National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

RATIONALIZING NAVAL INFORMATION SYSTEM TECHNICAL BOUNDARIES AND SYSTEM AUTHORITIES

Lieutenant-Commander Iain Richardson

JCSP 50

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

RATIONALIZING NAVAL INFORMATION SYSTEM TECHNICAL BOUNDARIES AND SYSTEM AUTHORITIES

Lieutenant-Commander Iain Richardson

RATIONALIZING NAVAL INFORMATION SYSTEM TECHNICAL BOUNDARIES AND SYSTEM AUTHORITIES

AIM

1. This paper will address the misalignment of NavIS technical boundaries, and the authorities granted to the various levels of the Royal Canadian Navy (RCN) responsible for its sustainment and management. How NavIS is defined is itself in need of clarification. For the purpose of this paper, it is therefore defined as the physical, and logical interconnections between the larger CAF network infrastructure and the infrastructure required to support ships at sea. It will propose a realigned authority structure and the formalization of network management best practices within a rewritten NAVORD 9100. It will also recommend necessary activities to support those changes.

INTRODUCTION

2. NavIS has grown and evolved since its inception over 20 years ago. The inability of the RCN to implement an effective change management process has led to a growing misalignment between the authorities and processes in NAVORD 9100 and the ground truth on ships and at the Network Operations Centres (NOC). This significantly hampers the fleet's ability to perform basic warfare duties, integrate into a coalition fleet, and conduct joint operations at the national level.

3. Limited efforts to realign policy have allowed for the retention of some centralized control, but the fleet remains governed by the tyranny of the immediate. The lack of effective centralized control leads to confusion regarding authorities, divergence of NavIS configurations both within and between classes of ship and makes the timely and efficient execution of capability sustainment and new capability insertion needlessly taxing. This has contributed to projects delivering non-functional outputs due to poor design (e.g., MINeMS) and obsolete equipment due to project time overrun (e.g., WADN NISK/NAG, WANOP). Misaligned governance is not the only culprit; project process and financial management are contributors, but the RCN has little control over these factors. We are, however, the sole authority for NavIS.

DISCUSSION AND ANALYSIS

4. This discussion will be divided in to three parts. The first will be a discussion of NavIS, and the policy environment. The second section will examine its weaknesses and show how and why the logic that underpins it is unfit for modern network operations. This will involve looking at how NavIS has evolved and plotting the divergence between system and governance. The last section will provide recommendations for updating the NAVORD to enable rather than hamper current modernization efforts, and future-proofing it to ensure it aligns with emergent future fleet requirements.

History and Current Status of NAVIS Governance

5. NavIS has always been a 'system of systems'; it exists to aggregate shore-based networks and deliver them in a manner suitable for a ship at sea, and to take data from the ship and distribute it across networks ashore. The number and type of systems NavIS supports has and will continue to grow at an ever-increasing pace, as will the speed at which those systems change. These external networks are managed by over a dozen separate organizations from five different Level 1 (L1) organizations. Importantly, Assistant Deputy Minister (Information Management) (ADM(IM)) and Assistant Deputy Minister (Materiel) (ADM(MAT)) dictate cybersecurity and engineering policy from which the RCN has limited scope to deviate. Most of the lower level stakeholder organizations fall under ADM(IM) and have the benefit of direct liaison that we lack.[1]

6. Whomever manages NavIS must not only be aware of these stakeholders but know under what circumstances they need to be consulted, what devolved authorities they hold, the status of their future and ongoing work, timelines for configuration management change requests, and they the same of us. There is no single desk in the RCN with the capacity and expertise to meaningfully engage with this, and current personnel constraints leave many of the desks that this task has been divided amongst under-crewed and lacking in the necessary expertise. This has led to the majority of integration and liaison work being outsourced to Naval Engineering and Test Establishment (NETE) under civilian contractor support. NETE have become the de-facto managers if NavIS, despite having no formal role in governance.[2]

7. The authorities and structures of NavIS are broadly aligned with the Naval Materiel Management System (NaMMS).[3] This is understandable, as NaMMS ensures the ship and associated systems are safe and fit for purpose. Section four of part 7 focuses specifically on NavIS and outlines top-level authorities and more specific guidance on the change management process[4]. Of note, it exempts NavIS for the requirement to conduct Engineering Change (EC) reviews for changes without a size, weight, or power impact. It also specifically separates NavIS from 'operational' information systems, such as the combat and propulsion management systems.

NAVORD 9100

8. NAVORD 9100 "establishes the RCN ownership, policy, and authorities of NavIS" and establishes the terms of reference for the supporting Working Groups (WG).[5] The NAVORD

---

[1] Cardillo, Guido, 'The Naval Information System Boundary' (Naval Engineering and Test Establishment, 22 August 2023), tbl. 1.
[2] Cardillo, Guido, 15.
[3] Cardillo, Guido, 'The Naval Information System Boundary'.
[4] 'Naval Materiel Management System (NaMMS)' (Assistant Deputy Minister (Materiel), 20 May 2011).
[5] 'NAVORD 9100-0' (Royal Canadian Navy, 15 January 2018), 2.

also summarizes and situates all other NavIS stakeholders. Governance has a three-month cycle for approving major configuration changes matched to a three-deep approval process for technical modifications (i.e. the Technical Authority (TA) recommends changes to the Design Authority (DA) who recommends them to the System Authority (SA) who approves them).[6] Also, "there is no one single authority for the NavIS that provides technical oversight across all systems in the fleet and has the authority to define fleet-level technical standards and reference architectures", thus NETE – whose role should be limited to testing and evaluation of changes against an established baseline – have assumed the role of developing and maintaining that baseline themselves. This lack of an Architecture Authority (AA) is a significant issue.[7]

9. It also contains instructions for managing the Naval Network Transformation Plan (NNTP). This was a spreadsheet tracker for major work on NavIS and also an issue-rectification tracker. It is described as "…the sole repository for all RCN network requirements".[8] The NNTP is not currently up to date, publicly available, or structurally fit for purpose.

NavIS Governance – Weaknesses and Solutions

10. There are three broad issues with the current state of affairs:

    a. Governance as it exists right now is reflective of a last-generation mindset that is too slow to react to change, burdened with excessive oversight, and does not reflect the operational criticality of NavIS;

    b. The RCN lacks the capacity and expertise to implement the current oversight model; and

    c. The RCN has failed to implement a technology-based solution to properly configurations manage NavIS and has effectively lost the ability to centrally manage the system to the degree required to meet modern warfighting requirements.

11. The RCN faces several constraints in dealing with these issues;

    a. NavIS has authorities external to the RCN that dictate many of the cybersecurity and engineering policies that we must follow. These policies can be slow and labour intensive. This is unlikely to change in the near future;

    b. Capacity and expertise to meet current oversight requirements or surge to conduct a complete process overhaul will remain absent for the foreseeable future; and

[6] 'NAVORD 9100-0', 5.
[7] Cardillo, Guido, 'The Naval Information System Boundary', 15.
[8] 'NAVORD 9100-0', 5.

c. The process of onboarding future fleet platforms is already consuming and will unavoidably consume even more resources, reducing the available capacity to address these underlying issues to near-zero.

12. These constraints have thwarted previous attempts at reform and have led to the outsize management role that NETE currently plays. The RCN has published or attempted to publish several documents to address these issues in the past (e.g., the IW strategy paper, RCN Network Operations Modernization 2018-2025, and others), none of which have had an appreciable long-term impact. These are endemic problems, are exacerbated by the current environment, and have resisted numerous attempts at elimination. These issues have caused significant issues with the evolution of NavIS.

The Evolution of NavIS

13. Pressing operational requirements have forced NavIS to evolve regardless of failed reforms. This unstructured evolution has caused significant configuration deviations within and between ship classes. It has also led to a blurring of the technical boundaries between NavIS and the broader CAF IT infrastructure.[9] No two ships have precisely the same configuration or hardware. The coastal Network Operations Centres (NOC) are also configured differently. The NOCs are where the interface between the broader CAF infrastructure and NavIS occurs, so this causes issues with a clearly delineated system boundary.

14. This Unstructured evolution of NavIS creates significant churn. Any time a change is required, each ship of the class must be surveyed to determine their individual configurations. If all configurations are not identical, there are often second- or third- order effects to the change in specific platforms that require roll-on changes. Many changes require liaison with external authority holders. Inconsistent and unclear network boundaries can require repeated engagements to talk through complexities, and the submitting of multiple or extremely complicated technical requests. These requests then take far longer to process, and – given the lack of configuration control – are frequently recalled and resubmitted multiple times as the system changes over time and unknown issues are discovered. This work consumes productivity from the top of the organization to the Base Information System (BIS) and Fleet Maintenance Facility (FMF) workers on the ships. This leaves less time to get ships fit for service and untangle configuration issues. It is a negative feedback loop that has been locked in by policy.

Consequences of the Negative Feedback Loop

15. These problems have all led to a state of affairs where the coastal BISs/FMFs are forced to forego following policy in order to rectify critical issues, and NETE frequently manages external technical liaison and security issues without any meaningful oversight. When higher-order issues arise, answers from the delegated authorities are often delayed, incoherent, or absent

[9] Cardillo, Guido, 'The Naval Information System Boundary', 13.

altogether. In the spirit of getting the job done, action is taken to solve the immediate problem. This action can and has compounded existing issues and interfered with future plans in addition to causing further configuration divergence between platforms.

16. It has also led to technical knowledge and situational awareness being degraded at the authorities. Again, there is a negative feedback loop that draws down the ability of the sitting authorities to function properly. Having NETE as the de-facto AA puts responsibility for RCN networks in the hands of civilian contractors to an unacceptable degree.

17. The specific security implications of this are beyond the scope of the paper, however the general consequences of sloppy configuration management to security standards are well known. These issues are discussed in some detail in the oft cited NETE report, sufficed to say that the current state of the networks on ship does not meet current CAF security standards, let alone the future standards or best practices of our allies.[10] The RCN is currently struggling to upgrade some elements of NavIS away from Windows Server 2008, which is no longer supported and received its final security update in January 2020.[11]

RECOMMENDATIONS

18. NAVORD 9100 is no longer fit for purpose. Any amendments sweeping enough to have an impact on the current state of NavIS will have significant follow-on consequences. Surge crewing to enact and manage change is severely constrained, and resources limited. These recommendations are intended to consolidate and push down authorities as low as possible in order to regain some semblance of control. This is not the ideal solution, but it at least recognizes who in the current system has awareness of the current situation and who exists at the points of contact where decisions are – in effect – already being made.

19. Recommendations for the amendment of NAVORD 9100 are as follows:

a. Governance;

i. Eliminate the Network Advisory Committee (NAC) and merge the NavIS Baseline Working Group (NBWG) and NavIS Technical Planning Working Group (NTPWG). Pass all functions of the NAC directly to Director Maritime Engineering Platform Management (Major Surface Combatant) (DMEPM(MSC)) 2 and Director Naval Information Warfare (DNIW) 6 with the authority to further delegate functions as they see fit;

ii. Establish Commanders Critical Information Requirements (CCIRs) for DNIW and DMEPM which require MSC 2 and DNIW SSO NavIS to

[10] Cardillo, Guido, 17–18.
[11] 'Windows Server 2008', in *Wikipedia*, 11 February 2024, https://en.wikipedia.org/w/index.php?title=Windows_Server_2008&oldid=1206296572#cite_note-60.

report only critical technical and operational issues. Automate them through the NNTP;

iii. Include a complete structural, operational and management plan for the NNTP in the appropriate annex. Give DNR 6-4 and DNIW SSO NavIS formal responsibility for the system;

b. Authorities;

i. Empower DMEPM(MSC) with the Architecture Authority (AA) role;

ii. Consolidate all other ADM(MAT) authorities for all ship classes and ashore under MSC;

iii. Consolidate Design and System Authority no higher than MSC 2, with the authority to delegate further. Remove the linear reporting requirement (TA-SA-DA) and allow TAs to submit change requests directly to the AA; and

iv. Create a TA for NavIS ashore. Allow for TAs to be delegated as low as possible, ideally to an MSC 2-X-X desk in the case of Minor War Vessels (MWV).

c. Structures;

i. Establish a formal support role for NETE, particularly in supporting the AA in meeting configuration management requirements, and with assisting in the management of external stakeholder relations and requirements; and

20. An upgraded NNTP is essential to mitigating the risk of delegating down authorities. Creating it will take uninterrupted work from a team of 3-4 skilled, knowledgeable people over the course of several months. It must be completed quickly in order to ensure the information it contains does not go stale prior to activation.

21. These changes are substantial. Given the complexity of IT management in DND/CAF there is a significant risk of serious unintended second order effects and failures of oversight, and the NNTP is the only mitigation. Given the current situation and how manifestly unfit current governance is for the future, these risks are necessary.

22. This is a significant workload increase for MSC, particularly MSC 2. Without additional personnel, these changes are not supportable. Every effort should be made to fully staff the section and augmentation should be provided. MSC 2 / NETE liaison will be key to supporting

the stand-up of the AA, and it is recommended that MSC be granted sufficient financial and contracting authorities to manage the portion of the greater NETE contract devoted to NavIS in its entirety.

23. These changes are intended to rectify immediate pressing issues, and while they will ease the transition to the fleet of the future, they will not support it. As platform specific instances of NavIS become more complex, authorities will have to be redistributed across additional desks, especially within ADM(MAT).

24. NETE has published a study that is cited widely in this paper. The technical recommendations contained therein must be actioned in support of this document to ensure the success of both.

CONCLUSION

25. You will notice the lack of the word 'risk' when discussing the current state of NavIS. The International Organisation for Standards (ISO) defines risk as the "effect of uncertainty on objectives… characterized by reference to *potential* events and consequences, or a combination of these."[12] All of the risks regarding the management and oversight of NavIS have long since materialized. The RCN is far past the point of mitigating or managing them. The remaining risks exist at the tactical edge, are severe, and are being managed piecemeal by civilian contractors and dockyard workers who are – on paper – peripheral to the system of governance. It is not a matter of how to prevent the governance negative-feedback-loop, or even how to patch over the damage it has caused, but what we must attempt before the situation has severe operational ramifications or a noncompliance issue arises that results in the RCN losing its authorities altogether.

26. By putting authorities at the lowest possible level, whilst still retaining them at the centre, it is hoped that the ongoing issues and problems with NavIS can be moderated, and a more agile, more responsive, and more effective model of management be created.

[12] 'ISO Guide 73:2009(En), Risk Management — Vocabulary', accessed 19 February 2024, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

BIBLIOGRAPHY

Cardillo, Guido. ‘The Naval Information System Boundary’. Naval Engineering and Test Establishment, 22 August 2023.

‘ISO Guide 73:2009(En), Risk Management — Vocabulary’. Accessed 19 February 2024. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

‘Naval Materiel Management System (NaMMS)’. Assistant Deputy Minister (Materiel), 20 May 2011.

‘NAVORD 9100-0’. Royal Canadian Navy, 15 January 2018.

‘Windows Server 2008’. In *Wikipedia*, 11 February 2024. https://en.wikipedia.org/w/index.php?title=Windows_Server_2008&oldid=1206296572#cite_note-60.