyber threat to America's beef," *FT Weekend*, 5/6 June 2021, 6.

16 The Economist, "The promise of open-source intelligence," 06 August 2021 available at: https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence, accessed 07 August 2021, and 01 September 2021); Elsa B. Kania, "AI Weapons in Chinese Military innovation," *Global China*, Brookings Institute, available at https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania.pdf, (accessed 07 September 2021), 2.

17 John Howard and Seamas Whitesel, "Data Sentinels," Defense Intelligence Agency, 16 April 2020, 1.

18 Howard, and Whitesel, "Data Sentinels," 3.

19 Edward A. Smith, *Effects Based Operations – Applying Network Centric Warfare in Peace, Crisis and War*, (Washington D.C.: US Department of Defense Command and Control Research Program, 2003), 104.

20 David Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare,* Second Edition, (Washington D.C.: Department of Defence C4ISR Cooperative Research Program 2000), 8.

21 Ministry of Defence, "Network Enabled Army C4," https://www.defence.govt.nz/what-we-do/delivering-defence-capability/defence-capability-projects/network-enabled-army-nea-tranche-one/, accessed 05 April 2021; Peter Greener, "Towards the Networked Force: an interview with CJFNZ," *Line of Duty*, 01 January 2020, https://defsec.net.nz/2020/01/01/networked-force/ accessed 05 April 2021

22 Evans, Rethinking Military Intelligence Failure, 30; Army Doctrine Publication*: Land Operations*; John Hughes-Wilson, *On Intelligence*: *The History of Espionage and the Secret World*, (London: Constable, London, 2016) *124*.

23 Hugh McAslan, CDI Speech, New Zealand Institute of Intelligence Professionals Conference, 15 October 2020

24 The Economist, "Open-source intelligence challenges state monopolies on information," 07 August 2021, available at https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information (accessed 06 August 2021.); The Economist, "The promise of open-source intelligence," 06 August 2021 available at: https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence, accessed 07 August 2021, and 01 September 2021); The Economist, "How spies should use technology," 05 July 2024, https://www.economist.com/leaders/2024/07/04/how-spies-should-use-technology, accessed 05 July 2024.

25 Howard Broad, *National Security System in 2016,* Speech by Howard Broad, Deputy Chief Executive – Security Intelligence Group, DPMC*,* Massey National Security Conference, 30 August 2016, available at https://dpmc.govt.nz/sites/default/files/2017-03/national-security-system-2016-howard-broad-speech.pdf (accessed 29 March 2021).

26 Mark M. Lowenthal, *Intelligence: From Secrets to Policy, 7th Edition*, (Los Angeles: CQ Press, 2017). Hughes-Wilson, *On Intelligence*; McMaster *Functional Concept;* Chris, Fussell, David Silverman, General Stanley McChrystal, Tantum Collins, Te*am of Teams: New Rules of Engagement for a Complex World (* United Kingdom: Penguin Books Limited, 2015); Michael T. Flynn, Michael Ledeen, *The Field of Fight: How We Can Win the Global War Against Radical Islam and Its Allies*, (United States: St. Martin's Publishing Group, 2016); Fred Kaplan, *The Insurgents: David Petraeus and the Plot to Change the American Way of War,* (United Kingdom: Simon & Schuster, 2013).

27 Chris, Fussell, David Silverman, Stanley McChrystal, Tantum Collins, Te*am of Teams: New Rules of Engagement for a Complex World.* United Kingdom, Penguin Books Limited, 2015; Fred Kaplan, *The Insurgents: David Petraeus and the Plot to Change the American Way of War,* United Kingdom: Simon & Schuster, 2013; Lawrence E. Cline, "Special Operations and the Intelligence System," *International Journal of intelligence and Counter-Intelligence*, 18:4, 575, 21 August 2006; US Army Field Manual FM 3-05.102, *Army Special Operations Forces Intelligence,* July 2001; Stanley McChrystal, *My Share of the Task: A Memoir*, (United States: Penguin Publishing Group, 2013) 127-129. William H. McRaven, *Sea Stories: My Life in Special Operations*, (United States: Grand Central Publishing, 2019);

28 ISTAR: Intelligence, Surveillance, Target Acquisition, and Reconnaissance.

29 Dave Travers, "Brigade ISTAR Operations," *The Army Doctrine and Training Bulletin,* 3/4 and 4/1, Winter 2000/Spring 2001, 48, available at http://publications.gc.ca/collections/Collection/D12-9-3-4E.pdf, accessed 04 April 2021.

30 Modern War Institute at West Point, "Artificial Intelligence in Counterterrorism and Counterinsurgency," *Irregular Warfare Podcast,* 31 December 2020, available at https://itunes.apple.com/WebObjects/MZStore.woa/wa/viewPodcast?id=1514636385&i=1000504036133 (accessed 18 March 2021).

31 Lawrence E. Cline, "Special Operations and the Intelligence System," *International Journal of intelligence and CounterIntelligence*, 18:4, 576, 21 August 2006.

32 Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Center for a New American Security (2010) Stable URL: http://www.jstor.com/stable/resrep06183 (accessed 20 March 2021); McChrystal et al, *Team of Teams, 138;* Robert Kaplan, *"Man Vs. Afghanistan," The Atlantic*, April 2010, available at http://www.theatlantic.com/magazine/archive/2010/04/man-versus-afghanistan/7983, (accessed 27 March 2021); McChrystal, *My Share of the Task: A Memoir*, 127-129; McRaven, *Sea Stories*.

33 Flynn, Pottinger, and Batchelor, Fixing Intel; McChrystal et al, *Team of Teams, 138;* Robert Kaplan, *"Man Vs. Afghanistan,"*; McChrystal, *My Share of the Task:* 127-129; McRaven, *Sea Stories*.

34 Lowenthal, *Intelligence: From Secrets to Policy,*

35 Hughes-Wilson, *On Intelligence*.

36 Ibid., 143.

37 V.H. Ruiz, *A knowledge taxonomy for army intelligence training: An assessment of the military intelligence basic officer leaders course using Lundvall's knowledge taxonomy,* Masters of Public Administration, Texas State University, San Marcos, TX, 2010.

38 Constantin Stan, & George Negru, " Culture of Intelligence and the training of Intelligence Officers," International Scientific Conference "Strategies XXI"; Bucharest Vol. 3, : 167-173. (Bucharest: «Carol I» National Defence University, 2012); S.B., Dahle and I.M. Mostulien, "Combining the Teaching of Intelligence, Arabic, and Culture at the Norwegian Defence Intelligence School," in K. Enstad & P. Holmes-Eber (eds) *Warriors or Peacekeepers?* (Cham: Springer, 2020), https://doi.org/10.1007/978-3-030-36766-4_8, accessed 11April 2021, 137-138.

39 Marygail K. Brauner, Hugh G. Massey, S.G. Moore, & Darren D. Medlin, "Improving Development and Utilization of U.S. Air Force Intelligence Officers," RAND Corporation Technical Report, 2009, available at https://apps.dtic.mil/sti/pdfs/ADA503766.pdf (accessed 28 March 2021.)

40 Flynn, Pottinger, and Batchelor, Fixing Intel; Leo Blanken and Justin Overbaugh, "Looking for Intel?...or looking for Answers? Reforming Military intelligence for a Counterinsurgency Environment," *Intelligence and National Security*, 27:4, 569.

41 Flynn, Pottinger, and Batchelor, Fixing Intel, 23; Blanken and Overbaugh, Looking for Intel?, 559-575.

42 H.R. McMaster et al, *Functional Concept,* 9, 12, 13, 25, 28, 32.

43 Georg Hegel cited in William Hoverd, "What is Research," Applied Research Methods, Massey University, 22 March 2021

44 William Hoverd, "What is Research," Applied Research Methods, Massey University, 22 March 2021.

45 Zina O'Leary, *Researching Real-World Problems: A Guide to Methods of Inquiry,* (London: Sage, 2005), 8 and 9.

46 SIGINT: Signals Intelligence; HUMINT: Human Intelligence; OSINT: Open Source Intelligence; GEOINT: Geospatial Intelligence.

47 Australia Army, LWD 2-0, 8.

48 Kaplan, *The Insurgents,* 132.

49 According to the National Security Intelligence Priorities (NSIPs), as published in: Department of Prime Minister and Cabinet, *Annual Report 2018/19 for the year ended 30 June 2019*, available at https://dpmc.govt.nz/sites/default/files/2019-10/dpmc-annual-report-2019.pdf, accessed 13 June 2020, 85.

50 Department of Prime Minister and Cabinet, *Annual Report 2018/19 for the year ended 30 June 2019*, available at https://dpmc.govt.nz/sites/default/files/2019-10/dpmc-annual-report-2019.pdf, accessed 13 June 2020, 85.

51 Ministry of Defence, *Strategic Defence Policy Statement,* Ministry of Defence, Wellington, July 2018, available at http://www.nzdf.mil.nz/downloads/pdf/public-docs/2018/strategic-defence-policy-statement-2018.pdf (accessed 07 May 2019).

52 CSIS technology and Intelligence Task Force, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence*, Centre for Strategic &International Studies, January 2021; Bruce Berkowitz, *Best Practice in the Information Age*, (New Haven, Connecticut: Yale University Press, 2000) 21-22; Evans, Rethinking Military Intelligence Failure, 27. Elsa B. Kania, "AI Weapons in Chinese Military innovation," 2. Concepts and Doctrine Centre, *Joint Doctrine Note 2/20: Threat Finance and the Economic Levers of Power*, UK Ministry of Defence, November 2020, available at www.gov.uk/mod/dcdc, 37; Bryan Harris and Dave Lee, "The cyber threat to America's beef," *FT Weekend*, 5/6 June 2021, 6.

53 CSIS, *Maintaining the Intelligence Edge*, X.

54 CSIS *Maintaining the Intelligence Edge*, 3 and 6.

55 If this was the case McChrystal would have reversed the rank paradigm and seen intelligence officers outrank operations officers.

56 CSIS, *Maintaining the Intelligence Edge*; Bruce Berkowitz, *Best Practice in the Information Age*, (New Haven, Connecticut: Yale University Press, 2000); Evans, Rethinking Military Intelligence Failure; Howard and Whitesel, *Data Sentinels*; Elsa B. Kania, "AI Weapons in Chinese Military innovation."

57 Ministry of Defence, Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations, Third Edition with Change 1, 2011, available at https://assets.publishing.service.gov.uk/government/uploads.system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf (accessed 29 September 2021) Section V, page 5-16 (page 155)