DFRT 19/11

Australian Government
Defence Force Remuneration Tribunal

DECISION

Defence *Act 1903*
s.58H—Functions and powers of Tribunal

JOINT CYBERSPACE WARFARE EMPLOYMENT CATEGORIES
(Matter 3 of 2019)

MS I. ASBURY, PRESIDENT

MR A. MORRIS, MEMBER

CANBERRA,29 AUGUST 2019

RADM J. GOLDRICK AO CSC RAN RTD, MEMBER

[1] This decision arises from a listing application[1] made by the Australian Defence Force (ADF) under section 58H of the *Defence Act 1903* proposing three new employment categories within Army and Air Force to align with the Navy cryptologic sailor workforce and provide a Joint[2] ADF cyberspace warfare capability.

[2] We were assisted in this matter by an inspection and demonstration at the Joint Cyber Unit in Canberra on 11 July 2019. We subsequently considered the matter in hearing on 12 July 2019. Mr J Philips SC appeared for the ADF and Mr J Preuss for the Commonwealth. Major General M Thompson AM, Head of Information Warfare, Colonel E Wunsch, Commandant Defence Command Support Training Centre, and Wing Commander D Clyde CSM, Commanding Officer 462 Squadron, all appeared as witnesses at the hearing.

[3] Evidence concerning some aspects of this matter was classified and will not be reproduced or expanded upon in this decision.

BACKGROUND

[4] For the purposes of this matter 'cyberspace' is regarded as all of the ADF computer networks and the digital systems that connect to those networks. 'Cyber warfare' is considered to be activities conducted in or through cyberspace to defend, attack or affect it and is deemed a further warfighting domain in addition to the sea, land, air and space domains.

[5] In Matter 12 of 2017 – *Royal Australian Navy: Cryptologic sailors*[3] a 'Cryptologic Network sailor' category was established to provide a dedicated and defined cyber workforce for Navy. No specific cyber warfare career paths presently exist within Army or Air Force and both Services utilise personnel from a range of employment categories to achieve their cyber warfare workforces.

SUBMISSIONS

ADF

[6] The submission proposes three new career structures within Army and Air Force, as part of an overall integrated ADF workforce, for the conduct of cyber warfare in the cyberspace environment. The ADF submits that cyber warfare operations "*will demand a flexible and modern approach to workforce employment so that this highly specialised workforce is equipped to meet the challenges of ever-growing technical sophistication and complexity in a rapidly evolving environment*".[4]

[7] Specifically, the ADF proposes to create:

a. a new Army Other Ranks category named 'Cyber Specialist';

b. two new Air Force categories named 'Cyberspace Warfare Analyst' and 'Cyberspace Warfare Officer' respectively.[5]

Cyber Specialist

[8] Army principally draws its cyber workforce from 138 Signal Squadron. The ADF submits that the proposed Army Cyber Specialist category will consist of approximately 200 positions. The Cyber Specialist category will be structured in rank from Private to Warrant Officer Class 1.

[9] Army believes a new career structure is achievable within five years and seeks salary protection to apply to members who volunteer and are accepted into the new category.

Cyberspace Warfare Analyst

[10] Air Force presently draws its cyberspace warfare workforce from 462 Squadron. For Air Force the proposed workforce will comprise approximately 90 Cyberspace Warfare Analysts.

[11] The Cyberspace Warfare Analyst category will be structured in rank from Aircraftman/woman to Warrant Officer.

Cyberspace Warfare Officer

[12] The Cyberspace Warfare Officer category will consist of 60 officers and be structured in rank from Pilot Officer to Wing Commander with the potential long-term need for more senior ranks.

[13] Air Force also believes the career structure is achievable within five years and seeks the same salary protection provisions as Army.

COMMONWEALTH

[14] The Commonwealth submission[6] was concerned with the "*absence of industrial history for cyber warfare categories*" and that "*pay placements for the three categories have been guided by comparable existing employment categories with the technical, intelligence and engineering families*".

[15] Overall the Commonwealth reported "*reservations as to whether the pay structures as proposed will have longevity*" and that it "*seems likely the ADF will need to address competitiveness of salary at a future point when the ADF has a trained experienced workforce attractive to potential employers outside of the ADF."*[7]

WITNESS EVIDENCE

Major General Thompson AM

[16] We note the written evidence of MAJGEN Thompson that "*we have the opportunity to build a Joint workforce right from the very start*".[8] We took particular note of the *ab initio* recruitment requirements expanded upon by MAJGEN Thompson and are encouraged by the approach described as: "*we seek to grow this workforce that we need to open to all avenues of entry and certainly, the Chief of Defence Force has, in consultation with the three Service Chiefs, agreed to consider on a case by case basis waivers to several traditional entry standards*".[9]

[17] In the hearing MAJGEN Thompson also expanded on this innovative approach outlining that: "*with the Total Workforce Model we've got greater flexibility between the permanent work-force and the part-time workforce*". He added that "*there's people who have joined us who can commit to 50 or 100 days a year, and several large companies from Australian industry have actually adjusted their personnel policies to provide additional leave for Reserve service and that's been particularly pleasing for us"*.[10]

Colonel Wunsch

[18] COL Wunsch outlined the scope of the workforce stating that "*the three Services are responsible for force generation of the workforce: raise, train and sustain. Once the capability is mature, the goal is to provide a trained capability for use in a combined environment or Joint operation. The concept is that the Services and Joint* [areas] *have a training system in place, provide a range of posting opportunities that will develop our people, and then provide those experienced people to the Joint areas across the ADF, Defence, and other agencies and countries to meet a range of Service and Joint* [area] *needs and requirements, protecting and defending networks and mission systems"*.[11]

[19] Again, expanding on the new workforce construct, COL Wunsch acknowledged that "*there is an acceptance that Army are not going to get such specialised people to be a platoon sergeant and lead a platoon out on a fighting patrol. These Cyber specialists should not be put in that role. We expect that these members will very likely be sitting in front of a computer in a secure building or forward location somewhere and be focused on protecting and defending networks"*.[12]

Wing Commander Clyde CSM

[20] WGCDR Clyde expanded on MAJGEN Thompson's evidence further detailing the recruitment parameters. During the hearing he highlighted the *"critical thinking skills and agility, or mental agility, the ability to take on volumes of data and then make decisions rapidly, make observations, make decisions, react"* and that *"the people with in the cyber warfare capability need to have strong communication skills to work effectively as a team"*.[13]

[21] In written evidence WGCDR Clyde detailed the challenges with the current workforce and how "*workforce stress is being generated because the individuals that work in this cyber space don't know what's next for them*".[14] Again, in the hearing he expanded on this stating that *"they're attractive to industry, they don't know what's next for them in their career path within the ADF because there's a lack of defined or workforce structure, they're facing the prospects of potentially being sent into areas that are not in their area of passion and we have had a number of instances in the last eight months where people who are approaching that stage in their progression through the squadron are choosing to leave*".[15]

[22] Additionally WGCDR Clyde detailed the reasons Air Force had elected to construct an officer workforce within the category, unlike Navy and Army. He gave evidence that "*Air Force has developed the Cyber Warfare Officer largely because we didn't have another officer category that we considered suitable, or acceptably suitable, to provide that leadership element within the cyber warfare capability*".[16]

CONSIDERATON

[23] We considered the evidence that all three of the Services are taking steps to develop their cyber warfare capabilities to conduct Joint operations. We agree that the current workforce is somewhat disjointed and lacks defined specialisations and formal career pathways to manage a Joint cyber capability.

[24] We considered the evidence that Army and Air Force have attempted to meet the needs for this workforce from related categories, however this has created a set of challenges and workforce behaviours that are undesirable including:

a. an inability to identify and recruit talented members likely to excel in the cyber warfare environment as no single employment category specialises in this field;

b. difficulty in developing and maintaining a sufficiently skilled workforce to meet the ADF's cyber warfare capability requirements as members post in and out of specialised and non-specialised positions;

c. difficulty for members to plan their own careers as a formal pathway does not currently exist; and

d. members being required to develop skills outside of their primary employment.[17]

[25] We further considered the evidence that creation of three new career structures will enable the ADF to maintain its cyber warfare capability through mitigating the difficulties of:

a. managing the increase in training requirements due to skills, knowledge, aptitude and other traits differential between cyber warfare and current technical and operations based workforces;

b. producing and implementing specialist selection screening and testing methods to mitigate workforce risks associated with training failure;

c. introducing career continuums to increase recruitment, mitigate workforce retention risk and facilitate the creation of an essential advanced skill level; and

d. managing workforce expectations when members pursuing a career in cyber warfare face career uncertainty with no specific training, guidance or direction explicit with current career and salary constructs.[18]

[26] We considered that Air Force requires an officer category within the workforce as it does not have General Service Officer option in the way that Army can utilise, nor another suitable warfare specialist such as the Maritime Warfare Officer within Navy.

[27] We accept that the typical skills used by this specialist workforce take years to develop and demand a long term approach to the career structure and management of the members. We agree that this workforce will need a career continuum that is flexible and adaptable. We considered the evidence that in order to allow this flexibility the alignment of pay and skill grades, as opposed to directly linking rank and skill grade to pay placement will be required.

[28] We agree with the ADF submission that the pay grade (PG) range between PG4 and PG7 for the Other Rank Cyber Specialist and Cyberspace Warfare Analyst is aligned with Navy's Cryptologic Sailor Networks. And that a pay range between PG2 and PG7 for Cyberspace Warfare Officers maintains relativity within the Graded Officer Pay Structure.

[29] We note that on transition members will retain their rank from their current employment category and, as appropriate, have relevant qualifications and competencies recognised.

[30] We accept the evidence that in-Service transfers from existing categories will commence from January 2020 with recruiting through Defence Force Recruiting expected from 2021.[19] We note that Air Force does not intend to place direct entry Reserve personnel into the two new categories, while Army has endorsed the recruitment of direct entry Reserves "*only where they meet Service need and skill grade pre-requisites*".[20]

CONCLUSION

[31] We accept there has been a conscious effort where possible to align the role descriptions and category structures relevant to cyber warfare capability across the three Services. We agree that the creation of these three new categories will now enable Army and Air Force to consolidate those members presently working in this field into designated and sustainable specialist career pathways.

[32] We agree that, in a similar way to Navy cryptologic sailors, advancement through career paths will predominantly be time and competency based. We also agree that, while completion of specific training courses will largely be mandatory for advancement, a delineation between the technical chain of command and military chain of command and rank is necessary due to the specialised nature of this workforce. We accept that the ADF retains an expectation that members will increase both skill and pay grade to gain promotion. We also accept that placement at a higher skill grade will therefore be competency based and mostly de-linked from rank.

[33] We agree to provide non-reduction salary provisions for a period of five years from 31 October 2019 in order to afford a reasonable time for the members involved to increase their skills and gain additional training.

[34] We accept that Air Force and Army are yet to identify the effects of the market 'pull' factors on this workforce and the impact that may have on additional remuneration in due course. We agree with the Commonwealth that, at present, the proposed approach "*makes sense in the context of the newness of the category, the lack of workforce data and industrial history to be guided by, and the likelihood these categories will be subject to ongoing scrutiny, review and adjustment as the categories mature over time*"[21]. Noting that, we require the ADF to return to us with an interim review in 2022, as part of the Annual Review of Determinations, with a final review of each category in 2025, each of which is to include progress of the salary non-provisions determined.

[35] Determination 6 of 2019 will give effect to this decision with effect from 31 October 2019.

MS I. ASBURY, PRESIDENT
MR A. MORRIS, MEMBER
RADM J. GOLDRICK AO CSC RAN RTD, MEMBER

Appearances:

Mr J Phillips assisted by Mr P Blady for the ADF

Mr J Preuss for the Commonwealth

Witnesses

Major General M A Thompson AM, *Head Information Warfare, Joint Capabilities Group.*

Colonel E F Wunsch, *Commandant Defence Command Support Training Centre.*

Wing Commander D J Clyde CSM *Commanding Officer 462 Squadron.*

---

[1] ADF letter DMR/OUT/2019/09 *Listing Application – Joint Cyberspace Warfare employment categories* dated 6 May 2019.
[2] 'Joint' is referred to throughout this decision as a term defining 'activities, operations and organisations, in which elements of at least two of the Services participate'.
[3] https://www.dfrt.gov.au/sites/default/files/Decision-Navy-Cryptologic.pdf and https://www.dfrt.gov.au/sites/default/files/decision_-_navy_-_cryptologic_network_0.pdf
[4] ADF submission *Matter 3 of 2019 Cyber Warfare Employment Categories* dated July 2019 (ADF 1) page 1 paragraph 1.4.
[5] ADF1 page 3 paragraphs 1.11 and 1.12.
[6] Commonwealth submission *Matter 3 of 2019 – ADF Joint Cyberspace Warfare Employment Categories* dated 26 June 2019 (CWLTH 1) page 4 paragraph 19.
[7] CWLTH 1 page 10 paragraph 70.
[8] Affidavit of Major General M A Thompson dated July 2019 (ADF 2) page 5 paragraph 25.
[9] Transcript 12 July 2019 page 8 lines 22-26.
[10] Transcript page 10 lines 20-26.
[11] Affidavit Colonel E F Wunsch dated 30 July 2019 (ADF 3) page 5 paragraph 21.
[12] ADF 3 page 13 paragraph 53.
[13] Transcript page 28 lines 10-15.
[14] Affidavit of Wing Commander D J Clyde CSM (ADF 5) page 4 paragraph 15.
[15] Transcript page 26 lines 26 – 33.
[16] Transcript page 30 lines 5-7.
[17] ADF 1 page 17 paragraph 4.8.
[18] ADF 1 page 33 paragraph 6.1.
[19] ADF 1 page 31 paragraph 5.32.
[20] ADF 1 page 29 paragraph 5.21.
[21] CWLTH 1 page 8 paragraph 56.