National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# ENABLING COALITION COMMAND AND CONTROL THROUGH CIS INTEROPERABILITY

Major Ian A.M. MacLellan

## JCSP 45

## Solo Flight

**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 45

## Solo Flight

**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 45 – PCEMI 45
2018 – 2020

SOLO FLIGHT

# ENABLING COALITION COMMAND AND CONTROL THROUGH CIS INTEROPERABILITY

Major Ian A.M. MacLellan

# ENABLING COALITION COMMAND AND CONTROL THROUGH CIS INTEROPERABILITY

## INTRODUCTION

The ability to communicate on the battlefield has always been of the utmost importance. Over the years, militaries have developed many ways to communicate internally and with allies. They have used signaling flags, light sequences, Morse code, and runners, to name a few methods from history, to facilitate communications. Over the years this requirement to communicate and share information has not changed, but the volume of information or data being shared, and the technology to facilitate it has changed immensely.

In the current global threat environment, there is a very low probability that a nation would conduct operations outside of a coalition. Additionally, in today's battlespace, information is being collected and stored all the time using a variety of sensors and other collectors. This information, depending on its content, can be used to support the planning of future offensive and defensive operations, and to support real time targeting activities. Access to this authoritative data collected and created by allies is more important then ever before when operating in the current conflicts around the world.

Canada's most recent Defence policy: Strong, Secure, Engaged, presents the framework guidance for Canadian Armed Forces (CAF) initiatives and priorities until 2037.[1] Within Strong, Secure, Engaged, "at least 33 of the SSE's 111 strategic investment Initiatives require strong and well-coordinated contributions from the Defence

[1] Department of National Defence, *Canada's Defence Policy: Strong, Secure, Engaged* (Ottawa: Canada Communications Group, 2017).

Information Programme, with the expectation that DND's enterprise capability development will enable the CAF to deliver on its core missions for day-to-day activities and operations."[2] Of these 33 strategic investment initiatives, there is a lot of emphasis on the development of new capabilities and integration of capabilities within a joint context to provide interoperability among CAF elements. However, the importance of integration and interoperability with our allies and coalition partners needs to be factored in concurrently. For this reason, interoperability with joint, interagency, multinational, and public (JIMP) partners has made it to the prioritized list of C4ISR strategic objectives for the CAF J6, and is considered one of the main lines of operations.[3]

It is the utmost importance to take the right steps to ensure we are able to communicate with our allies within a shared battlespace and the ability to share authoritative data, and what Canada and the international community are doing to achieve success in this area.

**AFGHANISTAN**

Many nations have the capability to extend their national networks, and to support administration and operations within a theatre of operation. However, the stand up of the International Security Assistance Force Afghanistan proved that these networks alone are not enough to provide effective communications for command and control within a coalition environment. As a result, the Afghan Mission Network (AMN) was created to facilitate communications and the sharing of information among the coalition partners. While the "AMN proved to be operationally successful, and demonstrated clear benefits

[2] Department of National Defence, Assistant Deputy Minister (Information Management), *Defence CIO and CAF J6 Direction and Guidance 2020 – IM and IT, and CAF Joint C2IS Planning* (Ottawa: DND Canada, 2020 (Draft)), 1.
[3] Ibid., 8.

of supporting coordinated military action, increasing operational response speed and reducing the risk of blue-on-blue engagements; however, it had some notable limitations."[4] The AMN was created out of necessity, using an ad hoc process, which created some significant security concerns and limited the ability to make it a fully integrated network. In some cases, to create full interoperability there was a requirement to have a person in the middle manipulating or transferring the data.

During the draw down of forces in Afghanistan, nations participated in the development and analysis of lessons learned from the AMN. The mission proved that future coalition activities will rely on the use of a similar network and that more research and development would be required to build on the successes of the AMN, including reducing its limitations.

**NORTH ATLANTIC TREATY ORGANIZATION**

Based on the lessons learned from the AMN, the North Atlantic Treaty Organization (NATO) elected to set the conditions for success of future missions. The goal was to ensure that coalition nations would have the ability to establish command and control interoperability at the onset of a deployment and not need to build an ad hoc solution. To achieve this, the "Federated Mission Networking (FMN) initiative"[5] was created and included the participation of NATO nations and other non-NATO affiliated nations. The non-NATO affiliated nations include Australia, Austria, Finland, Ireland, New Zealand, Sweden, and Switzerland.[6]

---

[4] Department of National Defence, Chief of Force Development, *The Canadian Federated Mission Network Vision and Scope Document* (Ottawa: DND Canada, 2014 (Draft)), 1.
[5] North Atlantic Treaty Organization, *Federated Mission Networking - Management Directive Version 2.0* (Belgium: NATO, 2018), 3.
[6] Ibid.

FMN is seen as a supporting initiative in maintaining NATOs ability to rapidly respond to incidents around the world. The management of the FMN initiative and the development of its capability "is one of the most relevant ongoing NATO initiatives to enhance interoperability, resiliency and agility of coalition forces."[7] In order for this initiative to be successful, NATO has ensured that there is a governance model in place to guide and support the development and delivery of this capability. This model is comprised of three main components, FMN Governance, FMN Framework and Mission Networks.

To provide clarification NATO has classified networks in two ways, enduring and episodic. Enduring networks are defined as the networks which are established and operate during peace time and in conflict. These networks are used daily, typically to support administration and planning. NATO has two primary networks which fall into this category, NATO Unclassified (NU) and NATO Secret (NS). Affiliated nations have the ability to communicated with NATO on these networks from their national networks through established connections. Episodic networks are defined as networks which are established for a specific task or mission, and typically only exist for a short period of time. These networks are used for the purposes of conducting command and control, and information sharing within a battlespace or specific mission. AMN is considered the initial episodic network, and the current capability being called Mission Secret (MS) network. Once a MS network is built to support a specific mission, it is given a name to define that particular network episode.

[7] Ibid., 4.

Each episodic network is different, as it supports the interconnection of a specific coalition, and provides services based on the mission requirements. The FMN Framework process is used to define networks and available services. Within the FMN Framework process services are released in increments, "each increment will be referred to as a Spiral."[8] Each affiliated nation is to conduct a periodical readiness verification so that it is known what Spiral they can use. The FMN Management Group provides timelines for affiliates to obtain Spiral compliance. Should an affiliate be unable to engineer their solution to meet the required standards within a Spiral, their ability to establish a connection with a future Mission Network will be come compromised. As details are published with respect to service availability, episodic networks can upgrade from one spiral to another.

The FMN Management and Governance directives layout the management structure, and the roles and responsibilities of the FMN Management Group and its subordinate organizations. Each affiliate has a series of representatives within the Management Group and this allows for their national interested to be presented in support of further development of the capability.

[8] North Atlantic Treaty Organization, North Atlantic Military Committee, *Military Committee Federated Mission Networking (FMN) Governance Directive* (Belgium: NATO, 2017), 4.

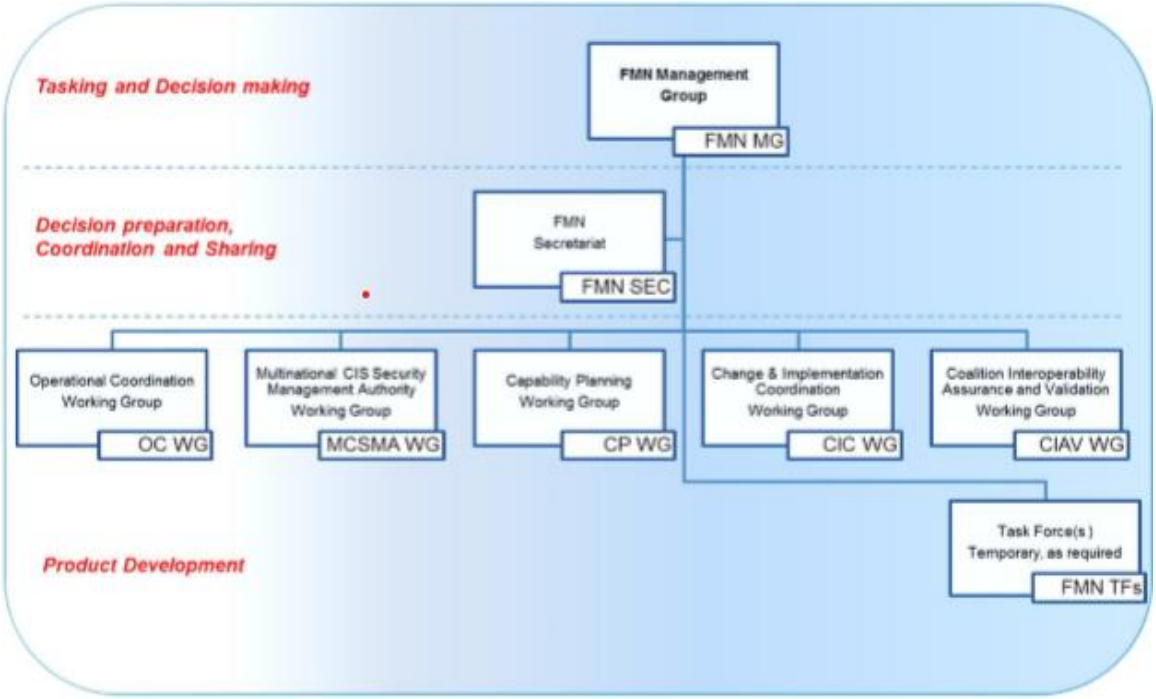


Figure 1: FMN Management, Roles and Functions[9]

NATO's model has grown from an identified need to improve interoperability in a coalition environment, and to share mission critical information to support command and control and the operational planning process. Using lessons learned from Afghanistan and establishing a management and governance model have set the conditions for success of affiliates in future mission. While NATO has taken the lead in this effort, the interest and engagement from non-NATO nations demonstrates that coalition interoperability is a concern for all likeminded allies. The creation of this collaborative environment, through a series of working groups, enables nations with specialities to support others in force development. The risk to this process is the level of buy-in at the national level; national representatives may support the FMN initiative, but if there is a lack of internal

[9] North Atlantic Treaty Organization, *Federated Mission Networking - Management Directive Version 2.0* (Belgium: NATO, 2018), 7.

cooperation within a nation, such as conflicts for resources progress towards coalition interpretability will be stalled.

To validate the current Spiral and baseline of applications and services, NATO holds a series of exercises to allow affiliate nations the ability to test and validate their systems. NATO has been able to establish a standby MS network through the use of various readiness assessment teams, using subject matter experts from affiliates. This MS network is primarily designed for use by the standby NATO Response Force (NRF). In recent years, the work on the development of the NRF MS network has also led to the development and initial deployment of another episodic instance of MS in support of the NATO Enhanced Forward Presence (eFP) mission in Latvia. This network is still in its infancy and has limited nations participating, but it is the first operational deployment of an episodic mission network since AMN.[10]

**FIVE-EYES**

The Five-Eyes (FVEY) community is made of Australia, Canada, the United Kingdom, the United States, and New Zealand. It is a community of likeminded nations that have agreed to share intelligence information. The FVEY has identified the interoperability of communications systems among its partners as a significant issue in its ability to function as a community. As such, the member nations have developed the PEGASUS programme to improve interoperability and provide more rapid access to authoritative data to be used in national and coalition decision making processes. While the intent is for this interoperability to be supported mostly on the enduring national

[10] Coalition Interoperability Assurance and Validation Working Group, Coalition Interoperability Assurance and Validation Working Group Session 23 (Ottawa, ON, October 3 – 7, 2016).

networks, there is a requirement to be able to extend services to episodic instances. It should be noted that the members of the FVEY community are also affiliates within the NATO FMN initiative: there is an attempt to synchronize efforts within both organizations. The challenge becomes the safeguarding of FVEY's information, that is not releasable to NATO partners.

The PEGASUS programme is looking to use technology to create a series of national databases that allow for the interconnection of national networks and the sharing of information based on security protocols within the user's credentials. This is to ensure that the national security orders of each nation are followed, and access is verified and logged. There exists a requirement to increase the speed at which FVEY's nations can gain access to authoritative data. Commanders on the ground require access to authoritative data as soon as possible to support their decision action cycles, the time value for intelligence data collected within a theatre can be very short. In some cases, information that is a few hours old can result in the inability for it to be used in support of target prosecution. Fixing this problem requires a lot of coordination and support from national security stakeholders and advisors within the participating nations. This has the interest of all national Chief Information Officers (CIO), with the understanding that a solution is required to set the conditions for success with respect to interoperability in coalition operations.[11]

**CANADA**

**Afghanistan**

[11] PEGASUS Programme, PEGASUS Working Group (Canberra, AUS, February 19 – 23, 2018).

The Canadian mission in Afghanistan was a Canadian Army (CA) led Task Force with other elements in support. As such, the CA provided the initial Canadian representatives that worked with the coalition partners as part of the development of AMN. Based on this engagement, the Canadian contribution was the CA Land Command Support System (LCSS). LCSS was developed to be a CA tactical level network that enabled command and control using radio equipment, computers, and other communication equipment to interconnect CA units within an area of operations. Additionally, LCSS was designed to interconnect with Canada's Operational and Strategic level network, the Canadian SECRET Network infrastructure (CSNI) network, so it was already interoperable with the United Sates to some degree. The challenge was interconnecting LCSS with the larger caveated coalition network and ensuring the integrity of the network to allow for the maintenance of communications with CSNI.[12]

While the Royal Canadian Navy (RCN) and the Royal Canadian Air Force (RCAF) have experience working in coalition environments, up until this point they either used enduring networks or had the lead nation network extended to their task force headquarters. As the early days of AMN remained a mostly CA concern, the initial Spiral 1 baseline from Canada was based on the LCSS baseline of the period.

**Post-Afghanistan**

As NATO began to development their FMN concept in the post Afghanistan period, the CA maintained their interest and ensured their members served as the Canadian representatives within the committees for the FMN Management Group. As a

[12] Department of National Defence, Commander, Canadian Army, *Army Network Environment (ANE), Concept of Operations Land Command Support System (LCSS) Version 0.5* (Ottawa: DND Canada, 2012).

result, many of the core services that received attention were those of benefit to the CA. This happened for two reasons: firstly, the CA was the lead for this initiative, and secondly the other elements did not see a benefit to redirecting engineering efforts.

In a separate, yet parallel effort, members of the CAF leadership, from a review of the lessons learned from the mission in Afghanistan, determined that there needs to be a focus on the ability to conduct JIMP operations and interoperability within a coalition environment. From this, the JOINTEX series of exercises was born with the first one being conducted in May 2010.[13] This series of exercises was "designed as a catalyst for furthering CF joint capabilities and development with focus on the operational level of war."[14] In the early stages, JOINTEX focused on the national enduring networks, validating the interoperability between the elements, and the operational command structure in Ottawa. The evolution of the series of exercise resulted in the development of the Joint Exercise Mission Network (JXMN) in support of JOINTEX 13. JXMN was based on the current LCSS baseline, with a vision to add some joint services for the RCAF and the RCN. With limited success, aside from core services such as email with attachment and VoIP telephony, it was determined that there was still a lot of work to be done with respect to command and control interoperability.

After the completion of JOINTEX 13, the JXMN was put on the shelf and archived. While the was an increased interest from staff within the Assistant Deputy Minister (Information Management) (ADM(IM)) and Chief of Force Development (CFD) division, there was still no one assigned, from a joint perspective, to guide the CAF's

---

[13] S.J. Bowes, *JOINTEX and Joint Operations Symposium Concept* (Canadian Joint Operations Command: file CJOC 3352-1 (RDIMS# 436964), 8 August 2017).
[14] S.A. Beare, *JOINTEX 13 Stage 4 Exercise Instruction* (Canadian Joint Operations Command: file 4500-1 (RDIMS# 285308), 8 November 2012), 1.

efforts within NATO's FMN framework. Additionally, "the need to ensure integration across the services is not overtly supported through the RCAF doctrine and is clearly distinct from the land and sea environments. This highlights the independent thought and direction of the RCAF."[15]

CFD did become more involved and began to draft CAF supporting documentation in support of the vision and scope of what was to be called the Canadian Federated Mission Network (CFMN). Much of this document mirrored many of the concepts presented by NATO within their FMN documents, but it also looked at CAN/US and FVEY interoperability. Even though there were more organizations involved than just the CA, ADM(IM) and CFD each had their own ideas as to what direction should be explored in achieving a solution to coalition interoperability. However, they recognized that there was "two separate enabling capabilities"[16] for CFMN to be realized, "(1) Network Convergence and (2) Data-Centric Protection."[17] These things would allow for some services that support interoperability to reside on the enduing networks and enable better user authentication for access to authoritative data.

With the progression of the JOINTEX series of exercises, and the increased participation in NATOs NRF validation exercise of 2015, there has been an increase interest from the RCN, and a stronger leadership role taken on by ADM(IM). ADM(IM)'s increase interested was a direct result of many CFD tasks transitioning to the Director of Joint CIS, within ADM(IM).

---

[15] E.A.S Gillingham, "Canadian Forces Joint Signal Regiment – A Joint Command and Control Enabler" (Command and Staff Programme Exercise Solo Flight Paper, Canadian Forces College, 2014), 10.
[16] Department of National Defence, Chief of Force Development, *The Canadian Federated Mission Network Vision and Scope Document* (Ottawa: DND Canada, 2014 (Draft)), 7.
[17] Ibid.

**Future Direction**

All countries want to ensure that their militaries have the most up to date technology to support military operations. Command and Control interoperability is viewed as one of the most important areas for a coalition, as it ensures the safe conduct of operations within the shared battle space. The challenge that Canada has within this space is the environments continue to place their needs above the joint needs of the CAF. As resources are finite, it is imperative that the CAF environmental and joint, engineering and capability development teams work together to ensure CAF success within the space. Given the CAFs recent deployment experience, it is a safe assumption that deployments will be part of a coalition environment for the foreseeable future. "With each service planning and executing based on stovepipe solutions, the CAF continues to re-identify shortfalls while operating in a joint, combined and/or coalition environment."[18] There is a need for an integrated network plan for command and control that supports a commander, regardless of mission, that is capable of being force generated at day zero.

It has been noted that "there has been a gap between strategic guidance and the desire to achieve adaptable CIS to support flexible C2 and the delivery on capability by the individual services."[19] With a significant amount of the Canadian direction and guidance documentation still in draft, it is difficult to secure engagement from all key stakeholders. However, in recent years the release of Canada's Defence policy, Strong, Secure, Engaged, and the CDS' Initiating Directive for the Governance of the Canadian Deployable Mission Networking (CDMN) Capability have begun to change this

[18] E.A.S Gillingham, "Canadian Forces Joint Signal Regiment – A Joint Command and Control Enabler" (Command and Staff Programme Exercise Solo Flight Paper, Canadian Forces College, 2014), 15.
[19] Ibid.

situation. Additionally, the draft Defence CIO and CAF J6 Direction and Guidance 2020 – IM and IT, and CAF Joint C2IS Planning document from ADM(IM) presents a vision to align current interoperability initiatives, and provide leadership and engineering support to create a unified effort.[20] The desired end result would be a series of enduing and episodic networks that support command and control and access to authoritative data, as depicted in figure 2.

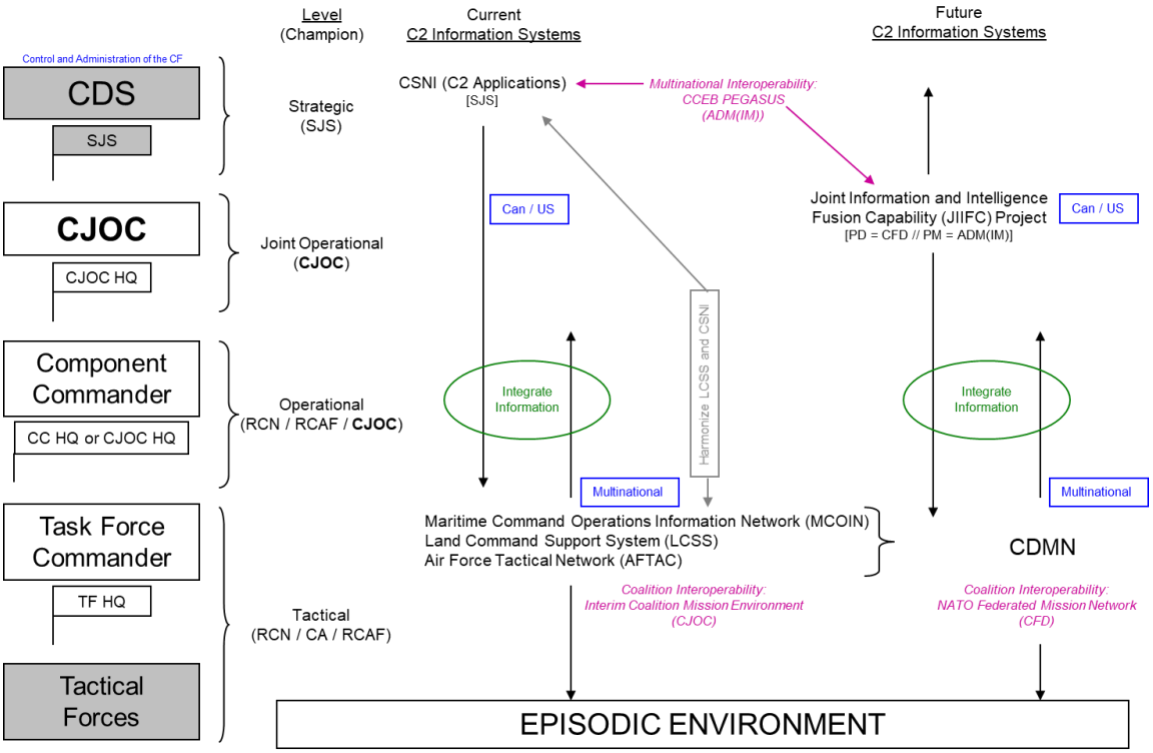


Figure 2: Command and Control Information Systems[21]

In support of this, and based on Canada's Defence policy, Strong, Secure, Engaged, the JOINTEX series of exercises have been aligned to have a rotating focus. Exercises will either have a National, North American, or NATO emphasis so that the

[20] Department of National Defence, Assistant Deputy Minister (Information Management), *Defence CIO and CAF J6 Direction and Guidance 2020 – IM and IT, and CAF Joint C2IS Planning* (Ottawa: DND Canada, 2020 (Draft)).
[21] PEGASUS Programme, PEGASUS Working Group (Canberra, AUS, February 19 – 23, 2018)

CAF continues to "improve…joint operational readiness and capabilities and to enhance interoperability with national and international partners."[22] This also allows for the development and validation of capabilities to support interoperability within our CAN/US, FVEY, and NATO affiliates.

[22] S.J. Bowes, *JOINTEX and Joint Operations Symposium Concept* (Canadian Joint Operations Command: file CJOC 3352-1 (RDIMS# 436964), 8 August 2017), 2.

## CONCLUSION

The ability to communicate on the battlefield has always been of the utmost importance. Over the years this requirement to communicate and share information has not changed, but the volume of information or data being shared, and the technology to facilitate it has changed immensely.

This paper looked at the importance of taking the right steps to ensure the CAF is able to communicate with its allies within a shared battlespace and the ability to share authoritative data, and what Canada and the international community are doing to achieve success in this area.

In the current global threat environment, there is a very low probability that a nation would conduct operations outside of a coalition. Access to the authoritative data collected by our CAN/US, FVEY, and NATO partners is of continued and growing importance. The ability to successfully execute command and control, and planning of future offensive and defensive operations, and to support real time targeting activities, at the operational and tactical level is dependant on access to this data.

There now exists strategic level direction and guidance to set the CAF up for success when operating within all JIMP environments. It is important for all Level 1 organizations and force generating environments to work together with a single goal, through the use of pooled resources. Without organizations stepping up and taking on the leadership roles assigned within the CDS' Initiating Directive for the Governance of the Canadian Deployable Mission Networking (CDMN) Capability, within a whole of CAF approach we will not be successful and stand the risk of being left behind, and out of the picture, by our allies.

**BIBLIOGRAPHY**

Assistant Deputy Minister (Information Management). "Information Management interoperability." Last accessed 2 May 2020. http://admim-smagi.mil.ca/en/about/governance/im-interoperability.page.

Canada. Department of National Defence. *Canada's Defence Policy: Strong, Secure, Engaged*. Ottawa: Canada Communications Group, 2017.

Canada. Department of National Defence. Chief of Defence Staff. *CDS Initiating Directive for the Governance of the Canadian Deployable Mission Networking (CDMN) Capability*. Ottawa: DND Canada, 2018.

Canada. Department of National Defence. Chief of Defence Staff. *CDS Directive CAF Integrated Command and Control Information System*. Ottawa: DND Canada, 2015.

Canada. Department of National Defence. Vice Chief of Defence Staff. *VCDS Tasking Directive – CF C4 Convergence in Support of CF Force Development*. Ottawa: DND Canada, 2012.

Canada. Department of National Defence. Vice Chief of Defence Staff. *The CAF C4ISR Strategic Vision, Goals and Objectives*. Ottawa: DND Canada, 2016.

Canada. Department of National Defence. Commander, Canadian Army. *Army Network Environment (ANE), Concept of Operations Land Command Support System (LCSS) Version 0.5*. Ottawa: DND Canada, 2012.

Canada. Department of National Defence. Assistant Deputy Minister (Information Management). *Defence CIO and CAF J6 Direction and Guidance 2020 – IM and IT, and CAF Joint C2IS Planning*. Ottawa: DND Canada, 2020 (Draft).

Canada. Defence Research and Development Canada. *Command and Control Canadian Armed Forces of Tomorrow (C2CAF-T)*. Ottawa: DND Canada, 2016.

Canada. Department of National Defence. Chief of Force Development. *Next Generation Deployable Communication and Information Systems Vision and Scope.* Ottawa: DND Canada, 2014 (Draft).

Canada. Department of National Defence. Chief of Force Development. *The Canadian Federated Mission Network Vision and Scope Document.* Ottawa: DND Canada, 2014 (Draft).

Canada. Department of National Defence. Chief of Force Development. *Federated Coalition Environment Vision and Scope Document.* Ottawa: DND Canada, 2014 (Draft).

Canada. Department of National Defence. B-GL-005-600/FP001, *CFJP 6-0 Command Support - Study Draft 2.* Ottawa: DND Canada, 2018.

Canada. Department of National Defence. Joint Doctrine Note 02-2014, *Command & Control of Joint Operations.* Ottawa: DND Canada, 2014.

Bowes, S.J. *JOINTEX and Joint Operations Symposium Concept*. Canadian Joint Operations Command: file CJOC 3352-1 (RDIMS# 436964), 8 August 2017.

Beare, S.A. *JOINTEX 13 Stage 4 Exercise Instruction*. Canadian Joint Operations Command: file 4500-1 (RDIMS# 285308), 8 November 2012.

North Atlantic Treaty Organization. *Federated Mission Networking - Management Directive Version 2.0*. Belgium: NATO, 2018.

North Atlantic Treaty Organization. *Federated Mission Networking - FMN High Level Operational Requirements*. Belgium: NATO, 2016.

North Atlantic Treaty Organization. North Atlantic Military Committee. *Military Committee Federated Mission Networking Governance Action Plan*. Belgium: NATO, 2018.

North Atlantic Treaty Organization. Consultation, Command and Control Board (C3B). *Cooperative Arrangement between Consultation, Command and Control Board and the Federated Mission Networking Management Group*. Belgium: NATO, 2017.

North Atlantic Treaty Organization. North Atlantic Military Committee. *Military Committee Federated Mission Networking (FMN) Governance Directive*. Belgium: NATO, 2017.

Coalition Interoperability Assurance and Validation Working Group. Coalition Interoperability Assurance and Validation Working Group Session 23. Ottawa, ON, October 3 – 7, 2016.

PEGASUS Programme. PEGASUS Working Group. Canberra, AUS, February 19 – 23, 2018.

Johannes, C.B.A. "Achieving Multinational Tactical Radio Interoperability." Joint Command and Staff Programme Service Paper, Canadian Forces College, 2018.

Gillingham, E.A.S. "Canadian Forces Joint Signal Regiment – A Joint Command and Control Enabler." Command and Staff Programme Exercise Solo Flight Paper, Canadian Forces College, 2014.

Kearney, R.E. “Canadian Forces Interoperability with the United States Military: A Must for Canada.” Command and Staff Course New Horizons Paper, Canadian Forces College, 2005.

Boettger, E.F. “Canada’s Stature and Influence in Coalitions: A Questions of Salience, Relevance and Interoperability.” Advanced Military Studies Programme Research Paper, Canadian Forces College, 2007.

Fletcher, C.M. “Canadian Forces Transformation Bucking the Trend – Interoperability Trumps ‘Jointness.’” Advanced Military Studies Programme Research Paper, Canadian Forces College, 2003.

Batsford, M.W. “Interoperability: The Key to CF Coalition Operations.” Advanced Military Studies Programme Research Paper, Canadian Forces College, 2006”

Fortin, M.W. “Fusing Islands of Information: The Canadian Forces’ Struggle Towards Command and Control System Interoperability.” Advanced Military Studies Programme Research Paper, Canadian Forces College, 2004”

Bouchard, M. “Interoperability: A Must for the Canadian Forces.” Joint Command and Staff Programme Master of Defence Studies Research Project, Canadian Forces College, 2010.